
bhv
АЛЕКСАНДР
ПОЛЯК-БРАГИНСКИЙ
ЛОКАЛЬНЫЕ СЕТИ
МОДЕРНИЗАЦИЯ И ПОИСК НЕИСПРАВНОСТЕЙ
От двух компьютеров до сети предприятия
Active Directory и приемы администрирования
Выход в Интернет и работа в удаленном режиме
Неисправности и их устранение
СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Александр Поляк-Брагинский

ЛОКАЛЬНЫЕ СЕТИ

МОДЕРНИЗАЦИЯ И ПОИСК НЕИСПРАВНОСТЕЙ

Санкт-Петербург
«БХВ-Петербург»
2006

УДК 681.3.06
ББК 32.973.202
П54

Поляк-Брагинский А. В.

П54 Локальные сети. Модернизация и поиск неисправностей. — СПб.: БХВ-Петербург, 2006. — 640 с.: ил.

ISBN 5-94157-803-2

В доступном изложении рассматриваются вопросы модернизации небольшой сети с изменением ее структуры, методы повышения качества и снижения трудоемкости при администрировании. Приведены примеры модернизации сети, связанной с ее расширением и подключением к Интернету. Примеры структурных схем охватывают диапазон от домашней (квартирной) сети до сети крупного офиса. Предложены пути перехода к более сложным структурам с наименьшими затратами времени и сил. Даны приемы установки и настройки Active Directory, администрирования растущей сети и обеспечения ее бесперебойной работы. Рассмотрены возможные неисправности в сети и пути их устранения. Все примеры воспроизводились автором при подготовке книги или работают в реальных сетях.

Для начинающих системных администраторов и опытных пользователей

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	*Екатерина Капалыгина*
Компьютерная верстка	*Натальи Смирновой*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.03.06.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 51,6.
Тираж 3000 экз. Заказ № 173
"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 5-94157-803-2

© Поляк-Брагинский А. В., 2006
© Оформление, издательство "БХВ-Петербург", 2006

Оглавление

Введение **1**

Для кого эта книга 1
О чем эта книга 3
Как читать эту книгу 4
Сети от FIDO до Internet-2 4
Выполнение операций с объектами ОС 6
Благодарности 9

Часть I. Как работают компьютерные сети? **11**

Глава 1. Общие принципы работы сети **14**

Какие бывают сети? 14
Сеть в вашей квартире 15
Офисная сеть 15
Сеть предприятия 16
Сеть в вашем доме или районе 16
Глобальные сети 16
Многоуровневая модель сети 17
Стандарты 19
Среда передачи данных 22
TCP/IP 24
Цифровой адрес 27
Маска 27
Другие протоколы 34
Порты 36
Имена в сети, как компьютеры узнают друг друга 37
NetBios 39
WINS и DNS 39
Оборудование, применяемое в сети 40
Защита сетевого оборудования по питанию 43
Случай 1 (на предприятии) 43
Случай 2 (домовая сеть) 43
Схема компьютерной сети 44
Схема 1 — самая простая 45
Схема 2 — маршрутизатор 47
Схема 3 — добавляем коммутатор 48

Схема 4 — сервер ... 49
Схема 5 — экономим ... 50
Схема 6 — дружим сетями ... 51
Неисправности ... 52

Глава 2. Операционные системы ... 55

Windows XP ... 55
Особенности Windows XP Professional ... 59
Клавиши Windows ... 63
Панель управления ... 63
Серверные возможности ОС Windows XP Professional ... 65
Обеспечение информационной безопасности ... 66
Синхронизация системных часов ... 67
Межсетевой экран ... 68
Автоматическое обновление ... 68
Windows 98 ... 69
Файловая система ... 70
Работа в сети ... 71
Linux ... 74
Файловая система ... 74
Работа в сети Windows ... 74
Windows Server 2003 ... 77
Файловая система ... 78
Возможности системы ... 78
Возможности применения на персональном компьютере ... 80
Настройка Windows Server 2003 для рабочей станции ... 80
В заключение ... 88

Глава 3. Физическая сеть ... 89

Что мы имеем? ... 89
Требования к компьютерам — рабочим станциям ... 90
Требования к серверу ... 94
Сетевое оборудование и кабельная система ... 94
Рабочее место администратора локальной сети ... 96
Рабочий компьютер ... 101
Оборудование серверной ... 102
Автоматическое проектирование сети ... 103
Структурная схема компьютерной сети ... 108
Спецификация ... 112
Техническое задание на разработку проекта компьютерной сети ... 115
Общие положения ... 115
Описание задачи ... 116
Поиск и устранение неисправностей в кабельной сети ... 119
Очевидная проблема ... 119

Проблема менее очевидная ... 120
Помехи ... 120
Длинная линия ... 121
Инструменты, материалы и оборудование ... 123
Неисправности в физической сети и их устранение ... 126
Вопросы начинающего администратора ... 127
Ответы ... 127

Часть II. Работа в одноранговых сетях ... 131

Глава 4. Настройка рабочих станций для работы в сети ... 134

Общие ресурсы ... 134
Настройка Windows XP ... 135
Если не заработало ... 142
Если в сети компьютер с ОС Windows 98 ... 145
Общее подключение к Интернету ... 147
Доступ по выделенной линии ... 149
Модем ... 162
ADSL-модем ... 165
Доступ к рабочей станции из Интернета ... 172
Если применяем dial-up ... 176
Общий принтер ... 177
Неисправности и их устранение ... 180

Глава 5. Защита информации в вашей сети ... 182

Брандмауэр ... 182
Маршрутизация ... 189
Шифрование ... 193
Антивирусная защита ... 195
Anvir Virus Destroyer (AnVir Task Manager) ... 195
Avast! ... 196
Microsoft AntiSpyware ... 196
Реальные ситуации ... 197
Великое переселение ... 197
Вот как это было ... 199
Выбор режима работы сервера ... 202

Часть III. Переход на выделенный сервер ... 205

Глава 6. Планируем сеть и свою работу в ней ... 208

Группы пользователей ... 209
Операционные системы в сети ... 212

Сервер терминалов ... 212
Где поставим сервер ... 215
Сети и подсети ... 216
Принтеры ... 219
Дополнительное оборудование ... 222
Организация работы администратора ... 223
Дневник администратора ... 224
Состав дневника ... 224
Инструменты администратора ... 227
Команда *Ping* ... 228
Команда *Ipconfig* ... 229
Утилита SuperScan ... 230
Управление компьютером ... 231
Просмотр событий ... 232
Active Directory — пользователи и компьютеры ... 233
DHCP и WINS ... 234
Другие средства ... 237
Radmin (Remote Administrator) ... 241
Возможности программы ... 241
Системные требования ... 242
Установка ... 242
Установка соединения ... 243
Подключение модем-модем ... 243
Настройка RADMIN-сервера ... 245
Установка/изменение пароля для Radmin-сервера ... 246
Окно обозревателя Radmin ... 247
Меню режимов ... 247
Настройки окна удаленного компьютера (Rscreen) ... 250
Управление из командной строки (Command line) ... 250
Вспомогательные средства ... 253
Прямое кабельное соединение ... 253
Правила администратора ... 258

Глава 7. Устанавливаем сервер ... 260

Windows Server 2003 ... 261
Некоторые отличия Windows Server 2003 от Windows 2000 Server ... 261
Установка ... 262
Подключение сети к Интернету ... 264
Почтовый сервер ... 274
Управление почтовым сервером ... 280
Web-интерфейс ... 281
О неисправностях ... 289
Не работает подключение к Интернету с компьютеров сети ... 289
Не удается принять или отправить почту с внешнего почтового сервера ... 290

Не удается принять или отправить почту с почтового сервера своей сети 290
Москва? Петербург на проводе! HELP ME! 291
Первое включение 292
Второе включение 296

Глава 8. Сколько у нас серверов? 302

DHCP-сервер 302
Установка 303
DNS-сервер 312
Установка и настройка 315
WINS-сервер 318
Сервер терминалов 323
Работа через Интернет 326
Возможные неисправности 328

Глава 9. Active Directory 329

Что же такое AD? 329
Установка AD 330
После перезагрузки 336
Политики 338
Добавление пользователей 340
Сетевой профиль 347
Регистрация компьютеров 348
Регистрация других объектов 349
Изменение свойств объектов 350
Сервер терминалов для всех 352
Перезагрузка 354
Интернет-подключение к удаленному рабочему столу 355
Чем этот способ лучше? 359
Возможные неисправности 360

Часть IV. Переход на выделенный сервер 363

Глава 10. Второй сервер 366

Автоматическое присвоение параметров сетевого соединения 384
Для тех, кому мало одного шлюза 386
Трафик надо экономить 387
Open VPN 393
Подключение к рабочим станциям сети 405
Интернет для первого сервера 408
Возможные неисправности и их устранение 411

Глава 11. Администрирование растущей сети и обеспечение ее бесперебойной работы 414

Источник бесперебойного питания 415
Программное взаимодействие 416
Удаленное администрирование 422
Дежурный администратор 424
Резервирование и архивирование данных 426
Acronis True Image Server — резервное копирование всей системы 427
Команда *Xcopy* 432
Нестандартные инструменты администратора 435
Работа с файловой системой 435
Поиск файлов 436
Telnet 439
Применение сценариев 441
Регулярные выражения 441
Сценарий отображения всех файлов в папке 444
Создание, удаление и изменение файлов и каталогов 445
Создание файлов 445
Создание и удаление каталогов 448
Изменение атрибутов файлов и каталогов 450
Вспомогательные средства 451
Управление учетными записями пользователей 454
Получение списка пользователей 455
Получение списка пользователей с помощью сценария VBScript 456
Получение списка групп, в которые входит пользователь, и списка пользователей, которые входят в группу 458
Добавление учетной записи пользователя и ее разблокировка 461
Добавление учетной записи пользователя 461
Создание большого числа учетных записей 465
Удаление пользователя 470
Изменение пароля пользователя 473
Изменение прав пользователя 475
Изменение параметров учетной записи пользователя 476
Создание группы 478
Общий доступ к файлам и папкам 479
Программы в формате HTA 480
Работа сценариев на старых машинах 486

ЧАСТЬ V. РАСТУЩАЯ СЕТЬ — ПРОБЛЕМЫ И ВОЗМОЖНОСТИ 489

Глава 12. Некоторые проблемы администрирования 492

Применение старых ОС 492
Настройка рабочих станций с операционной системой DOS 493

Установка операционной системы MS-DOS 7.1 493
Установка Microsoft Network Client v3.0 for MS-DOS 499
"Портативный" Web и FTP-сервер 504
Autoexec.nos 505
Файл HTTPD.BAT 507
Файл Ftpusers 507
Краткий список команд для управления сервером 508
Настройки DHSP и WINS на сервере Windows 2000 Server 509
Применение настроек рабочей станции DOS при обслуживании компьютеров сети 511
Настройка рабочих станций с операционной системой Windows 9*x* 518
Ограничения для старых ОС в новых сетях 523
Обслуживание рабочих станций 524
Учет трафика в сети 529
Управление удаленным компьютером 532
Telnet и Windows 98 535
Сценарии входа в сеть 536
Средства устранения неисправностей 540

Глава 13. О развлечениях 543

Беспроводная сеть дома 543
Оборудование 543
Организация сети 548
Модем 557
Мобильный Web-сайт как средство общения 558
Реализация идеи 560
Локальные компоненты 561
Лавры ICQ 572
Видеокамера в сети 576
Интеллектуальные развлечения 577
Технические подробности 579

Приложение. Справочные сведения 583

Протоколы TCP/IP 583
Описание расширений масок подсети 585
Соответствие русскоязычных и англоязычных наименований объектов системы 590
Порты 595
Аббревиатуры, сокращения и определения 596
Беспроводная сеть 596
Витая пара 597
Драйвер (driver) 597
Интерфейс 598
Коаксиальный кабель 598

Коммутатор (switch) 598
Компьютерная сеть 598
Коннектор 599
Концентратор (хаб, Hub) 599
Маршрутизатор (router) 599
Модем 600
Одноранговая сеть 600
ОС (операционная система) 600
Пакет 600
ПО (программное обеспечение, программы) 600
Порт 601
Протокол 601
Разрешение имени в адрес 601
"Расшаренный диск" 601
Сегмент сети 602
Сервер 602
Сервер удаленного доступа 602
Сетевая плата 602
Сетевой адаптер (сетевая карта/сетевая плата) 602
Сетевой кабель 603
AD (Active Directory) 603
AUI (Access Unit Interface) 603
Auto-sensing 10/100 Mbps (автоматическое распознавание скорости передачи данных 10/100 Мбит/с) 603
BNS 604
Bridge (мост) 604
Bridge/Router (мост/маршрутизатор) 604
Broadcast (широковещательная рассылка) 604
Broadcast Domain (домен широковещательной рассылки) 604
Broadcast Storm ("лавина" широковещательных пакетов) 604
DFS (Distributed File System) 605
DHCP (Dynamic Host Configuration Protocol) 605
DNS (Domain Name System) 605
DOS ODI и DOS NDIS 605
EFS (Encrypting File System) 606
Ethernet 606
Fast Ethernet 606
FTP (File Transfer Protocol) 606
Gigabit Ethernet 606
Hub 606
HTML 606
Interface 607
ISDN (Integrated Service Digital Network) 607
LAN (Local Area Network) 607
LINKLOCAL 607
MAC-адрес 607

MUI (Multilingual User Interface) 607
NetBEUI (NetBIOS Enhanced User Interface) 607
Proxy Server (Proxy-сервер) 608
TCP/IP (Transmission Control Protocol/Internet Protocol) 608
Telnet 609
Throughput (производительность, пропускная способность) 609
UTP (неэкранированная витая пара) 609
Virtual LAN (VLAN, виртуальная локальная сеть) 609
XML (Extensible Markup Language, расширенный язык разметки) 610
WAN (Wide Area Network, территориально-распределенная сеть) 610
WINS (Windows Internet Name Service) 610
10BASE2 (тонкий коаксиальный кабель) 610
10BASE5 (толстый коаксиальный кабель) 610
10BASE-FL (оптоволоконный кабель 10 Мбит/с) 610
100BASE-FX (оптоволоконный кабель 100 Мбит/с) 611
10BASE-T (витая пара 10 Мбит/с) 611
100BASE-T (Fast Ethernet) 611
Вопросы и ответы 611

Предметный указатель 619

Введение

Еще совсем недавно пользователей ПК волновали вопросы работы с Windows 98, в небольших сетях под управлением этой ОС работали серверы и маршрутизаторы, активно применялась DOS в различных модификациях. Но прогресс неумолимо идет вперед, незаметно ускоряясь, окружая нас все более совершенной техникой, новыми операционными системами, заставляя системных администраторов делать преобразования в существующих сетях, а при создании новых сетей ориентироваться на новейшие достижения в области информатики, все более отвечающие пожеланиям пользователей и требованиям времени. Появление новых операционных систем, новых сетевых технологий требует новых знаний, умения ориентироваться в выборе решений задач, которые встают перед администраторами больших и малых компьютерных сетей. Знания, как известно, даются трудом, а опыт синяками и шишками, набитыми при ошибках, допущенных нами в поиске решения. Есть ошибки, которых человеку невозможно избежать. Ребенок не может перенять опыт ходьбы у родителей. В то же время более старшим детям не требуется попадать под автомобиль, чтобы запомнить, как следует переходить дорогу. Конечно, эксплуатация локальных компьютерных сетей это такая область человеческой деятельности, где невозможно составить правила, подобные правилам дорожного движения. То, что запрещено в одних сетях, разрешено в других. То, что в одной сети является ошибкой, в другой может быть правилом. Найти правильный путь не всегда легко. Но и набивать шишки не всегда есть необходимость. Рост числа компьютеров и компьютерных сетей несколько опережает рост числа сертифицированных специалистов в области информационных технологий. К счастью, существуют книги, в которых многие практические вопросы и возможные ошибки достаточно подробно рассмотрены.

Для кого эта книга

Вот и эта книга — одна их тех, что призваны помочь начинающим администраторам локальных сетей, подсказать наиболее простые пути решения часто встречающихся задач. Для того чтобы вы приобрели уверенность в полезности этой книги для вас, я предлагаю вам небольшой психологический тест. Для определения результатов теста необходимо сложить баллы, соответствующие ответам на вопросы. Число баллов записано в двоичной систе-

ме счисления (bin). В этой же системе следует производить сложение и записывать результат.

Вопрос 1. Считаете ли вы себя таким ассом в деле сетестроения и эксплуатации ЛВС, которому известны абсолютно все тонкости этого вопроса и никакие подсказки не нужны?

Да — 100 (bin)

Нет — 0 (bin)

Вопрос 2. Вы считаете, что достаточно хорошо понимаете, что такое сеть, и как с ней работать?

Да — 10 (bin)

Нет — 0 (bin)

Вопрос 3. Вам предстоит или уже пришлось столкнуться с необходимостью обеспечить работу локальной сети (дома или в офисе), но опыта для уверенной работы явно недостаточно.

Да — 1 (bin)

Нет — 0 (bin)

Проверка результата теста

Если вы, прочитав трижды три строчки перед первым вопросом, не смогли понять, как получить результат теста, то эта книга вам не подходит.

Если вы набрали:

- 100 (bin) баллов, то вероятнее всего вы покривили душой и не очень честно ответили на все вопросы;
- 110 (bin) баллов, то вполне возможно, что ничего нового в книге вы не найдете, но вам будет интересно ее пролистать;
- 10—11 (bin) баллов, то эта книга может оказаться помощником в поиске правильных решений;
- 1 (bin) балл, то эта книга вам просто необходима.
- 0 (bin) баллов, то книга, скорее всего, вам не принесет пользы. Вам не приходилось и не придется работать с локальными вычислительными сетями.

Работать с новыми операционными системами в сети приходится не только опытным администраторам локальных сетей, но и обычным пользователям ПК, которые сталкиваются с необходимостью создания и модернизации локальных сетей. На небольших предприятиях нередко администрировать сеть приходится специалистам совершенно в другой области, например, эконо-

мистам или бухгалтерам, которые хорошо знают специфику работы предприятия, имеют большой опыт работы с ПК, но лишь общее представление о работе сети. В домашних условиях пользователи сталкиваются также с необходимостью организации сети в своей квартире или в своем доме. Такие сети становятся совершенно обычным явлением в нашей жизни, но требуют к себе внимания квалифицированного администратора. Для тех пользователей, которым пришлось столкнуться с организацией локальной сети, и предназначена эта книга. Но полезна она будет и другим читателям. Студенты, специализация которых связана с эксплуатацией сетей, найдут в книге практические примеры организации сетей различного уровня сложности и доступные объяснения некоторых теоретических аспектов вопроса. Молодым пользователям ПК, ищущим свою дорогу в жизни, книга поможет сориентироваться в выборе профессии.

О чем эта книга

Уже из того, что было сказано раньше, в общих чертах вы составили представление о теме данной книги. Тем не менее, расскажем об этом подробнее. Книга проведет вас по этапам создания и модернизации локальных сетей. При этом значительное внимание будет уделено неисправностям в сети, их поиску и устранению. Для кого-то важна информация о начале с нуля, а кому-то необходимо усовершенствовать свою сеть или отладить ее работу. У каждого системного администратора есть определенное недовольство работой своей сети. В одних случаях это недовольство вызвано глубокими знаниями, огромным опытом и сознанием невозможности реализовать идею ввиду технических ограничений. К сожалению, в этих случаях книга бессильна. Недовольство менее опытных администраторов может быть вызвано пониманием того, что сеть работает не совсем так, как хотелось бы (или совсем не так), но знаний и опыта не достаточно для того, чтобы самостоятельно найти истинные причины проблемы. В таких случаях книга может помочь. Большинство начинающих администраторов реально столкнутся с ситуациями, описанными в книге. Сеть, которая рассматривается здесь, основана на операционных системах Microsoft Windows последних версий. MS-DOS, Windows 95 да и Windows 98 уходят из сетей. Некоторые поставщики услуги доступа в Интернет уже прекратили поддержку старых операционных систем ввиду их слабой защищенности, что создает потенциальную угрозу не только для пользователя этой системы, но и для сети в целом. Все же, в ряде случаев старые операционные системы присутствуют на компьютерах, работающих в сети, и отдельные вопросы, связанные с этими операционными системами, будут рассмотрены.

Как читать эту книгу

Материал в книге рассматривается по принципу "от простого к сложному". Поэтому, не имея опыта работы в сети, лучше читать все. Тем не менее, если определенный опыт есть, и требуется лишь помощь в настройке определенного режима работы сети, можно начинать прямо с того места, где есть необходимое описание. Если встретится не совсем понятное предложение или ссылка на рассмотренный ранее материал, нужно, конечно, обратиться к предыдущим разделам. Иногда в книге приводятся ссылки на материал из других источников. По мере возможности информация на эту тему раскрывается в минимально необходимом объеме, но для более детального рассмотрения вопроса следует обратиться к указанным источникам — "нельзя объять необъятное". Иногда изложение может показаться не совсем последовательным. Одних и тех же результатов (с практической точки зрения) можно достичь, применяя различные сетевые технологии. Кто-то при создании своей простой сети опирался на одни технологии, кто-то на другие. Поэтому еще до подробного рассмотрения отдельных технологий и принципов работы сети могут присутствовать упоминания и рекомендации связанные с ними.

Сети от FIDO до Internet-2

Прежде чем мы начнем рассмотрение основного материала книги, полезно кратко ознакомиться с историей развития сетей, собранной по материалам, доступным в Интернете. Информация, представленная здесь, несколько отрывочна, но дает представление о пути развития сетевых технологий, как говорят "от печки" до технологий будущего. Говорят, что причиной начала работ в области сетевых технологий явился запуск первого искусственного спутника Земли. Возможно, что это не совсем так, но даты говорят в пользу этого предположения.

В 1961 г. работу, посвященную коммутации пакетов, опубликовал в Массачусетском технологическом институте Леонард Клейнрок. Это было первое упоминание о коммутации пакетов. Теперь такая технология передачи информации является основой протокола TCP/IP.

В августе 1962 г. доктор наук Джон Ликлайдер, работавший в лаборатории Массачусетского технологического института, представил доклад под названием "Galactic Network", в котором он предсказывал появление глобальной сети, соединяющей компьютеры по всему миру, получить доступ к которой сможет любой желающий. Помимо общей идеи, в докладе были достаточно подробно описаны принципы, на которых должна строиться такая сеть.

В 1965 г. Томас Мэрилл и Лари Робертс, соединив посредством телефонных линий Массачусетский компьютер TX-2 с компьютером AN/FSQ-32, находящимся в институте Беркли (Калифорния), доказали, что для объединения компьютеров в сеть не обязательно прокладывать специальные линии, а вполне можно воспользоваться линиями, уже проложенными телефонными компаниями.

Первую в мире ЛВС (локальную вычислительную сеть) создал в 1967 г. Дональд Дэвис в Национальной физической лаборатории Великобритании. Эта сеть к началу 70-х работала со скоростью 0,25 Мбит/с, обслуживая около 200 пользователей.

В 1970 г. на Гавайских островах Норман Абрамсон создал сеть ALOHA — прообраз будущих Ethernet и IEEE 802.11. Это была первая в мире пакетная радиосеть.

В 1972 г. на Международной конференции по компьютерным коммуникациям (ICCC), состоявшейся в Вашингтоне, прошла первая публичная демонстрация сети, работающей на телефонных линиях.

В 1973 г. появился протокол FTP, предназначенный для передачи файлов по сети.

В 1973 г. Боб Меткалф предлагает фирме Xerox создать Ethernet. Первая Ethernet-сеть, созданная Бобом Меткалфом и Дэвидом Боггсом в исследовательском центре PARC (Palo Alto Research Centre) фирмы Xerox, работала со скоростью 2,944 Мбит/с и соединяла друг с другом два компьютера.

С 1978 г. начали появляться BBS — электронные доски объявлений, и в 1980 г. уже было более тысячи пользователей FIDO — глобальной некоммерческой сети, работающей на основе телефонных сетей (существует до настоящего времени).

В 1979 г. была основана компания 3Com (COMputer COMmunications COMpability — совместимость компьютерных коммуникаций). В ее задачу входило производство сетевого оборудования, соответствующего будущему стандарту Ethernet.

В конце 70-х, начале 80-х на прилавках магазинов появились первые персональные компьютеры, доступные для домашнего пользования. Примерно в это же время началась продажа простых модемов.

В 1977 г. Вард Кристенсен написал утилиту MODEM.ASM (позже переименуется в XMODEM), которая вошла в историю как первая терминальная программа для персональных компьютеров.

В 1984 г. количество узлов в сети ARPAnet (по имени агентства по разработке передовых технологий при Министерстве обороны США — ARPA) перевалило за тысячу, прежняя система адресации стала неудобной (адреса вводились в числовом виде, а для описания всех хостов существовал большой

справочный файл). В это время появилась таблица Пола Мокапетриса Domain Name System (DNS). А первый домен symbolics.com был зарегистрирован 15 марта 1985 г.

Пожалуй, именно эту дату можно было бы считать днем рождения современного Интернета (это мое личное мнение).

В октябре 1996 г. в Чикаго на совместной встрече представители 34 университетов подняли вопрос о том, что пропускной способности магистральных каналов Интернета становится недостаточно для проведения необходимых исследовательских работ. Было принято решение о создании закрытой сети с высокоскоростными линиями передачи данных, применяемой лишь для исследовательских целей. Университеты — участники проекта взялись сами финансировать проект, выделяя на него ежегодно 500 000 долларов. При участии правительства США был разработан и реализован проект Internet-2. В качестве основной транспортной магистрали Internet-2 использует оптоволоконную сеть Abilene.

14 апреля 1998 г. вице-президент США Альберт Гор на церемонии в Белом доме анонсировал начало создания этой сети. Ее разработка началась в феврале 1999 г. Полное развертывание сети, работающей на скорости 2,5 Гбит/с, было закончено через 10 месяцев. В феврале 2003 г. была начата трансконтинентальная программа модернизации сети. В результате скорость передачи данных увеличилась до 10 Гбит/с. В качестве основного протокола используется новый протокол IPv6. Для организации этой сети компанией Qwest Communications было выделено 10 000 миль оптоволоконных линий.

Протокол IPv6, применяемый в новой сети, теоретически позволяет предоставить персональный IP-адрес каждому человеку и каждому устройству. Насколько это полезно, мы увидим, рассматривая подключение к Интернету и ограничения, которые существуют в настоящее время. Для обычных пользователей IPv6 доступен пока только в виде экспериментальных подключений. Но есть надежда, что через несколько лет он станет таким же обычным протоколом передачи данных, как и IPv4, применяемый в настоящее время.

Сейчас глобальная сеть Интернет и локальные сети оказываются тесно связаны практически, а границы этих сетей можно определить по диапазонам применяемых адресов и протоколов. В какой сети я работаю, когда подключаюсь к сети предприятия, находясь от него на расстоянии около сорока километров, да еще в автомобиле?

Выполнение операций с объектами ОС

Предлагая к рассмотрению примеры, связанные с настройками операционной системы, приходится указывать места нахождения объектов, к которым необходимо обратиться. Пути к объектам часто очень похожи, отличаются

лишь несколькими последними символами. Но строки с записью этих путей выглядят длинными и плохо читаемыми. Поэтому предлагаю ознакомиться с некоторыми условностями, применяемыми в книге. Они помогут сократить длинные и плохо воспринимаемые строки, а также длинные тексты пояснений, касающихся действий над объектами.

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.
3. 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.
4. Выполните **<Имя Команды>** — это значит, что следует нажать кнопку **Пуск**, выбрать команду **Выполнить**, набрать в поле ввода команды **<Имя Команды>** и нажать кнопку **ОК**.
5. 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.
6. 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.

Учитывая, что вы знакомы с компьютером достаточно хорошо, мы не будем рассматривать способы настройки интерфейса операционной системы. Чем дольше вы общаетесь с ПК, тем более индивидуальным становится интерфейс вашей ОС, а кто-то даже отказывается от использования графического интерфейса — современные операционные системы от Microsoft позволяют это сделать.

Ко многим объектам Windows можно добраться с помощью "горячих" клавиш. Этот вариант доступа будет также описан в *разд. "Клавиши Windows" главы 2.*

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

Спасибо Евгению Рыбакову, чья неоценимая поддержка и консультации по вопросам создания книги позволили ей появиться.

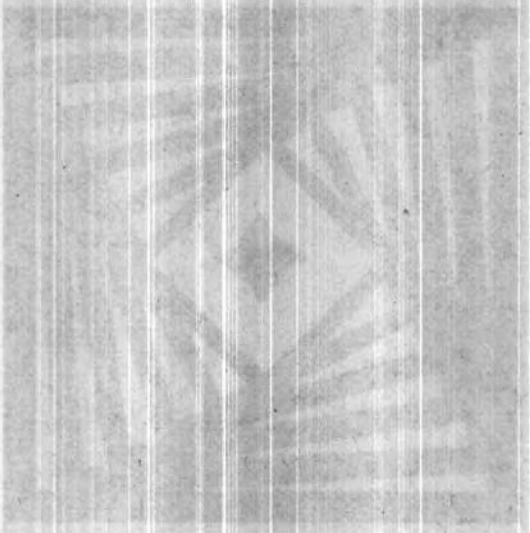
Большое спасибо моей жене и детям, которые относились с пониманием и терпели мое отсутствие дома по выходным дням, пока шла работа над книгой.

Спасибо всем читателям моих книг, которые заинтересовались ими и задавали вопросы, делились своим мнением. Это помогало составить правильное представление о том, какой должна быть эта книга.



ЧАСТЬ I

Как работают компьютерные сети?



Как бы нам ни не хотелось, но с определенной порцией теории нам необходимо познакомиться, прежде чем мы приступим к работе в сети.



Глава 1

Общие принципы работы сети

Прежде чем рассматривать вопрос о работе сетей, следует определиться — о каких сетях будет идти речь. Для этого попытаемся создать небольшой классификатор компьютерных сетей.

Какие бывают сети?

Пожалуй, в вершину классификатора можно поместить два вида сетей — реальные и виртуальные. Если не вникать глубоко в суть работы виртуальной сети, то это сеть, "живущая" в другой сети. Виртуальная сеть не может существовать без какой-либо реальной сети, так же, как реальная сеть не может существовать без физической среды передачи данных.

Вторую ступень классификатора создадим по признаку размера сети. Сети могут быть локальные, региональные и глобальные. Границы между этими категориями бывают довольно расплывчаты. Сеть района или небольшого города по числу узлов и занимаемой территории может оказаться меньше локальной сети крупной организации.

Далее можно разделить сети по возможности постоянного взаимодействия компьютеров между собой. Постоянное взаимодействие компьютеров возможно практически во всех сетях, использующих протокол TCP\IP и имеющих постоянно действующую среду передачи данных. Сети второго вида — это все сети, использующие временное подключение, например, dial-up, и сети, подобные FIDO. В этих сетях возможно подключение одного компьютера к другому в пределах ограниченного времени. Невозможно рассчитывать на передачу файлов или работу с приложением, когда для этого требуется подключение к другому компьютеру в произвольный момент времени. Также к этому виду можно отнести сети, использующие протоколы передачи данных, не позволяющие взаимодействовать произвольному числу

компьютеров между собой. Так, например, если сеть рассчитана только на передачу почтовых сообщений, для получения которых необходимо произвести некоторые действия на принимающей стороне, то оперативное взаимодействие компьютеров в этой сети невозможно.

Мы будем рассматривать сети преимущественно реальные, локальные, с возможностью постоянного взаимодействия компьютеров. Также рассмотрим простой вариант виртуальной сети и возможности взаимодействия сетей.

Сеть в вашей квартире

Не трудно представить себе квартиру, жильцы которой имеют не один компьютер. Учитывая, что техника постоянно совершенствуется, приобретаются новые компьютеры, а старые, оставаясь в рабочем состоянии, переходят к детям. Появляются мобильные компьютеры. Наличие дома двух-трех компьютеров требует передачи информации между ними, подключения каждого из них к Интернету. Появляются устройства, которые позволяют управлять собой с помощью компьютера, медиапроигрыватели, домашние кинотеатры. Есть устройства, которые позволяют просматривать видео- и прослушивать аудиоинформацию прямо из Интернета (HDTV-телевизор Philips Streamium 23PF9976i, например), но это требует их подключения к домашней сети. Постепенно сеть в квартире становится явлением, хотя до сих пор и не совсем обычным, но распространенным. Как и всякая компьютерная сеть, домашняя сеть требует обслуживания. Кто-то должен взять на себя функции администратора этой сети. Несмотря на небольшой размер сети, задачи ее администратора могут оказаться совсем не простыми.

Офисная сеть

В зависимости от размеров офиса и числа сотрудников в нем его сеть может быть очень маленькой и простой, состоящей из двух компьютеров, или весьма внушительной. Как и домашняя сеть, сеть офиса требует обслуживания. Оборудование, работающее в офисной сети, может быть таким же, как и в домашней, но скорее всего там будет больше принтеров, сканеров. В отличие от домашней сети, офисная сеть может потребовать решения вопросов безопасности информации, ограничения прав доступа сотрудников к тем или иным сетевым ресурсам, организации взаимодействия с сетями других офисов. Правда, в последнем случае скорее всего небольшая офисная сеть должна будет влиться в сеть предприятия.

Сеть предприятия

Эта сеть может содержать большое число компьютеров, управление которыми становится делом хлопотным и трудоемким. Такая сеть должна иметь некоторый центр, в котором размещены один или более серверов. Задачи, решаемые данной сетью, обычно связаны с объединением всех ее вычислительных ресурсов с целью решения единой задачи — обеспечение работы предприятия. Кадровая служба и бухгалтерия, специализированные отделы и производственные участки требуют постоянной поддержки в области информационных технологий. В такой ситуации уже невозможно заниматься администрированием сети попутно с другой работой. Часто кроме штатного системного администратора поддержкой работы сети и вычислительной системы занимается целый штат сотрудников отдела информационных технологий.

Сеть в вашем доме или районе

Это еще один вариант достаточно крупной сети, объединяющей обычно компьютеры жильцов (а значит и домашние сети), но, возможно, принимающие под свое крыло и мелкие офисы. Чтобы отличить в дальнейшем такую сеть от домашней, назовем ее домовой. Домовые сети могут быть построены как на добровольной основе, так и на коммерческой. Задачи таких сетей определяются требованиями участников и самих создателей сети. Вполне возможно, что в вашем доме или районе уже есть такая сеть. Но возможно, что вместе с группой единомышленников вы решили самостоятельно ее создать. Такая сеть по размерам (числу компьютеров) может быть похожа на сеть предприятия, а по задачам — на домашнюю сеть. Игры по сети, обмен файлами, общий доступ в Интернет — вот наиболее частые задачи домовой сети.

Глобальные сети

Это очень серьезные сети, часто входящие в Интернет, но не обязательно. В таких сетях начинающих администраторов не бывает. Кто доверит начинающему администрировать сеть министерства обороны, например? Технологии, применяемые в этих сетях, могут весьма отдаленно напоминать технологии сетей из предыдущих разделов. Поэтому в этой книге мы их рассматривать не будем. Но пользоваться услугами глобальной сети Интернет будем. Для этого нам не потребуется разбираться в том, как и с какими операционными системами работают серверы глобальных сетей, как организованы межконтинентальные каналы передачи данных, и в других пробле-

мах глобальных сетей. Но в любом случае, будь то глобальная сеть, или ваша домашняя, состоящая из двух компьютеров, создаются они в соответствии с определенными правилами, а для передачи данных используют специальные среду и протоколы.

Многоуровневая модель сети

Для обеспечения единообразного представления данных при передаче информации по линиям связи была сформирована Международная организация по стандартизации (International Standards Organization, ISO). Эта организация разрабатывает модели международных коммуникационных протоколов, которые описывают международные стандарты систем передачи данных.

ISO предложила базовую модель взаимодействия открытых систем (Open Systems Interconnection, OSI). Эта модель стала международным стандартом проектирования систем передачи данных. Модель содержит семь уровней:

1. Физический — битовые протоколы передачи данных.
2. Канальный — формирование кадров, управление доступом к среде.
3. Сетевой — маршрутизация, управление потоками данных.
4. Транспортный — обеспечение взаимодействия удаленных процессов.
5. Сеансовый — поддержка диалога между удаленными процессами.
6. Представительный — интерпретация передаваемых данных.
7. Прикладной — пользовательское управление данными.

Основная идея модели заключается в том, что каждому уровню отводится конкретная роль. Благодаря этому общая задача передачи данных расчленяется на отдельные, легкообозримые задачи. Необходимые соглашения для связи одного из уровней с высшими и низшими уровнями называются *протоколами*.

Процесс взаимодействия пользователя с сетевой средой заключается в последовательном преобразовании передаваемых данных на передающей стороне от седьмого уровня до первого и в обратном преобразовании на приемной стороне.

- На первом, физическом, уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физическая связь и неразрывная с ней эксплуатационная готовность являются основной функцией 1-го уровня. Стандарты физического уровня включают рекомендации V.24 MKKTT (CCITT), EIA RS232, X.21, ISDN (Integrated Services Digital Network, цифровая сеть связи с комплексными услугами). В качестве среды передачи данных используют

медный кабель (неэкранированная витая пара), коаксиальный кабель, оптоволоконный кабель и радиорелейную линию.

- Канальный уровень преобразует данные, полученные от 1-го уровня, в так называемые кадры и последовательности кадров. На этом уровне осуществляются: управление доступом к передающей среде, используемой несколькими ЭВМ, синхронизация, обнаружение и исправление ошибок.
- Сетевой уровень устанавливает в вычислительной сети связь между двумя абонентами. Соединение происходит благодаря функциям маршрутизации, которые требуют наличия сетевого адреса в пакете. К задачам сетевого уровня также относится обработка ошибок, мультиплексирование, управление потоками данных. Пример стандарта этого уровня — рекомендация X.25 МККТТ (для сетей общего пользования с коммутацией пакетов).
- Транспортный уровень поддерживает непрерывную передачу данных между двумя взаимодействующими друг с другом пользовательскими процессами. Надежность и непрерывность передачи данных возможны благодаря встроенной в протокол системе обнаружения и исправления ошибок, а также аппаратно-независимой реализации сервиса транспортировки.
- Сеансовый уровень обеспечивает управление диалогом, т. е. координирует прием, передачу и поддержку одного сеанса связи. Для координации необходим контроль рабочих параметров, управление потоками данных промежуточных накопителей и диалоговый контроль, гарантирующий передачу имеющихся в распоряжении данных. Кроме того, сеансовый уровень имеет дополнительные функции: управление паролями, подсчет оплаты за использование ресурсов сети, синхронизация и отмена связи в сеансе передачи после сбоя из-за ошибок в низших уровнях.
- Представительный уровень обеспечивает форму представления передаваемых по сети данных, а также их подготовку для пользовательского прикладного уровня. На этом уровне происходит преобразование данных из кадров, используемых для передачи данных, в экранный формат или формат для печатающих устройств оконечной системы.
- На прикладном уровне необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское прикладное программное обеспечение.

Для передачи по коммуникационным линиям информация преобразуется в цепочку следующих друг за другом битов (кодировка с помощью двоичной системы счисления, в которой используются только два знака "0" и "1").

Передаваемые алфавитно-цифровые знаки представляются в виде битовых комбинаций. Битовые комбинации располагаются в определенной кодовой таблице, содержащей 4-, 5-, 6-, 7- или 8-битовые коды.

Количество представленных знаков в коде зависит от количества используемых в нем битов. 4-битовый код позволяет передать максимум 16 значений, 5-битовый код — 32 значения, 6-битовый код — 64 значения, 7-битовый — 128 значений и 8-битовый код — 256 алфавитно-цифровых знаков.

Стандарты

Разные фирмы предлагали различные варианты структуры локальных сетей. Эти варианты отражены в различных стандартах, описывающих правила соединения компьютеров в сеть, типы сетевого оборудования, применяемые кабели, разъемы и прочие тонкости строения сети. Нас будут интересовать преимущественно сети Ethernet — стандарт, широко используемый в России и подходящий для работы с распространенными операционными системами и сетевым оборудованием. После появления экспериментальной сети Ethernet Network фирмы Xerox в 1975 г. этот стандарт неоднократно модернизировался, появилось несколько его модификаций. В настоящее время стандарт Ethernet и его модификации применяются в подавляющем числе компьютерных сетей.

Применение стандарта Ethernet позволяет относительно простыми средствами добиться стабильной работы сети. Рассмотрим эти средства подробнее. Информация в компьютерных сетях обычно передается в двоичном коде — в том виде, в котором ее могут использовать компьютеры. Если несколько компьютеров одновременно передадут какие-то данные в сеть, то, несмотря на наличие адреса, ни один компьютер эту информацию принять не сможет. "Мешанина" из нулей и единиц не будет распознана как осмысленное сообщение с определенным адресом, и информация будет утеряна. Для того чтобы не терять информацию, включенные в сеть компьютеры должны "поделить" среду передачи данных между собой. Возможны различные способы раздела этой среды. По аналогии с радио, можно было бы передавать информацию в виде высокочастотного сигнала с частотной, фазовой или амплитудной модуляцией, разделив применяемый в сети частотный диапазон между компьютерами и используя в качестве адреса узла значение длины волны или частоты несущей этого сигнала. Недостаток такого метода разделения среды передачи данных очевиден. Чтобы в такой сети увидеть все подключенные компьютеры, требуется сканирование по всему частотному диапазону, а передача информации, предназначенной для нескольких или даже всех компьютеров сети, превращается в достаточно сложную задачу. Во всех сетях типа Ethernet применяется более простой метод разделения среды передачи данных — это метод CSMA/CD (Carrier Sense Multiply Access with Collision Detection, множественный доступ с контролем несущей и обнаружением конфликтов).

Примечание

CSMA/CD — метод доступа к среде передачи (кабелю), определенный в спецификации IEEE802.3 для локальных сетей Ethernet. CSMA/CD требует, чтобы каждый узел, начав передачу, продолжал прослушивать сеть на предмет обнаружения попытки одновременной передачи другим устройством — коллизии. При возникновении конфликта передача должна быть незамедлительно прервана и может быть возобновлена по истечении случайного промежутка времени. В сети Ethernet с загрузкой 35—40% коллизии возникают достаточно часто и могут существенно замедлить работу. При небольшом числе станций вероятность коллизий существенно снижается.

Другими словами, этот метод можно назвать так: "Метод коллективного доступа с опознаванием несущей и обнаружением коллизий". Этот метод не требует деления частотного диапазона между компьютерами, что, кроме упрощения всего процесса, повышает быстродействие каналов связи.

Суть метода заключается в следующем: сформированный TCP/IP-пакет информации помещается в отдельный кадр данных, а компьютер ждет момента, когда в сети не будет несущей — физического носителя информации, представляющего собой электромагнитные колебания определенных частот. Компьютер ждет полной тишины. В наступившей тишине он передает свой кадр информации. Другие компьютеры обнаруживают факт передачи и анализируют наличие в передаваемом коде их адреса. Обнаружив свой адрес, компьютер принимает информацию и посылает ответ об удачном завершении передачи кадра. Одновременная передача кадров двумя компьютерами приводит к ситуации, которая называется *коллизией*. Обнаружение коллизии — залог правильной передачи информации. Передающие компьютеры сравнили то, что отправляли, с тем, что оказалось в сети, и при следующем удобном случае опять пошлют этот кадр. И так до получения положительного ответа о приеме кадра. Таким образом, в каждый момент времени "говорить" позволено одному компьютеру. Остальные должны "слушать". Ясно, что к одному кабелю невозможно подключить бесконечно большое число компьютеров. Частоты, на которых передается информация в сетях Ethernet, довольно высоки, достигают десятков и сотен мегагерц. Несмотря на высокие частоты несущей, длительность самого кадра оказывается весьма заметной. Кроме того, после передачи или приема информации каждый компьютер должен выдержать паузу в несколько микросекунд, а после обнаружения коллизии длительность паузы определяется по случайному закону и может принимать значения, достигающие десятков миллисекунд. За единицу времени по сети может передаваться некоторое ограниченное количество информации. Кроме того, по технологии CSMA/CD сигнал о случившейся коллизии компьютер должен получить до окончания передачи своего кадра. Следовательно, длина кабеля в сети тоже ограничена. Как видим, на параметры сети по объективным причинам накладывается целый ряд ограничений. Определенные ограничения накладываются и на тип используемого

кабеля и сетевого оборудования стандартом 10Base-T (802.3L). Этот стандарт предполагает использование витой пары — кабеля, предназначавшегося ранее для передачи голоса. Применение качественного телефонного кабеля для передачи информации в компьютерных сетях оказалось чрезвычайно плодотворным.

В стандарте определены также концентраторы или хабы (hub). Эти устройства предназначены для подключения к одной точке кабеля нескольких компьютеров. Для надежной работы сети количество концентраторов между любыми двумя рабочими станциями не должно быть больше четырех (правило четырех хабов). В результате учета всех ограничений стандарт 10Base-T позволяет создать сеть со следующими параметрами:

- максимальное количество станций в сети — 1024;
- максимальное расстояние между двумя узлами сети (двумя точками подключения станций или концентраторов) — 500 м;
- максимальная длина сегмента — 100 м;
- максимальная пропускная способность сети — 10 Мбит/с или 100 Мбит/с в сетях 10Base-T Fast Ethernet (быстрый Ethernet).

Сети Fast Esernet — это усовершенствованные сети Esernet, для реализации которых применяется современное оборудование, позволяющее работать на скорости 100 Мбит/с. Вместо обычных концентраторов в современных сетях применяются активные коммутаторы. Они позволяют ограничить направления распространения сигнала в сети определенным маршрутом, что существенно снижает число коллизий в сети, позволяя усложнить ее топологию. Применение оптоволоконных линий позволяет еще более увеличить скорость передачи данных по сети. Она может достигать 1 Гбит/с и более.

Разработкой стандартов для компьютерных сетей занимается комитет 882 Института инженеров по электротехнике и радиоэлектронике (The Institute of Electrical and Electronics Engineers, IEEE), основанного еще в 1884 г. Полный перечень основных направлений работы комитета 882 (его подкомитетов) показывает разнообразие существующих на сегодняшний день стандартов, сетевых технологий и самих сетей.

- 802.1 — Internetworking — объединение сетей.
- 802.2 — Logical Link Control, LLC — управление логической передачей данных.
- 802.3 — Ethernet с методом доступа CSMA/CD.
- 802.4 — Token Bus LAN — локальные сети с методом доступа Token Bus.
- 802.5 — Token Ring LAN — локальные сети с методом доступа Token Ring.
- 802.6 — Metropolitan Area Network, MAN — сети мегаполисов.

- 802.7 — Broadband Technical Advisory Group — техническая консультационная группа по широкополосной передаче.
- 802.8 — Fiber Optic Technical Advisory Group — техническая консультационная группа по волоконно-оптическим сетям.
- 802.9 — Integrated Voice and data Networks — интегрированные сети передачи голоса и данных.
- 802.10 — Network Security — сетевая безопасность.
- 802.11 — Wireless Networks — беспроводные сети.
- 802.12 — Demand Priority Access LAN, 100VG-AnyLAN — локальные сети с методом доступа по требованию с приоритетами.

Наименование стандарта складывается из имени подкомитета и символов латинского алфавита. Так, один из современных стандартов работы беспроволочной сети имеет название IEEE 802.11g. Наиболее применяемые стандарты локальных сетей — IEEE 802.3, в числе которых IEEE 802.3 Ethernet, IEEE 802.3u Fast Ethernet и IEEE 802.3ab Gigabit Ethernet. В описании сетевых устройств обычно указывают, какие стандарты этим устройством поддерживаются.

Среда передачи данных

В любой сети информация от одного компьютера до другого передается через некоторую среду передачи данных. Мы будем рассматривать, в основном, кабельные сети, но затронем и беспроводное соединение. В кабельных сетях информация в форме электрического сигнала передается по кабелю. На сегодняшний день для построения сетей применяются три вида кабеля:

- коаксиальный;
- витая пара;
- волоконно-оптический.

Скорость передачи данных по волоконно-оптическому кабелю многократно превышает скорости передачи данных по медным кабелям. От качества и характеристик кабеля во многом зависит качество работы сети. Поэтому не лишним будет ознакомиться с применяемыми кабелями более подробно. Для передачи электрического сигнала требуется, как минимум, два проводника. По сути, и кабель представляет собой два проводника, но конструктивно они выполнены таким образом, что передаваемый по ним сигнал претерпевает меньше искажений, меньше затухает (теряет в мощности), может иметь более широкую полосу частот, чем сигнал, передаваемый по обычным проводам.

Коаксиальный кабель представляет собой гибкий изолированный снаружи цилиндрический проводник, внутри которого строго по его оси расположен второй проводник, а пространство между проводниками заполнено диэлектриком. В настоящее время этот вид кабеля применяется редко, а выпускаемые сетевые адаптеры часто не содержат соответствующих разъемов для его подключения.

Неэкранированная витая пара или кабель UTP (Unshielded Twisted Pair) представляет собой кабель, состоящий из двух или более пар скрученных между собой проводников, покрытых изоляцией и заключенных в общую защитную полимерную "рубашку". Каждый проводник в таком кабеле имеет свою уникальную расцветку и номер. Маркировка кабеля обычно содержит сведения о его категории "CATEGORY 5 UTP". Информация о применении разных категорий медного кабеля приведена в табл. 1.1.

Таблица 1.1. *Применение различных категорий кабеля типа "витая пара"*

Категория	Область применения
1	Используется для телефонных коммуникаций и не подходит для передачи данных в компьютерных сетях
2	Используется для передачи данных со скоростью до 4 Мбит/с включительно
3	Используется для передачи данных со скоростью до 10 Мбит/с включительно. Применяется в сетях
4	Используется для передачи данных со скоростью до 16 Мбит/с включительно. Применяется в сетях Token Ring
5	Используется для передачи данных со скоростью до 100 Мбит/с включительно. Применяется в современных сетях
6 и 7	Используются для передачи данных со скоростью до 1000 Мбит/с включительно. Применяются в современных сетях

Кроме кабельных сетей существуют и сети с невидимой средой передачи — радиосети. Эти сети строятся в соответствии со стандартами 802.11 и применяются достаточно широко в западных странах. Принцип работы этих сетей практически тот же, что и у кабельных сетей Esernet. Точки доступа — устройства, обеспечивающие связь хостов с сетью, могут находиться на расстоянии до 70 км от клиентского компьютера. К сожалению, в нашей стране этот вид сетей используется только на ограниченных площадях, таких как офисы, квартиры, или для связи зданий, между которыми невозможно ор-

ганизовать кабельное или оптическое соединение. Это связано с существующим в настоящее время порядком распределения частот для радиосвязи.

Примечание

Справедливости ради следует сказать, что радиоканал применяется для подключения к Интернету через спутник. Но это не совсем обычная сеть, которая требует однократной настройки, как и другие виды доступа в Интернет. В настоящее время такой вариант подключения к Интернету применяется в удаленных районах, где другой вариант доступа невозможен.

Оптический вариант связи, упомянутый в предыдущем абзаце, использует специальные преобразователи электрических сигналов в оптические, и наоборот. Они позволяют реализовать некоторое подобие оптоволоконного кабеля, но без механических элементов (световода и рубашки кабеля). Этот вид связи подвержен влиянию погодных условий и состояния атмосферы. Применение такой среды передачи в локальных сетях очень ограничено.

В своей практике вы, возможно, столкнетесь с применением различных сред передачи данных. Но основной средой будет кабель "витая пара". В отдельных случаях будет использоваться все более распространяющийся вариант радиоканала — Wireless-сети, предназначенные для исключения кабеля там, где он не удобен.

TCP/IP

Для полной и безошибочной передачи данных между узлами сети необходимо придерживаться определенных правил. Все эти правила оговорены в *протоколе* передачи данных. Протокол передачи данных — это описание способа передачи информации, которого придерживаются разработчики компьютерной техники и программного обеспечения, связанного с передачей данных по сети.

Протокол передачи данных описывает составляющие процесса передачи данных и его свойства.

- Синхронизация — механизм распознавания начала блока данных и его конца.
- Инициализация — установка соединения между взаимодействующими партнерами.
- Блокирование — разбиение передаваемой информации на блоки данных строго определенной максимальной длины (включая опознавательные знаки начала блока и его конца).

- Адресация — идентификация оборудования, которое во время взаимодействия обменивается информацией.
- Обнаружение ошибок — установка битов четности и вычисление контрольных битов.
- Нумерация блоков — присвоение каждому блоку идентификационного номера позволяет выявить ошибочно передаваемую или потерявшуюся информацию.
- Управление потоком данных — процесс распределения и синхронизации информационных потоков. Так, например, если в буфере устройства не хватает места или данные обрабатываются в периферийных устройствах (например, принтерах) недостаточно быстро, то это может привести к накапливанию сообщений и/или запросов без их утери.
- Методы восстановления процесса передачи данных после его прерывания, позволяющие вернуться к определенному положению для повторной передачи информации.
- Разрешение доступа — распределение, контроль и управление ограничениями доступа (например, "только передача" или "только прием").
- Сетевые устройства и среда передачи.

Наиболее употребительными в современных сетях стали протоколы группы TCP/IP. Задуманы эти протоколы для работы в сети Интернет, что отражено и в их названии, но, как оказалось, в локальных сетях они не менее полезны.

TCP/IP-протоколы отвечают за передачу и прием проходящей по сети информации. Протокол TCP — основной транспортный протокол в наборе протоколов Интернета, обеспечивающий надежные, ориентированные на соединения, полнодуплексные потоки. Для доставки данных информация в соответствии с этим протоколом делится на пакеты. Протокол IP эти пакеты нумерует и высылает по заранее определенному цифровому адресу в виде кадра информации — пакета, в который вложен пакет, созданный на основе TCP-протокола. На приемном конце пакеты принимаются, сортируются и собираются в исходном порядке. Рисунок 1.1 иллюстрирует работу IP-протокола.

Даже в самой сложной сети, допускающей передачу информации по наиболее короткому или наименее загруженному в настоящий момент пути, пакеты на приемном конце сортируются согласно последовательности их передачи, тогда как реальная последовательность приема может существенно отличаться от исходной, тем не менее, искажений информации не происходит.

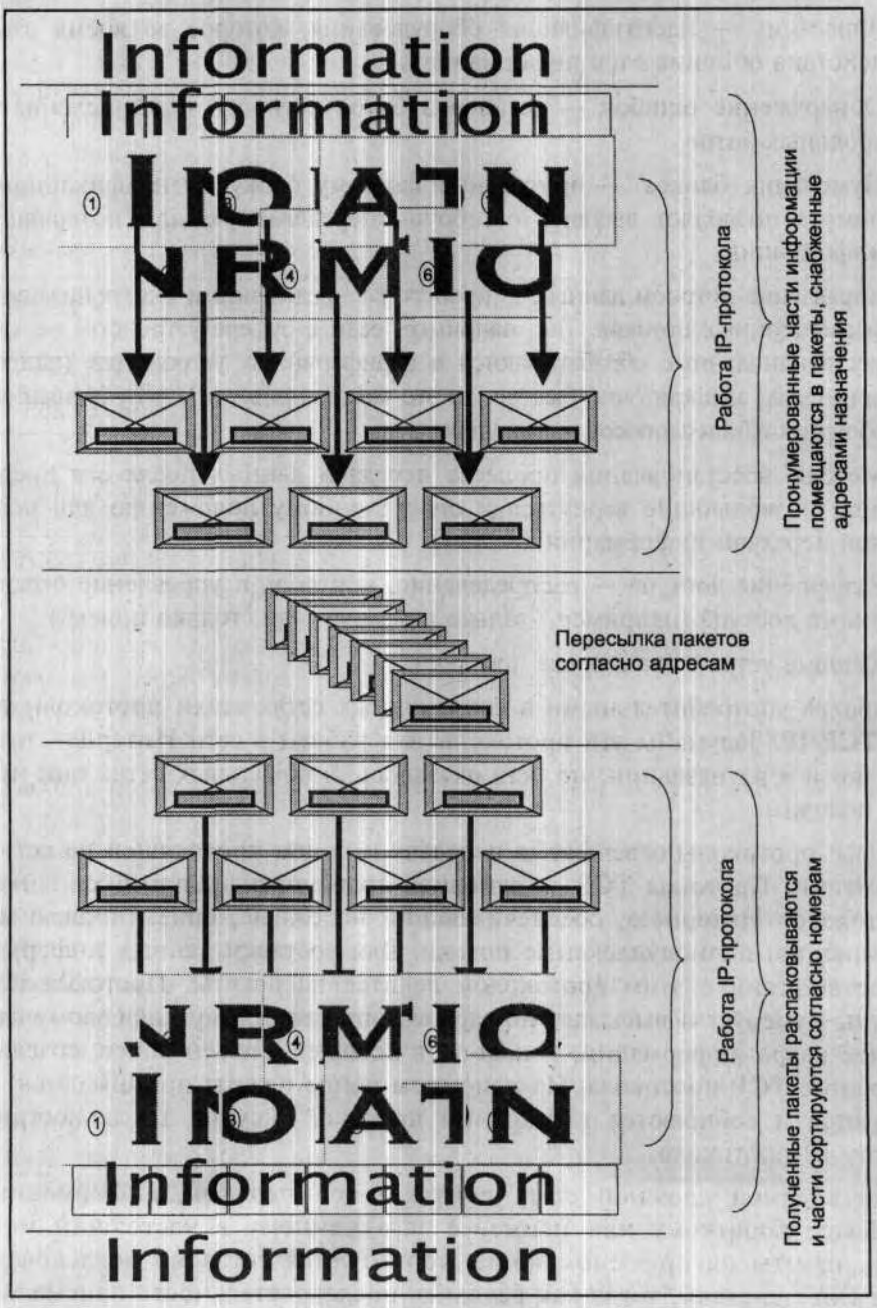


Рис. 1.1. Иллюстрация работы IP-протокола

Цифровой адрес

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 три основных класса. Каждому классу соответствует свой диапазон адресов (табл. 1.2).

Таблица 1.2. *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	С 10.0.0.0 по 10.255.255.255 С 127.0.0.0 по 127.255.255.255
B	255.255.0.0	128.0.0.0 — 191.255.0.0	С 169.254.0.0 по 169.254.255.255.255 С 172.16.0.0 по 172.31.255.255
C	255.255.255.0	192—222	С 192.168.0.0 по 192.168.255.255

Маска подсети указывает на биты, предназначенные для указания адреса сети, в остальных полях адреса должен располагаться адрес компьютера. Каждому классу сети соответствует свой диапазон применяемых и неприменяемых в Интернете (зарезервированных) адресов.

Структура адреса становится более понятной при представлении в двоичном коде. Например, маска 255.255.255.0 в двоичном коде выглядит так: 11111111.11111111.11111111.0. Все поля адреса сети заняты единицами. Адрес 198.168.55.1 в двоичном коде выглядит так: 11000110.10101000.110111.1. По таблице можно определить, что это адрес сети класса "С", а адрес компьютера (узла) выражен младшей единицей. Чем ниже класс сети, тем больше адресов сети может существовать и тем меньше компьютеров может находиться в такой сети. Каждый компьютер в сети имеет свой уникальный адрес, назначенный администратором сети или полученный автоматически. Именно с такими адресами и работает протокол IP.

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

В табл. 1.2 есть поле **Маска подсети**. В этом поле указана очень важная и нужная характеристика адреса. Создавая несколько небольших сетей, вы можете использовать очень похожие адреса, но разбить весь диапазон на

участки. При этом каждой сети (подсети) задать определенную маску, которая ограничит число возможных узлов в этой сети. Предположим, что вам необходимо создать сеть, состоящую из четырех компьютеров, но разбить ее на две подсети, которые связаны друг с другом физически, но логически — это разные сети. Каждая из этих подсетей может иметь свое подключение к Интернету, свои принтеры, и другие сетевые устройства. Решение этой задачи очень простое.

Примем условно, что в сети № 1 должно быть два компьютера, один сетевой принтер (о том, как принтер может работать без компьютера, мы еще поговорим в книге), и подключение к Интернету через некоторое устройство, так же не связанное с компьютером (об этом тоже будет разговор). Всего получилось четыре узла сети. Для возможности маневра в будущем оставим возможность подключения еще восьми компьютеров. Всего четырнадцать узлов. Для сети № 2 решаем оставить возможность подключения всего шести узлов, учитывая, что в настоящий момент в ней будут работать всего два компьютера. Все параметры сети выбираем условно, только для примера.

Выберем один из зарезервированных диапазонов адресов из табл. 1.2. Например, 192.168.0.0—192.168.255.255. Маска, соответствующая этим адресам в таблице, — 255.255.255.0. Это значит, что нам предлагают использовать первые три октета адреса для адреса сети, а последний — для адресов узлов. Поскольку адреса, оканчивающиеся на 000 и 255, для узлов сети использовать нельзя, мы получаем возможность создать сеть, содержащую 254 узла. Но у нас должно быть две сети и всего 20 узлов с учетом развития. А если мы захотим позднее организовать еще несколько подсетей? Для экономии адресного пространства можно воспользоваться другими масками. В данном случае нам могут подойти следующие варианты:

- 255.255.255.240 (11111111.11111111.11111111.11110000) — для сети № 1;
- 255.255.255.248 (11111111.11111111.11111111.11111000) — для сети № 2.

Почему именно такие? А вот почему. Переписав маску в двоичном виде (показано в скобках), мы видим, что для узлов сети № 1 оставлены четыре двоичных разряда. При этом адреса, заканчивающиеся на 0000 и 1111, запрещены.

Примечание

Это общее правило для всех IP-адресов. Начальный и конечный адреса, соответствующие определенной маске (принадлежащие подсети), не могут использоваться для узлов.

Двоичное число 1111 соответствует десятичному числу — 15. Но 1111 использовать нельзя, остается 14 адресов. Для сети № 2 осталось три разряда,

а это значит, что можно использовать шесть адресов (двоичное 111 соответствует десятичному числу 7).

Конечно, в примере число узлов сети подобрано так, чтобы максимально использовать адресное пространство возможных подсетей. На практике выбор определенной маски может дать число узлов, близкое к требуемому, но не равное ему.

Тем не менее, мы получили адреса для двух подсетей, вот диапазоны их адресов:

- сеть № 1 с 192.168.0.1 по 192.168.0.14 при маске 255.255.255.240/28;
- сеть № 2 с 192.168.0.17 по 192.168.0.22 при маске 255.255.255.248/29.

После значения маски я дописал еще одну характеристику адреса — расширение. Это число равно количеству двоичных единиц в двоичном представлении маски. Использовать расширение адреса очень удобно, когда необходимо сделать его запись максимально компактной. Например, для сети № 2 один из адресов узлов можно записать так: 192.168.0.17/29. Без развернутого указания маски мы записали все характеристики этого адреса и подсети, в которую он входит.

В табл. 1.3 показаны все диапазоны адресов с расширениями от 24 до 30. Эти расширения наиболее часто применяются в локальных сетях. В таблице указано также число подсетей, которые могут быть созданы с данным расширением. Расширения менее 24 используются обычно в очень больших и глобальных сетях. Пользуясь таблицей, не забывайте, что начальный и конечный адреса подсети не могут назначаться ее узлам.

Таблица 1.3. *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

Таблица 1.3 *(продолжение)*

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

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

Таблица 1.3 (продолжение)

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
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

Таблица 1.3 *(окончание)*

Маска подсети 255.255.255.252 /30 (11111111.11111111.11111111.11111100)			
64 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
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
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. 1.4 представлены все маски подсети в двоичном и десятичном (побайтовом) представлении и соответствующие расширения. Указано и количество подсетей для каждого расширения.

Таблица 1.4. *Связь между расширением маски подсети, двоичной записью маски и побайтовой записью*

Расширение	Маска подсети в двоичном представлении	Побайтовое представление	Кол-во	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
/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

Таблица 1.4 (окончание)

Расширение	Маска подсети в двоичном представлении	Побайтовое представление	Кол-во	Класс
/24	11111111.11111111.11111111.00000000	255.255.255.0	1	C
/25	11111111.11111111.11111111.10000000	255.255.255.128	128	
/26	11111111.11111111.11111111.11000000	255.255.255.192	64	
/27	11111111.11111111.11111111.11100000	255.255.255.224	32	
/28	11111111.11111111.11111111.11110000	255.255.255.240	16	
/29	11111111.11111111.11111111.11111000	255.255.255.248	8	
/30	11111111.11111111.11111111.11111100	255.255.255.252	4	
/31	11111111.11111111.11111111.11111110	255.255.255.254	2	
/32	11111111.11111111.11111111.11111111	255.255.255.255	1	

Интересно расширение 32. С таким расширением может существовать только одна подсеть, причем в этой подсети может быть только один адрес. Для этого расширения не может быть диапазона адресов. Один адрес соответствует одной подсети. Это единственный случай, когда нет начального и конечного адреса диапазона.

Другие протоколы

Существуют и другие протоколы передачи данных, например, NetBEUI (NetBIOS Enhanced User Interface — протокол расширенного пользовательского интерфейса сетевой базовой системы ввода/вывода). Такое название протокола мы увидим, настраивая компьютер для работы с его использованием. NetBIOS (Network Basic Input/Output System — сетевая базовая система ввода/вывода) — это протокол, дополняющий спецификацию интерфейса NetBIOS, используемую сетевой операционной системой. NetBEUI формализует кадр транспортного уровня, не стандартизованный в NetBIOS. Данный интерфейс не соответствует какому-то конкретному уровню модели OSI. Он охватывает транспортный уровень, сетевой уровень и подуровень LLC (Logical Link Control — управление логическим соединением, верхний подуровень канального уровня). NetBEUI взаимодействует напрямую с NDIS (Network Driver Interface Specification — спецификация стандартного интерфейса сетевых адаптеров) подуровня MAC (Media Access Control — управление доступом к среде передачи, подуровень канального уровня, задающий методы доступа к среде, формат кадров, способ адресации). Это

немаршрутизируемый протокол, что ограничивает его применение в современных сетях. Работает он с обычными буквенно-цифровыми именами и отвечает за сеансы передачи данных между узлами сети, в нашем случае — между компьютерами. Он применяется только в локальных сетях и упрощает работу с сетевыми адресами, позволяя использовать понятные имена компьютеров, которые могут быть связаны с именем пользователя или назначением компьютера в сети. Это существенно облегчает навигацию в сети, поиск необходимого адреса и связь с ним. Но новыми операционными системами этот протокол поддерживается только для совместимости со старыми. А адреса становятся понятными за счет применения других средств, о которых будет разговор в других главах книги.

Вот еще один из широко применяемых сетевых протоколов — UDP (User Datagram Protocol — протокол пользовательских датаграмм). Он предоставляет прикладным процессам транспортные услуги, которые не многим отличаются от услуг, предоставляемых протоколом IP. Протокол UDP обеспечивает ненадежную доставку датаграмм и не поддерживает соединений из конца в конец. Информация, передаваемая по этому протоколу, содержит сведения о том, на какой порт она должна поступить. Для обеспечения целостности данных передается информация о контрольной сумме.

Многие протоколы используют в своей работе другие протоколы. UDP, например, использует IP, а SNMP (Simple Network Management Protocol — простой протокол управления сетью) использует UDP. Протокол TCP используют Telnet, FTP и SMTP.

Вероятно, вам знакомы имена протоколов POP3, SMTP, FTP — все это протоколы передачи данных. Одни работают в почтовых системах, другие в системах обмена файлами.

Возможно, что вам встретится протокол IPX. Точнее это комплект протоколов, который был разработан фирмой Novell для собственной сетевой операционной системы NetWare. Фирма Microsoft добавила поддержку этого протокола в операционную систему Windows. Комплект протоколов IPX состоит из двух частей: собственно протокола IPX (аналог протокола IP в TCP/IP) и SPX (эквивалент протокола TCP в TCP/IP).

Подробное рассмотрение работы каждого протокола может занять достаточно много времени. Если вам интересны подробности о работе какого-либо протокола, обратитесь к сети Интернет. С помощью поисковых систем вы найдете огромное количество информации о любых протоколах, применяемых в сетях. Наша задача состоит в том, чтобы применять эти протоколы, зная их назначение. Часто наименование протокола применяется и при наименовании службы, которая этот протокол использует. Протоколы POP3 и SMTP, например, применяются соответствующими службами на серверах Windows.

Порты

Протоколы передачи данных используют определенные порты для взаимодействия с системой. Иногда это вполне определенные порты, которые рекомендованы для использования с каким-либо протоколом, а иногда порт может выбираться пользователем при настройке программного обеспечения. Термин "порт" является абстрактным понятием, используемым для упрощенного описания механизма установления соединения между компьютерами, он представляет собой потенциальный канал передачи данных. Использование механизма портов существенно облегчает процесс установления соединения и обмена информацией между узлами сети. Всего существует 65 535 портов, начиная с первого. POP3-протокол использует обычно порт 110, FTP — порт 21, HTTP — протокол всемирной паутины (WEB) обычно использует порт 80. Применение того или иного порта обусловлено соглашениями. Понятно, что, принимая почту, не слишком удобно искать порт, на который она может прийти. Но в отдельных случаях можно использовать нестандартные номера портов. Это может быть удобно, когда применяются два сервера одинакового назначения, да еще и с одним IP-адресом. Чтобы их отличить, можно использовать различные номера портов.

Серверы обычно имеют заранее известные номера портов. FTP-протокол передачи файлов получает для своего сервера номер TCP-порта 21. Каждый Telnet-сервер имеет TCP-порт 23, а сервер протокола TFTP (Trivial File Transfer Protocol — простой протокол передачи файлов) — UDP-порт 69. Протоколам TCP/IP обычно назначаются номера портов в диапазоне от 1 до 1023. Назначает номера портов для общеупотребительных протоколов и приложений организация Internet Assigned Numbers Authority (IANA).

Кроме полезных приложений, наличием большого числа портов пользуются и трояны (разновидность вирусов). В Интернете можно найти огромные списки портов, которые подвержены атакам. Один из таких адресов — **http://www.sans.org/resources/idfaq/oddports.php**.

Я думаю, что, взглянув на этот внушительный список, а там более 350 записей, вы уже теперь задумаетесь о защите своей сети путем закрытия лишних, не используемых сетью портов.

Наиболее употребительные порты, используемые протоколом TCP, приведены в табл. 1.5.

Таблица 1.5. *Наиболее распространенные номера портов*

Номер	Сервис	Протокол
20	FTP-data	TCP
21	FTP	TCP

Таблица 1.5 (окончание)

Номер	Сервис	Протокол
23	Telnet	TCP
25	SMTP	TCP
37	Time	TCP
53	DNS	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
119	NNTP	TCP

Имена в сети, как компьютеры узнают друг друга

Для того чтобы компьютеры сети могли находить друг друга в сети, существуют IP-адреса. Но человеку не удобно ими пользоваться. Трудно запомнить десятки адресов, принадлежащих компьютерам вашей сети и серверам в Интернете. Для упрощения работы с адресами применяют символьные имена компьютеров и серверов в Интернете. Часто работа с такими адресами становится похожа на работу с файловой системой. Обычно, задавая путь к файлу, мы пишем что-то похожее на:

<Буква диска>/<Имя папки>/<Имя файла>

Адрес страницы в Интернете может выглядеть так:

<Имя протокола:>//<Имя сервера>.<Имя домена второго уровня>.<Имя домена первого уровня>/<Имя папки на сервере>/<Имя файла страницы>

Адрес компьютера в локальной сети может состоять просто из имени компьютера или быть таким:

<Имя компьютера>.<Имя домена второго уровня>.<Имя домена первого уровня>

В цифровом виде все это выглядело бы иначе. Вместо имен компьютеров и доменов приходилось бы писать IP-адреса. Причем самое неприятное во всем этом то, что адреса могут меняться. Это происходит и в локальной сети, и в Интернете, когда применяются динамические адреса. Система имен в сетях позволяет запоминать адреса и быстро их находить, даже при измен-

чивости IP-адреса. Для того чтобы стало возможно применение символьных имен в сети, применяющей протоколы TCP/IP, были созданы специальные механизмы, разрешающие символьные имена в IP-адреса.

Один из самых простых механизмов разрешения имен имеется на каждом компьютере с операционной системой Windows. Это файл с именем Hosts, который находится по адресу C:\WINDOWS\system32\drivers\etc\Hosts. Примерное содержание этого файла приведено в листинге 1.1. Все строки, начинающиеся с символа решетки, считаются комментариями и не учитываются операционной системой при чтении этого файла. Обычно в файле в виде комментариев приведено краткое описание файла и примеры записей. В листинге приведен перевод имеющихся в файле комментариев и показаны примеры реальных записей.

Листинг 1.1

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Это типовой файл хостов, используемый протоколом Microsoft TCP/IP для
# Windows.
#
#  Этот файл содержит соответствия IP-адресов именам хостов. Каждая
#  запись должна находиться на отдельной строке. IP-адрес размещается
#  в первом столбце, а после него указывается имя хоста.
#  IP-адрес и имя хоста должны быть отделены не менее чем одним
#  пробелом.
#
# Комментарии могут помещаться в строках, каждая из которых
# начинается с символа #, дополнительные комментарии
# могут размещаться в конце строки записи после пробела и символа "#"
#
# Пример:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
#
# Далее показаны реальные записи
# Следующая запись указывает на соответствие адреса
# 127.0.0.1 условному имени локального компьютера
127.0.0.1  localhost  #2004-06-16 13:48:18:966
```

```
#
#
#
81.195.117.138          Server22        # Мой сервер
192.168.55.1            nejan           # Сосед через модем
192.168.119.1           Alexey          # Компьютер Алексея
```

Операционная система перед другими попытками определения имени компьютеров в сети обращается к данному файлу. Поэтому его следует использовать при отсутствии других средств разрешения имен. Имена, приведенные в файле, могут быть придуманы вами и не соответствовать реальным именам компьютеров в сети.

NetBios

В современных операционных системах этот протокол используется поверх TCP/IP-протокола. Но раньше он применялся и самостоятельно. В рамках этого протокола возможна передача от хоста к хосту информации об имени компьютера, которое может содержать сведения и о рабочей группе, к которой принадлежит компьютер. Этот способ разрешения имен используется в одноранговых сетях, где нет никаких серверов, способных выполнить эту работу. Подробно рассматривать технологию разрешения имен по этому протоколу мы не будем. Но в одноранговых сетях он действует, и для нас этого достаточно. Важно знать, что в NetBIOS имена не содержат сведений о доменах. Это символьные имена, которые поддерживаются и современными операционными системами. Учитывая, что имена компьютеров по различным протоколам формируются по-разному, вы можете обнаружить, что имя одного и того же компьютера, определенное разными методами, может быть неоднозначным. Далеко за примером ходить не надо — файл Hosts уже позволил нам создать имена самостоятельно.

WINS и DNS

WINS — это служба Windows Internet Naming Service (преобразование IP-адреса в имена и обратно). Он позволяет использовать протокол NetBIOS в сети, основанной на протоколе TCP/IP.

DNS (Domain Name Services) — служба имен Интернета, применяемая также в системах Microsoft Windows 2000 и Microsoft Windows 2003. Для работы службы выделяются специальные серверы.

И WINS, и DNS выполняют разрешение имен, которое представляет собой процесс преобразования компьютерного имени в IP-адрес. WINS преобра-

зовывает внутренние имена NetBIOS в IP-адреса, а DNS преобразует в IP-адреса интернет-имена. Современные сети используют те же технологии, что и сеть Интернет. Единообразие сетевых технологий — дело полезное. Используя одинаковые протоколы для организации доступа в Интернет и внутри своей сети, мы можем существенно выиграть в простоте обслуживания всей системы. Исключением могут быть очень маленькие сети. Но станут ли исключением ваши сети, решать вам. Даже если вы решили, что непосредственно в данный момент DNS вам не нужна, придет время, когда сеть разрастется, и потребность в DNS возникнет. Более подробно о работе серверов DNS и WINS у нас еще будет повод поговорить.

Оборудование, применяемое в сети

Для того чтобы сеть могла полноценно работать, кроме компьютеров в ней должны быть и некоторые устройства, обеспечивающие ее нормальное функционирование. Конкретный вид и тип оборудования выбирается в процессе организации, расширения или модернизации сети. Отдельные задачи могут решаться как на программном уровне, так и на аппаратном. Например, задача маршрутизации может быть решена как с помощью аппаратного маршрутизатора, так и программно, средствами операционной системы. В самой простой сети, состоящей из двух компьютеров, может вообще не применяться никаких дополнительных устройств. Достаточно того, чтобы в компьютерах были сетевые адаптеры, а для соединения их между собой может быть использован перекрестный кабель "витая пара".

Примечание

Другие типы кабеля мы рассматривать не будем, поскольку подавляющее число малых и средних локальных сетей теперь работают на витой паре.

Если вам еще не известно, что такое перекрестный кабель, сделаем небольшое отступление для объяснения.

Обычный сетевой кабель состоит из четырех закрученных пар проводников. Закручены они для повышения помехозащищенности кабеля и улучшения его характеристик. Для работы сетевого соединения достаточно всего двух пар, остальные остаются не у дел. В табл. 1.6 показано обычное распределение жил кабеля по цветам и номерам контактов на разъемах RJ-45. Такие разъемы применяются для подключения кабеля к сетевым адаптерам и другому сетевому оборудованию. В последнем столбце таблицы указано — используется эта жила кабеля для обычных сетевых подключений или нет.

Таблица 1.6. *Разводка кабеля*

Разъем 1	Цвет провода	Разъем 2	Используется
1	Бело-зеленый	3	ДА
2	Зеленый	6	ДА
3	Бело-оранжевый	1	ДА
4	Синий	4	НЕТ
5	Бело-синий	5	НЕТ
6	Оранжевый	2	ДА
7	Бело-коричневый	7	НЕТ
8	Коричневый	8	НЕТ

Кабель "витая пара" пятой категории. Длина кабеля не должна превышать 100 м, но вам, вероятнее всего, понадобится меньше. Необходимо измерить путь, по которому будет проложен кабель, и добавить к полученной величине еще 3—5 м на случай перемещения компьютеров.

Приобретая кабель, спросите у продавца обжимной инструмент. Коннекторы (вилки) RJ-45 требуют обжатия по каждому контакту, но процедура эта не сложная. Имея в своем распоряжении коннекторы, кабель и обжимной инструмент, вы не будете зависеть от сторонних специалистов, когда необходимо срочно подключить компьютер или сетевое устройство, но нет готового обжатого кабеля.

Итак, кабель обжат. Можно соединять компьютеры. Далее мы будем рассматривать схемы локальных сетей, но вариант сети с соединением перекрестным кабелем отдельно мы не будем рассматривать ввиду его простоты. Все настройки компьютеров, которые справедливы для соединения через коммутатор, будут справедливы и для перекрестного кабеля, за исключением случаев, когда к коммутатору подключено более двух компьютеров.

А пока перечислим более сложное оборудование, которое может быть применено в локальной сети. Если начинать с простейшей сети из двух компьютеров, то первое устройство, которое может быть применено, это модем и/или маршрутизатор для создания подключения к Интернету.

Для этой цели может использоваться несколько типов устройств или их сочетание:

- аналоговый модем;
- DSL-модем;
- DSL-маршрутизатор (router);

- любой из перечисленных модемов и маршрутизатор, обеспечивающий подключение модема;
- вторая сетевая карта в одном из компьютеров, если Интернет подключается выделенным кабелем через более крупную сеть.

Для одноранговой сети из более чем двух компьютеров потребуется коммутатор. Это связано с тем, что перекрестным кабелем можно соединить только два компьютера в сеть. Для подключения к сети большего числа компьютеров необходимо устройство, позволяющее реализовать такое подключение. Раньше в таких случаях применялись самые простые концентраторы. Второе название этих устройств **HAB** (хаб). С появлением более совершенных устройств — коммутаторов — хабы практически вышли из употребления, и остались еще в немодернизированных старых сетях. У коммутаторов тоже есть англоязычное название — **switch**. На первый взгляд эти устройства отличаются незначительно. Но, на самом деле, отличия очень существенны, но не в способе подключения, а в принципе работы. Хаб, получив сигнал на один из своих входов, направляет его сразу на все выходы, возлагая задачу фильтрации лишних (чужих) сигналов на компьютеры сети. Вся сеть в этом случае заполнена сигналами компьютеров. Пакеты, созданные в соответствии с правилами, определенными уже рассмотренными протоколами, бродят по сети, пока их примут получатели. Коммутаторы — устройства более интеллектуальные. Однажды определив маршрут пакета, коммутатор запоминает его и в следующий раз пересылает по этому маршруту, не засоряя ненужной информацией сеть. Если при наличии всего трех компьютеров преимущества еще не очень заметны, то при большем числе машин в сети явно заметно ускорение ее работы.

С укрупнением сети состав оборудования может меняться, но основные его типы будут сохраняться.

Не лишним, вероятно, будет поговорить о вспомогательном оборудовании, которое не участвует напрямую в работе сети, но обеспечивает ее работоспособность в нештатных ситуациях. Компьютеры и другое сетевое оборудование плохо переносят внезапные выключения питающего тока и броски напряжения. Для защиты сети от таких проблем применяют сетевые фильтры и источники бесперебойного питания. Первые защищают устройства от резких перепадов (бросков) напряжения, а вторые могут обеспечить, кроме того, и автономное питание в течение некоторого времени при отключении питающего тока. Применение таких устройств повышает надежность сети и сохраняет ваши нервы и нервы пользователей сети, которую вы администрируете.

Защита сетевого оборудования по питанию

Позволю себе небольшое отступление от основной темы нашего разговора для иллюстрации необходимости применения средств защиты сетевого оборудования по питанию.

Случай 1 (на предприятии)

Это произошло несколько лет назад, когда число компьютеров в нашей сети увеличивалось, а средств для приобретения всего необходимого для их нормальной работы не хватало. Видимо, у организации, которая обеспечивала нас электричеством, тоже не хватало средств. Напряжение в сети стало периодически меняться, а иногда и полностью отключаться. Первые два выключения привели лишь к необходимости проверки дисков после некорректного завершения работы компьютеров. Надо сказать, что сервер сети уже тогда был защищен по питанию источником бесперебойного питания. Но вот на третий раз мы получили "сюрприз". Напряжение отключилось всего на пару секунд. Некоторые компьютеры даже не почувствовали этого, другие выключились. В этот момент ведущий программист нашего отдела отсутствовал на своем месте (было время обеда), а по возвращении, посетовав на нестабильность питания, он попытался включить свой компьютер...

Хорошо, что результаты своей работы он сохранял на сервере и внешних носителях. Осмотр компьютера при вскрытии показал, что сгорело в нем все, что могло сгореть, начиная от блока питания и заканчивая дисководами всех имеющихся в нем видов.

Вы можете себе представить, как рад был программист, и как был рад я, когда через несколько минут поступили сообщения от пользователей сети, повествующие об очень похожих ситуациях. Еще один компьютер оказался полностью выведенным из строя.

Мы сэкономили на сетевых фильтрах, а потеряли два компьютера. В который раз подтверждается поговорка — скупой платит дважды.

Случай 2 (домовая сеть)

Я переехал на новую квартиру. Радость, конечно! Сразу стал рассматривать варианты подключения к Интернету. В нашем городе выбор довольно широкий. Можно dial-up оставить, можно Стрим подключить (вариант ADSL для физических лиц с приемлемой оплатой), а можно к районной сети подключиться. Скорость работы соединения в первом случае известна. Во втором при приемлемой для меня цене скорость 256 Кбит/с и входящий безлимитный трафик, а в третьем обещали 10 Мбит/с при лимите 1500 Мбайт и цене, равной второму варианту. Полтора гигабайта для меня вполне достаточно, и я выбрал третий вариант. Несколько насторожила квалификация

ребят, пришедших проводить кабель в квартиру, но руки у меня есть, что и как сделать, представляю, и через день Интернет пришел в мою квартиру. Дня три все было прекрасно. Но вот наступил выходной день. Судя по скорости закачки файлов, до 10 Мбит в секунду было очень далеко. Ну, это еще можно понять. Сколько пользователей в этот момент перекачивало что-нибудь нужное им, можно было представить. Но ближе к ночи вообще прервалось подключение к Интернету. Служба поддержки работала только в дневное время. Утром я дозвонился до специалистов-сетевиков, и голос в трубке сообщил мне, что был бросок напряжения в нашем доме и мастеру отправлена "эсэмэска" К вечеру подключение восстановилось, но на следующей неделе это повторилось трижды. Потом наступили три праздничных дня, в течение которых, видимо, некому было посылать "эсэмэски". Я уж решил предложить деньги на какой-нибудь бесперебойник, но мне сказали, что разместить его негде. Может быть, у администраторов этой сети действительно трудности с размещением фильтров и источников бесперебойного питания, но мне Интернет нужен был постоянно.

В один из воскресных дней, ожидая очередного восстановления подключения к Интернету через районную сеть, я подключился через dial-up и зарегистрировал заявку на Стрим. Получив номер заявки, пошел в ближайший офис МТУ и приобрел DSL-модем, завершив оформление заявки. Через два дня у меня появилось устойчивое подключение к Интернету, а администраторы районной сети потеряли клиента. Может быть, это для них не имеет существенного значения, но мне всегда казалось, что если кто-то предлагает услугу за деньги, то он рассчитывает на привлечение клиентов, а не на их отпугивание.

Вот так. Два случая из совершенно разных сетей, в которых не продуман был вопрос защиты оборудования по питанию. Я думаю, что к этому вопросу мы больше обращаться не будем. Для администратора сети должно быть аксиомой — установка источников бесперебойного питания или фильтров по питанию необходима для ЛЮБОГО сетевого оборудования. Возможен, конечно, и другой вариант — организовать отдельную чистую систему электроснабжения. Но вы же не станете в квартире держать дизель-генератор в горячем режиме, блок аккумуляторов и преобразователь напряжения. Этот вариант явно не для малых сетей.

Схема компьютерной сети

Если уж мы решили администрировать сеть, заниматься ее усовершенствованием и искать в ней неисправности, следует рассмотреть для начала общую структуру сети и ее варианты, с которыми нам придется столкнуться. Эта га-

лерея схем не претендует на полноту, сеть — дело творческое, и решения могут быть разнообразными. Постепенно вникая в работу своей сети, сравнивая ее с другими известными вариантами, вы начнете чувствовать красоту правильной организации сети. Совсем не обязательно использовать дорогостоящие программные продукты, когда можно найти простое и эффективное решение задачи. В нашей галерее схем представлены несколько основных решений для небольших сетей. Встречающиеся на рисунках IP-адреса приведены только для большей наглядности, и не стоит их воспринимать как рекомендованные. В отдельных случаях, когда IP-адрес должен быть именно таким, как на рисунке, будет соответствующий комментарий. Во всех случаях будем считать, что сеть подключена к Интернету. Современная сеть, даже совсем небольшая, должна иметь выход в глобальную сеть. Если окажется, что в вашем конкретном случае это не требуется, то можно не рассматривать это подключение, как необходимую часть. Сеть будет работать и без выхода в Интернет. Но в какой-то момент вам придется столкнуться с такой необходимостью, и случится это быстрее, чем вы сейчас думаете.

Схема 1 — самая простая

Это самый простой вариант сети (рис. 1.2). Всего два компьютера объединены в сеть. Выход в Интернет обеспечивается одним из компьютеров, который подключен к модему или выделенной линии. Вариантов подключения может быть несколько, и мы их рассмотрим применительно к разным вариантам сети. Для соединения компьютеров можно применить перекрестный кабель, но мы сразу предполагаем расширение сети в будущем. Это условие требует стандартного включения компьютеров в сеть через концентратор или коммутатор. Начиная с этой простейшей схемы, мы будем применять коммутаторы.

Несмотря на простоту, даже эта сеть требует некоторого внимания и первичной настройки. Как и в больших сетях, компьютеры этой сети должны иметь свои IP-адреса. Выбор адреса для компьютера, с которого вы начнете настройку сети, может быть в большой степени произвольным. Но существующих ограничений на применение IP-адресов в локальных сетях лучше придерживаться сразу. Это избавит нас от необходимости делать глобальные изменения в адресной политике, когда сеть вырастет. В очень больших локальных сетях часто используются адреса из зарезервированного диапазона для сетей класса **A** (табл. 1.2), начинающиеся на **10**. Так называемые адреса самонастройки, которые компьютеры себе назначают сами, когда недоступны другие средства назначения адресов, находятся среди зарезервированных адресов в классе **B**. Эти адреса начинаются на **169.254**. В том же классе есть еще один диапазон зарезервированных адресов, который может применяться в локальных сетях. В классе **C** также зарезервирован диапазон адресов для малых локальных сетей. Адреса этого диапазона используются Microsoft при автоматизации некоторых настроек в сети. И, наконец, диапазон заре-

зервированных адресов из класса A, начинающийся на **127**, вообще не применяется в сетях, а используется для внутреннего локального адреса компьютера. По этим адресам можно установить связь компьютера с самим собой.

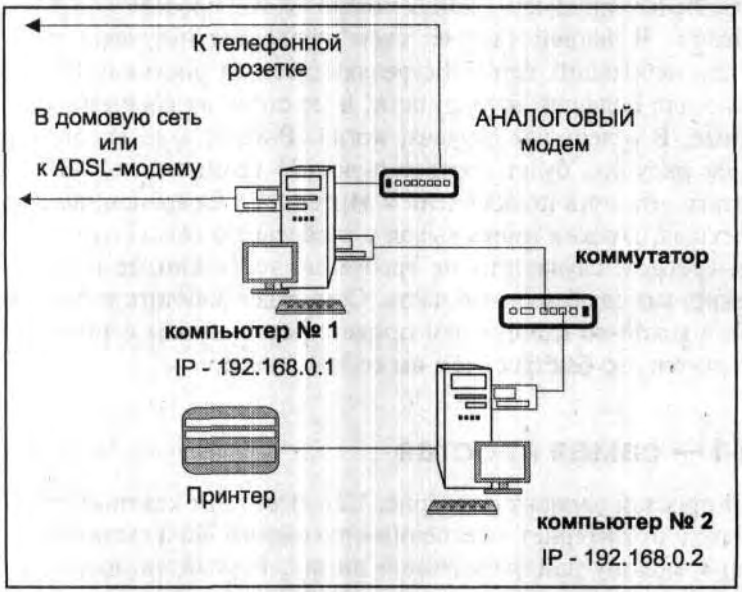


Рис. 1.2. Простейшая сеть из двух компьютеров

Вы вправе выбрать любой из разрешенных в локальных сетях диапазон адресов. Если никогда не предполагается подключать сеть к Интернету, то и другие диапазоны могут быть использованы без особых проблем. Тем не менее, работа в сети должна быть организована по правилам, и мы будем их соблюдать с самого начала.

Одинаковые компьютеры под управлением ОС Windows XP Pro, объединенные в сеть, образуют *одноранговую* сеть. У нас нет сервера, и все компьютеры в такой сети равны. Но тот факт, что один из компьютеров должен обеспечить выход в Интернет, уже нарушает равноправие. Компьютер становится *шлюзом* в Интернет для всей сети. При этом наиболее просто все настройки шлюза выполняются, когда ему присвоен адрес 192.168.0.1. Это один из "особых" адресов в малых локальных сетях, но простота настроек при использовании этого адреса не делает его единственно возможным для шлюза. О различных вариантах настройки мы будем говорить в следующих главах. Кроме компьютеров в нашей сети есть и другие устройства — принтер, модем. Они используются всеми клиентами сети. Значительно удобнее послать на печать подготовленный документ или Web-страницу по сети, чем переписывать ее на дискету и нести на другой компьютер. На рисунке показаны

сразу два подключения к Интернету. Одно посредством обычного аналогового модема, а другое через выделенную линию, или ADSL-модем. Так может быть и на самом деле. Во всяком случае у меня дома именно так и сделано. Всякое может случиться — то профилактические работы у поставщика услуги подключения к Интернету, то забыли оплатить вовремя за эти услуги. Если есть такая возможность, лучше подстраховаться, особенно когда подключение требуется постоянно.

Схема 2 — маршрутизатор

Возможны различные варианты построения сети из двух компьютеров. Посмотрите на рисунок (рис. 1.3).

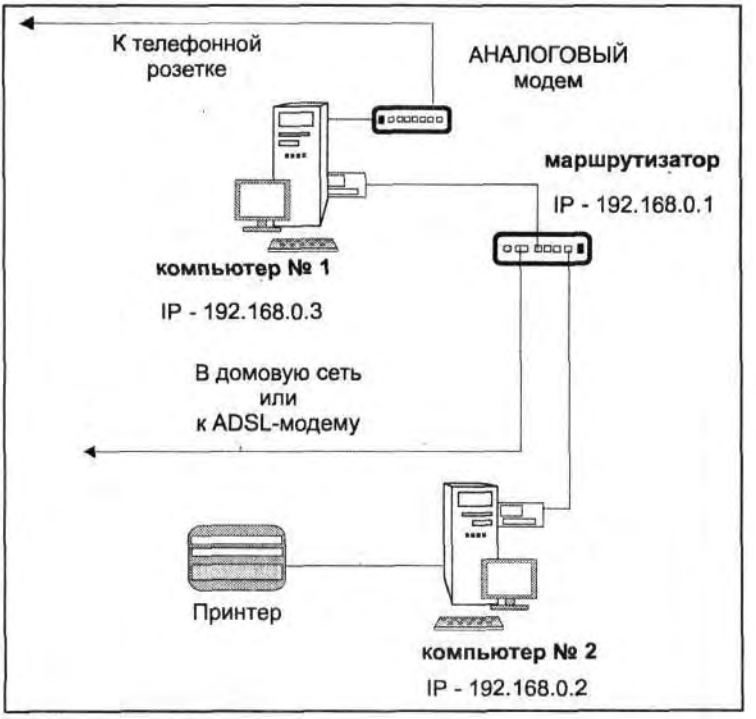


Рис. 1.3. Модифицированная сеть из двух компьютеров

На первый взгляд почти ничего не изменилось, но у компьютера № 1 поменялся IP-адрес, исключен один сетевой адаптер, вместо коммутатора установлен маршрутизатор. Сейчас в продаже появилось достаточно много недорогого сетевого оборудования для домашних и офисных сетей. И этим можно воспользоваться, выбирая наиболее оптимальный вариант своей сети.

Что нам дали такие изменения? Они позволили сделать все компьютеры равноправными. Обязанности по предоставлению общего доступа к Интернету взял на себя маршрутизатор. Теперь он должен иметь "особенный" IP-адрес, но значение его может отличаться от того, которое указано на рисунке. Обычный модем остался подключенным к компьютеру, которому наиболее важно всегда быть на связи.

Схема 3 — добавляем коммутатор

Можно пойти еще дальше. На рис. 1.4 показана схема сети, в которой есть и маршрутизатор, и коммутатор. Зачем? Дело в том, что среди маршрутизаторов есть такие, у которых только один Esernet-порт. Для того чтобы подключить к ним несколько компьютеров, необходим и коммутатор.

Если у коммутатора более четырех разъемов Esernet для подключения компьютеров, например, восемь, то сеть может расширяться до семи компьютеров. Это уже сеть офиса приличных размеров. Большая часть настроек компьютеров при этом будет очень похожа.



Рис. 1.4. Сеть из двух компьютеров с маршрутизатором и коммутатором

Схема 4 — сервер

Компьютерные сети не ограничиваются одноранговыми. Большинство локальных сетей имеют не только рабочие станции, но и серверы.

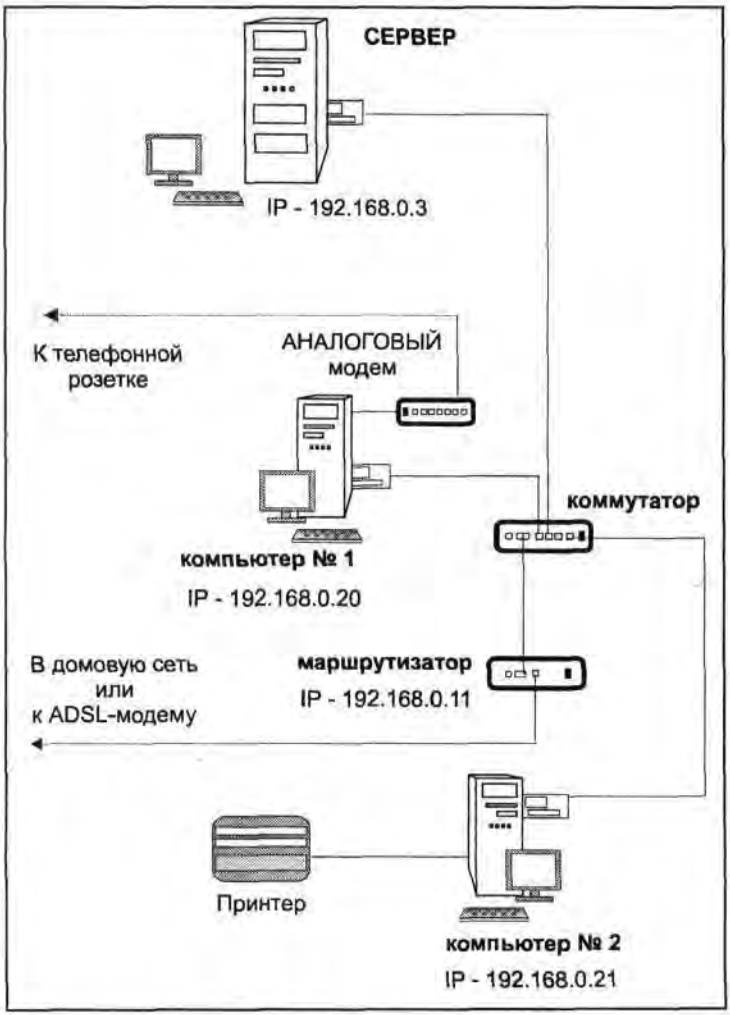


Рис. 1.5. Сеть с сервером

Серверов может быть один, два и более, в зависимости от задач, решаемых в сети. Давайте посмотрим на варианты построения простой сети с сервером (рис. 1.5). Обратите внимание на изменение IP-адресов у компьютеров. Это произошло не случайно. Если сеть имеет сервер и другие сетевые устройст-

ва, которые могут иметь свои IP-адреса, необходимо соблюдать некоторую систему их выделения. Это упростит задачи администрирования сети. Отдельные группы адресов могут быть выделены и группам компьютеров, обладающих какими-либо особенностями. Но обычно все компьютеры небольшой сети имеют адреса из одной, отведенной для этого области. Это вызвано тем, что при настройке автоматического выделения адресов в сети удобнее настраивать предназначенный для этого DHCP-сервер. В данном случае слово сервер применено в отношении программы, а точнее службы, находящейся на сервере-компьютере. Сам сервер-компьютер при этом имеет фиксированный адрес, как и другие серверы, которые могут быть добавлены в сеть позднее. Для всех серверов сети также отведен некоторый диапазон адресов.

Схема 5 — экономим

Возможен и упрощенный вариант подключения сети к Интернету без применения маршрутизатора. Такой вариант показан на рис. 1.6.

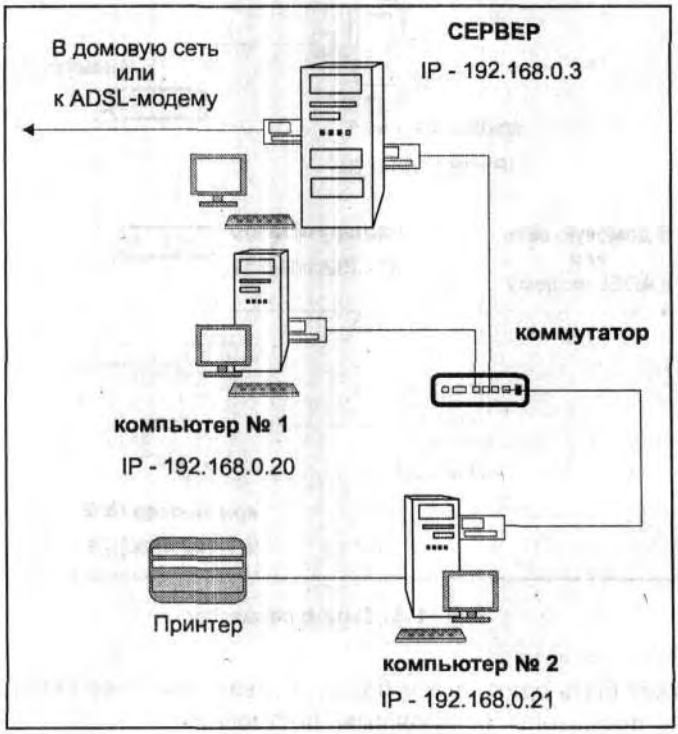


Рис. 1.6. Сеть с сервером, подключенным к Интернету

В данном случае подключение к глобальной сети осуществляется через сервер сети. Но надо сказать, что это не лучшее решение, особенно, когда сервер в сети единственный. Но если этот сервер специально предназначен для работы служб Интернета, то это удобное решение.

Не рекомендуется подключать к глобальной сети серверы, содержащие служебные данные, выполняющие важные расчетные и другие задачи. Всегда есть вероятность проникновения в сеть вирусов или злоумышленников, пытающихся получить доступ к информации на сервере через Интернет. Тем не менее, такие сети существуют и нормально работают, только администраторам этих сетей приходится уделять повышенное внимание мерам защиты своей сети со стороны глобальной сети.

Схема 6 — дружим сетями

Иногда наступает необходимость установить связь между двумя локальными сетями. Причины, которыми вызвана такая необходимость, могут быть разными. Это и доступ к данным удаленных сотрудников, и сетевые игры с соседями по дому, и необходимость передачи информации от автоматизированных систем, и удаленное администрирование нескольких сетей... Да, не удивляйтесь. Начали мы рассмотрение вариантов построения сетей с двух компьютеров, но вполне возможно, что вам придется заняться организацией, пусть даже простых, но нескольких сетей. При этом администрирование этих сетей будет осложнено необходимостью вашего присутствия сразу в двух или более местах. Но это, как вы понимаете, невозможно. Поэтому рассмотрим последний в этой главе пример, иллюстрирующий связь двух удаленных сетей. Таких вариантов, как и вариантов самих сетей, может быть множество. Один из них показан на рис. 1.7. Две локальных сети, имеющих выход в Интернет, соединены защищенным каналом VPN (Virtual Private Network — виртуальная частная сеть). Установлена связь между компьютером администратора, находящимся в сети № 1, и сервером сети № 2. Реально канал связи, конечно, проходит в Интернете, но для пользователей и компьютеров этот канал выглядит так, как будто проложен отдельный кабель. Никакой связи между данным каналом и Интернетом нет. Это значит, что канал защищен со стороны Интернета, а связь через него абсолютно безопасна. Пока нам не важно, как это достигается. В этой главе рассмотрены лишь основные принципы работы и схемы локальных сетей.

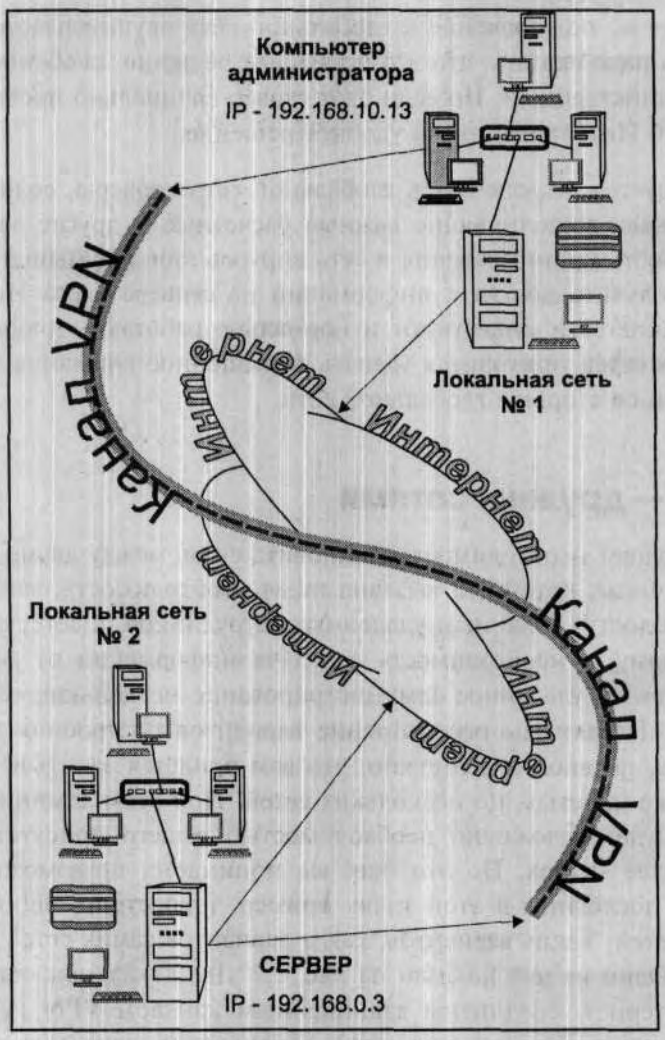


Рис. 1.7. Связь двух сетей через Интернет

Неисправности

Мы только начали рассмотрение вариантов локальных сетей, но уже сейчас следует обратить внимание на возможные неисправности, которые вам встретятся при создании или расширении сети. Часто эти неисправности вызваны не плохо работающим оборудованием, а всего-навсего плохим контактом. Обжимая кабель самостоятельно, будьте внимательны. Современные

сети, работающие на скорости сто и более мегабит в секунду, весьма чувствительны к качеству кабеля, качеству соединений. Отсутствие контакта там, где он нужен, или наличие его там, где его не должно быть, как и в электротехнике и электронике, приводит к дефекту в работе локальной сети.

Иногда проблема возникает не оттого, что что-то не работает или отсутствует контакт, а от неправильного представления администратором возможностей сети. Одна из распространенных ошибок состоит в том, что, имея физическую сеть с исправным оборудованием, администратор желает заставить компьютер работать в двух логических сетях. Мы уже видели, что адрес сети складывается не только из собственно IP-адреса, но и из маски подсети. Если в одной физической сети двум компьютерам назначить адреса, соответствующие одной подсети, а двум другим адреса — соответствующие другой подсети, то они могут видеть друг друга попарно. При этом между этими парами никакой связи не будет. При полностью работоспособном оборудовании и кабельной системе не будет сетевой связи между исправными компьютерами. Они работают в разных подсетях. И что же, спросите вы, неужели нельзя компьютер заставить работать в двух подсетях? Можно. В такой ситуации можно решить вопрос сетевого взаимодействия компьютеров, назначив им не один адрес, а два. Тогда к компьютеру можно будет обращаться по любому из назначенных адресов, он сможет работать в двух подсетях.

Конечно, и оборудование может подвести. Прежде чем устанавливать сетевые адаптеры, коммутаторы и маршрутизаторы на свои рабочие места, следует обязательно испытать их. Лучше обнаружить дефект до начала эксплуатации оборудования в сети. Многопортовые коммутаторы и маршрутизаторы следует проверять по каждому порту. Не стоит надеяться на то, что устройство изготовлено такой-то фирмой и обязательно будет работать. "И на старуху бывает проруха". Чем дольше вы будете работать с сетевым оборудованием, чем чаще проводить его замену (не обязательно только в одной сети), тем быстрее вы убедитесь, что личный контроль работоспособности устройства перед установкой никогда не помешает. Есть в необходимости такого контроля и еще одна положительная сторона. Коммутаторы, маршрутизаторы и другое современное сетевое оборудование изготавливаются разными фирмами. Каждая из них применяет какие-то свои разработки, средства управления оборудованием. В одних случаях есть просто кнопки, в других Web-интерфейс, в третьих — только telnet. Тонкости настройки оборудования лучше осваивать, пока оно работает в тестовом режиме. Это касается и компьютеров, а особенно серверов. Если вы пришли в уже созданную сеть, и сервер был настроен до вас, иногда совсем не просто разобраться в неожиданно возникшей проблеме. Начав "с нуля", вы имеете возможность предварительно опробовать варианты наиболее подходящих настроек, обнаружить моменты ваших заблуждений. Согласитесь, что понять тупиковость выбранного пути настройки сложного оборудования, когда все уже подго-

товлено и сеть ждет завершения этих настроек — не совсем приятная ситуация. Испытав же оборудование на работоспособность, а себя на сообразительность при чтении запутанных рекомендаций по настройке и расшифровке смысла параметров, назначение которых не описано, вы будете уверены, что оно вас не подведет, а вы в состоянии решить любую возникшую проблему, связанную с работой этого оборудования.

Соблюдая принцип предварительного ознакомления со средствами, которые необходимо применить, следует также ознакомиться и с возможностями операционных систем, применяемых в сети. Это относится как к серверным операционным системам, так и к ОС рабочих станций. Операционные системы Windows XP и Windows Server 2003 теперь стали основными сетевыми операционными системами. В большинстве случаев можно настоятельно рекомендовать замену старых ОС новыми. В следующей главе будут рассмотрены возможности современных операционных систем применительно к работе в сети.



Глава 2

Операционные системы

В локальных сетях применяются различные операционные системы. Но в современных сетях с серверами Microsoft Windows Server может полноценно работать только Windows XP. Тем не менее, у пользователей есть компьютеры под управлением Windows 98 и даже Linux различных версий, которые поддерживают не все сетевые технологии Microsoft. В этой главе будут описаны основные возможности и особенности этих операционных систем.

Windows XP

С момента начала широкого применения сетевых технологий на стороне клиентов (пользовательских компьютеров в сети) применялись различные операционные системы. Но на сегодняшний день сложилась ситуация, когда основными ОС стали Windows XP, Windows 2000 и Windows 98. Причем две последние операционные системы встречаются все реже. Windows XP позволяет работать со всеми приложениями, которые функционировали в более старых ОС, но она обладает целым рядом преимуществ по сравнению с ними. Особенно это касается последней ее версии со вторым пакетом обновления (Windows XP Sp2).

- Система стала стабильной. Во всяком случае, если раньше приверженцы Linux гордились стабильностью своей операционной системы и высказывали множество колкостей и острот в отношении Windows, то теперь поводов для такой критики практически не остается. При равном уровне квалификации пользователя обе системы работают стабильно. На собственном опыте могу ответственно заявить, что активная работа моего компьютера вполне возможна без перезагрузки на протяжении нескольких недель.
- Поддержка новых версий сетевых протоколов сделала более гибкими настройки сети, повысила безопасность работы в сети.

- Значительно усовершенствованы средства администрирования системы, что делает работу администратора более удобной.
- Появились развитые средства управления системой посредством командной строки. Отсутствие полноценных средств командной строки в предыдущих версиях Windows также было поводом для саркастических шуток "линуксоидов", в неофициальных разговорах называвших пользователей Windows "виндузятниками". Теперь очень большую часть своей работы администратор Windows может выполнять из командной строки. Да и для обычного пользователя эти средства во многих случаях удобнее графических, позволяют автоматизировать множество часто выполняемых операций. Мне, например, частенько приходится изменять сетевые настройки ноутбука. Чтобы не исправлять все в окнах свойств сетевого подключения, подготовлены несколько часто применяемых командных файлов. Каждый из них устанавливает необходимые параметры подключения перед входом в соответствующую сеть.
- Появилось множество встроенных средств, функции которых ранее были доступны только при использовании программ сторонних производителей. Система стала почти самодостаточной. Для организации ее работы в сети практически не требуется программ, не входящих в состав системы. Показательным примером может быть служба SMTP. Ранее для реализации возможности отправки почтовых сообщений, минуя внешние SMTP-серверы, требовалось применение дополнительных программ. Теперь это возможно средствами самой операционной системы.
- Появились встроенные средства удаленного доступа. Это и telnet, который существует уже в Windows 2000, и удаленный доступ к рабочему столу.
- Усовершенствованная файловая система позволяет надежно разграничивать доступ к данным как для локальных, так и для удаленных пользователей.
- Многие операции, начиная с установки устройств и программ и заканчивая настройками для работы в сети, автоматизированы для стандартных ситуаций, что позволяет выполнять эти настройки даже начинающим администраторам с минимальным риском что-либо испортить.
- Средства восстановления системы теперь позволяют очень быстро возвращать ее в рабочее состояние после возникновения проблем, вызванных установкой несовместимого оборудования, некорректными действиями пользователя, другими неблагоприятными воздействиями.
- Появились весьма удобные и развитые средства защиты системы от несанкционированного доступа из сети как локальной, так и глобальной.

- Для домашних пользователей в системе существует множество средств развлечений.

Можно еще долго перечислять возможности новой операционной системы. Но следует сразу сказать, что Windows XP выпускается в нескольких вариантах, включая 64-разрядные версии. Наиболее распространены Windows XP Professional и Windows XP Home Edition. Это версия для профессионалов и версия для домашних пользователей, их возможности различны. В табл. 2.1 указаны главные особенности и различия этих систем.

Таблица 2.1. *Особенности и различия Windows XP разных версий*

Возможности системы Windows XP Professional	**Windows XP Home Edition**
Новый интерфейс пользователя — поиск необходимых средств становится более простым и быстрым. Надежная платформа — стабильная работа компьютера поддерживается даже в самых сложных условиях. Проигрыватель Windows Media для Windows XP — полнофункциональное средство, обеспечивающее поиск, воспроизведение, упорядочивание и хранение цифрового мультимедиа-материала. Мастер установки сети — помогает легко подключать и совместно использовать компьютеры и устройства, применяемые в домашних условиях. Служба сообщений Windows Messenger — эффективное средство связи и совместной работы, поддерживающее передачу немедленных сообщений, проведение голосовых и видеоконференций, а также совместное использование приложений. Центр справки и поддержки — упрощает решение текущих проблем и помогает своевременно получать необходимую техническую поддержку	+
Обеспечение доступа к корпоративной сети пользователей, находящихся вне офиса	
Эффективные средства поддержки переносных компьютеров (включая технологии ClearType и DualView, а также усовершенствованное управление электропитанием) — находясь в дороге, пользователь может выполнить такой же объем работ, как в офисе	+
Беспроводное подключение — автоматическая беспроводная конфигурация сети с использованием стандарта 802.1*x*	+
Удаленный доступ к компьютеру — можно подключаться в удаленном режиме к ПК, работающему под управлением Windows XP Professional, с любого другого ПК, на котором установлена операционная система Windows. Таким образом, можно работать со всеми приложениями и данными, находясь вне офиса	–

Таблица 2.1 *(продолжение)*

Обеспечение доступа к корпоративной сети пользователей, находящихся вне офиса	
Автономные файлы и папки — доступ к файлам и папкам, хранящимся на общем сетевом диске даже во время отключения компьютера от сервера	–
Быстрый отклик системы и способность одновременно работать над выполнением нескольких задач	
Быстрый запуск и усовершенствованное управление электропитанием — ускоряют загрузку системы и переход из спящего режима в рабочий	+
Многозадачность — несколько приложений могут выполняться одновременно	+
Масштабируемая поддержка процессора — вплоть до поддержки двусторонней многопроцессорной обработки	–
Защита данных и обеспечение конфиденциальности	
Брандмауэр интернет-подключений — автоматически защищает подключенный к Интернету ПК от несанкционированного доступа	+
Поддержка технологии безопасности Internet Explorer 6 — контроль использования личной информации при посещении Web-сайтов	+
Шифрованная файловая система — защита важных данных, содержащихся в файлах, хранящихся на диске, на котором используется файловая система NTFS	–
Управление доступом — запрещение доступа к избранным файлам, приложениям или другим ресурсам	–
Возможность работы с серверами Microsoft Windows Server и системами управления предприятиями	
Централизованное администрирование — подключение систем, работающих под управлением Windows XP Professional, к домену Windows Server открывает доступ к многообразным эффективным средствам управления и обеспечения безопасности	–
Групповая политика — упрощает администрирование групп пользователей и компьютеров	–
Установка и поддержка программного обеспечения — автоматическая установка, настройка, восстановление и удаление приложений	–
Перемещаемые профили пользователей — доступ ко всем своим документам и настройкам независимо от компьютера, используемого для входа в систему	–

Таблица 2.1 (окончание)

Возможность работы с серверами Microsoft Windows Server и системами управления предприятиями	
Служба удаленной установки — поддержка удаленной установки операционной системы на компьютеры, подключенные к сети	–
Отображение текста на разных языках (технология Single Worldwide Binary) — можно вводить текст на любом языке и запускать версию приложений Win32 для любого языка, используя соответствующую версию операционной системы Windows XP	+
Многоязычный пользовательский интерфейс — можно менять язык пользовательского интерфейса, чтобы работать с локализованными диалоговыми окнами, меню, файлами справки, словарями, средствами проверки правописания и т. д.	–

Сразу обращает на себя внимание то, что большинство возможностей, необходимых при работе в сети с сервером отсутствуют в Windows XP Home Edition. Следовательно, для работы в нормальной локальной сети эта операционная система пригодна, но ограниченно. Только самые простые сетевые задачи, которые возникают в одноранговых сетях, и доступ в Интернет доступны для домашней версии операционной системы Windows XP. Поэтому и рассматривать примеры мы будем в основном на базе ОС Windows XP Professional. Она может быть локализована для любого языка. Поэтому при использовании англоязычной версии системы следует установить пакет MUI (Multilingual User Interface — многоязыковый интерфейс пользователя). Кроме MUI есть смысл установить, если еще не установлен, пакет обновления SP2. Это приведет вашу систему в состояние, соответствующее требованиям защиты компьютера при работе в сетях.

Особенности Windows XP Professional

Давайте посмотрим, какими особенностями обладает эта операционная система. Кое-что мы уже знаем из предыдущего описания и табл. 2.1. Теперь познакомимся с интерфейсом операционной системы. Поскольку основной интерфейс графический, и может быть настроен пользователем индивидуально, вид рабочего стола и главного меню могут очень сильно отличаться от машины к машине. Поэтому нам необходимо выяснить такие способы доступа к элементам интерфейса, которые всегда будут неизменны. Это поможет в понимании примеров настройки компьютеров, а также поможет быстро сориентироваться на машине пользователя, как бы он ее не приук-

расил под себя. Да и без приукрашивания интерфейс системы по умолчанию не содержит значков на рабочем столе, к которым многие пользователи привыкли со времен Windows 98. Одна из первых рекомендаций, которую можно встретить после установки операционной системы Windows — начните работу с нажатия кнопки **Пуск**. Результат этого нажатия зависит от настроек меню **Пуск**. Два варианта этого меню, полученные на одном компьютере, приведены на рис. 2.1 и 2.2.

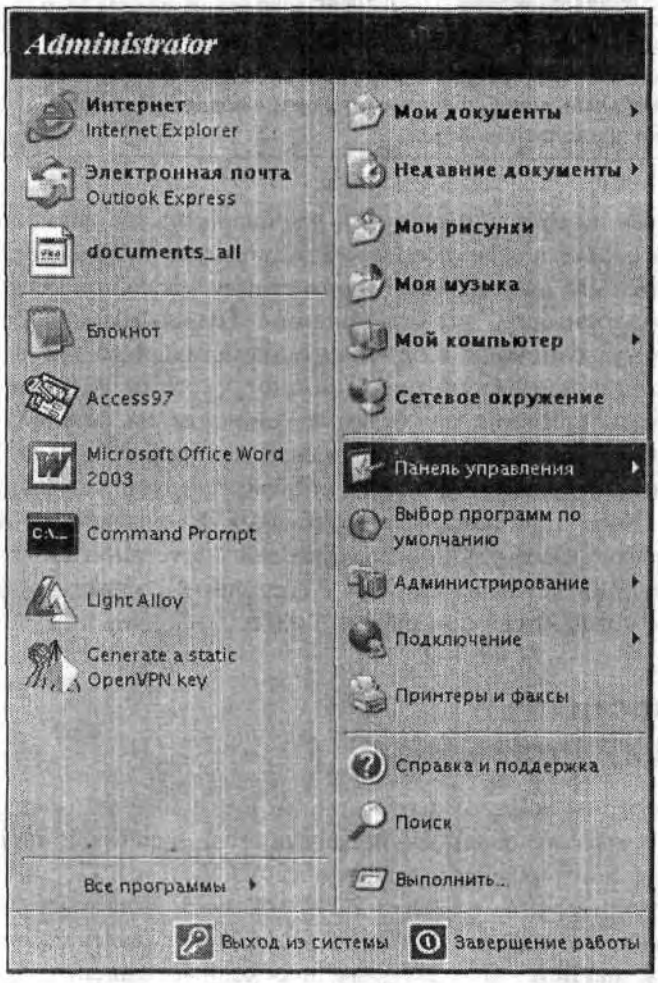


Рис. 2.1. Меню **Пуск** (вариант по умолчанию)

На рис. 2.3 и 2.4 показано окно настройки меню **Пуск** для разных вариантов интерфейса, если у вас в меню отсутствуют необходимые пункты, вы можете поместить их туда, отметив соответствующие флажки в этом окне.

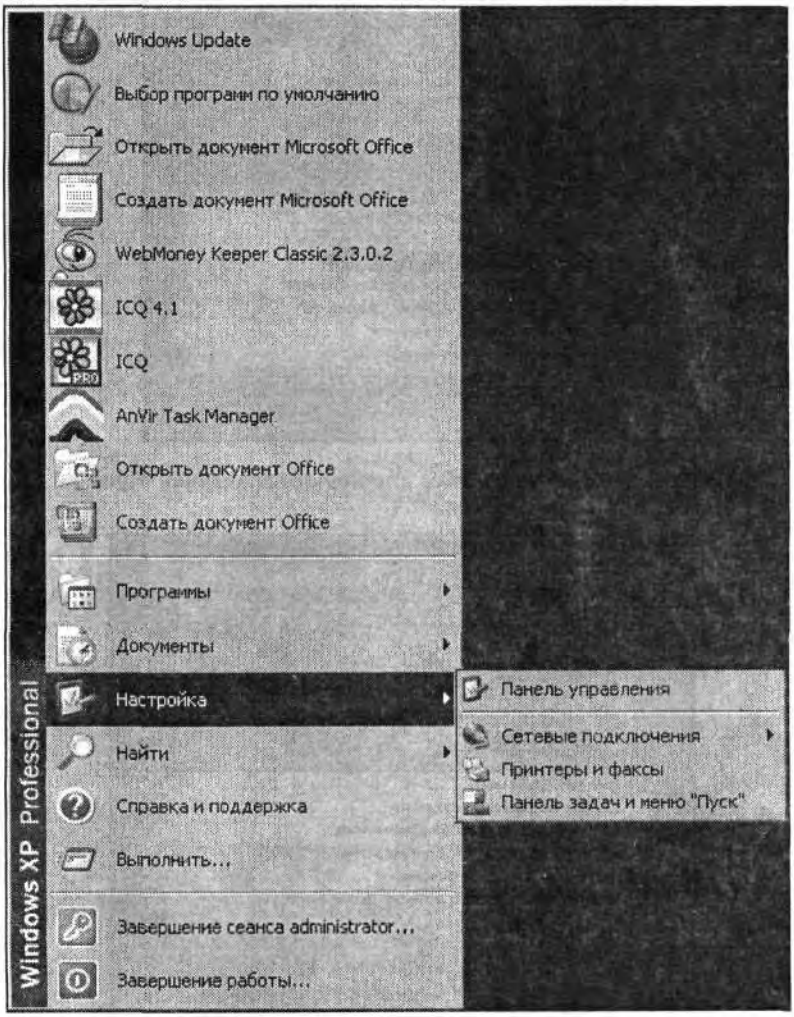


Рис. 2.2. Меню **Пуск**
(вариант "классический")

Как видите, уже на самом первом шаге в системе мы можем видеть перед собой различные интерфейсы.

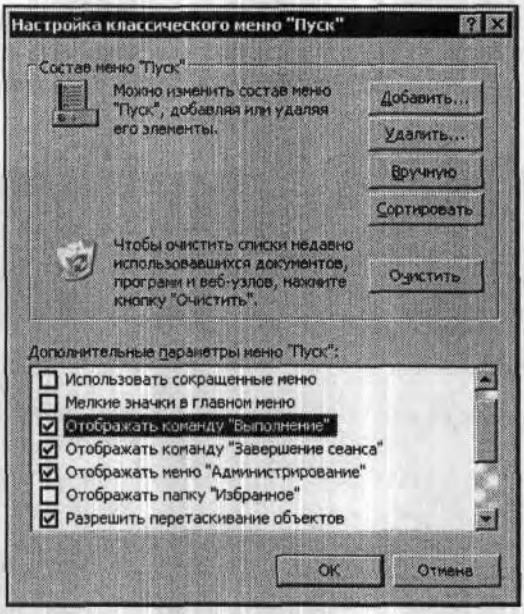


Рис. 2.3. Окно **Настройка классического меню "Пуск"**

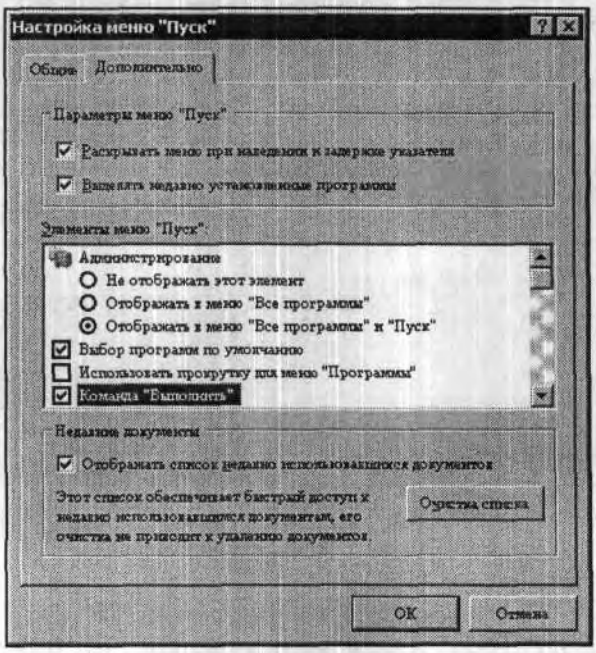


Рис. 2.4. Окно **Настройка меню "Пуск"**

Клавиши Windows

Мы не будем настраивать интерфейс Windows каким-либо определенным образом. Зачем ограничивать свободу самовыражения пользователя этой ОС? Windows XP позволяет обращаться к большинству необходимых нам элементов с помощью клавиатуры. Открыть меню **Пуск** можно, нажав сочетание клавиш <Ctrl>+<Esc> или клавишу <Win>, на которой изображен символ операционных систем Windows. Окно **Запуск программы**, которое вызывается через пункт главного меню **Выполнить**, можно открыть сочетанием клавиш <Win>+<R>. Сочетание <Win>+<Break> откроет окно **Свойства системы**, <Win>+<E> — **Мой компьютер**.

Если сначала нажать <Win>+<R>, а затем ввести в поле открывшегося окна `control` и нажать **ОК** или <Enter>, то откроется **Панель управления**. Если сначала нажать <Win>+<R>, а затем ввести в поле открывшегося окна `cmd` и нажать **ОК** или <Enter>, то откроется **Окно командной строки**. Когда вы открыли множество окон и они не помещаются на экране, можно переключаться между ними с помощью сочетания клавиш <Alt>+<Tab>, нажимая повторно <Tab> и не отпуская <Alt> до выбора необходимого окна.

Примечание

Вы можете самостоятельно изучить горячие клавиши Windows, нажав <Win>+ +<F1>, а затем набрав в поле поиска "клавиши Windows".

Таким образом, мы можем при любой настройке интерфейса быстро получить доступ к необходимым объектам операционной системы. Далее мы не будем заострять внимание на способе доступа к объектам системы (кое-что на эту тему было сказано и во *Введении*). Поэтому на слова, подобные "откройте **Панель управления**" реагируйте, пожалуйста, любым доступным вам способом, кроме эмоциональных возмущенных возгласов — "А как?!"

Панель управления

Теперь проведем экскурсию по **Панели управления**. Это, вероятно, будет наиболее часто посещаемый нами объект системы Windows XP. В нем сосредоточены почти все другие, необходимые нам объекты — апплеты (applet) панели управления, как их еще называют. Слово applet образовано от application — приложение, это небольшое вспомогательное приложение.

Каждый апплет в окне панели управления представлен значком, при открытии которого могут появляться как окна с закладками, так и окна, содержащие другие значки. Рассмотрим апплеты, которые имеют отношение к сетевым настройкам системы.

Откройте **Панель управления**.



Рис. 2.5. Окно **Панель управления**

Внешне это окно напоминает окно обычной папки Windows. Число значков в нем и их наименования могут отличаться на вашем компьютере. Не только Windows помещает туда свои апплеты, но и программы других разработчиков.

Какие же апплеты нас интересуют с точки зрения работы в сети?

- **Система** — позволяет получить доступ к свойствам самого компьютера, его имени, свойствам установленного оборудования, параметрам обновления, параметрам доступа к компьютеру (управления им), многим системным параметрам, связанным с обеспечением стабильной работы компьютера. Дает возможность управления профилями пользователей.
- **Сетевые подключения** — позволяет получить доступ к настройке всех сетевых интерфейсов. Через меню окна этого апплета есть доступ и к сетевому окружению.
- **Телефон и модем** — позволяет настраивать модемные соединения, имеющиеся у этого компьютера.

- **Брандмауэр Windows** — содержит средства настройки брандмауэра, обеспечивающего защиту компьютера со стороны сети. Может достаточно тонко подстраиваться при сложных сетевых настройках. Для отдельных сетевых подключений, к которым есть полное доверие, можно полностью отключать защиту, при сохранении ее на других интерфейсах.
- **Учетные записи пользователей** — понятно, что позволяет управлять учетными записями пользователей. Но пользователи, управление которыми доступно, это только локальные пользователи компьютера. Допустить же пользователя сети к ресурсам компьютера можно. В группы учетных записей локального компьютера могут быть включены сетевые пользователи.
- **Администрирование** — это самый сложный и емкий по своим возможностям апплет. Перечень его компонентов может меняться в зависимости от установленных на вашей машине средств администрирования. Один из компонентов — **Управление компьютером** — позволяет не только управлять своим компьютерам, но и подключаться к другим компьютерам сети, при наличии соответствующих прав, для управления ими. С другими возможностями **Администрирования** мы будем знакомиться по мере необходимости.

Эти апплеты обязательно присутствуют в вашей панели управления. Если на рисунке вы увидели значки, которые отсутствуют в вашей системе, — не расстраивайтесь. Может быть, их у вас и не должно быть. Иногда программы, устанавливаемые на компьютер, добавляют свои апплеты в панель управления.

Серверные возможности ОС Windows XP Professional

Среди особенностей Windows XP Professional есть возможность создания почтового и Web-сервера средствами самой системы. Для этого должны быть установлены соответствующие компоненты. Доступ к администрированию серверов находится по пути **Администрирование | Internet Information Services** (Службы Интернета). Правда, почтовый сервер работает только по SMTP-протоколу. Для создания POP3-сервера требуется дополнительное программное обеспечение.

Раз уж в системе есть возможность создавать серверы, то должна быть и возможность удаленного администрирования серверных служб. И такой способ тоже имеется — **Удаленный доступ к рабочему столу** — встроенный в систему компонент, позволяющий удаленно подключаться к компьютеру и работать так же, как и в локальном варианте, видя перед собой рабочий стол, имея доступ ко всем приложениям и службам, если при входе в систему авторизоваться в качестве администратора. Эта же возможность мо-

жет быть использована и при обычном удаленном доступе к домашнему компьютеру.

Windows XP хорошо справляется с работой нескольких сетевых адаптеров. При необходимости подключения компьютера сразу к двум или даже трем сетям обычно не возникает проблем. Вы можете спросить — а зачем это нужно? А вот зачем: работая в домашней сети, вы можете быть подключены к Интернету индивидуально (не через домашнюю сеть); кроме того, вам может понадобиться доступ к рабочему компьютеру или серверу. Итого — три сети. Во всяком случае, для меня это обычный вариант работы на домашнем компьютере. Три сети — это не роскошь, а вполне обычная рабочая ситуация. Тем более, если компьютер выполняет функции сервера, возможны и другие ситуации, в которых используются несколько сетевых подключений одновременно.

Обеспечение информационной безопасности

В Windows XP Professional есть возможность обеспечить информационную безопасность системы путем редактирования *локальных политик безопасности*, доступ к которым открыт через **Администрирование | Локальные политики безопасности**. Есть возможность применять шаблоны безопасности, уже подготовленные разработчиками, или создавать свои шаблоны для быстрого применения параметров безопасности на машинах сети.

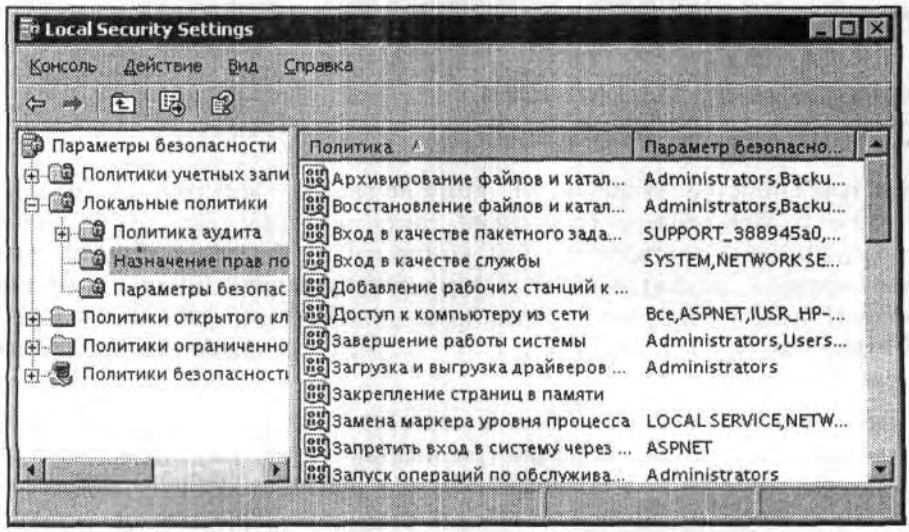


Рис. 2.6. Окно **Local Security Setting**

Для управления политиками безопасности предусмотрен графический интерфейс (рис. 2.6), через который можно редактировать значительное число параметров безопасности, что с одной стороны, может показаться сложным на первый взгляд, но с другой — дает возможность администратору компьютера контролировать проблемы безопасности с открытыми глазами.

Синхронизация системных часов

На этот вопрос обычные домашние пользователи чаще всего не обращают внимания. Что может случиться, если часы вашего компьютера отстают или спешат на несколько минут? Даже если на несколько дней — ничего не случится. Windows XP Professional имеет в своем составе средства синхронизации времени, которые самостоятельно настраиваются в зависимости от варианта работы компьютера. Если компьютер подключен к Интернету, но не включен в сеть с контроллером домена или сервером времени, то в окне **Свойства: Дата и время** появится вкладка **Время Интернета** (рис. 2.7). В других случаях этой вкладки вы не увидите, и время будет синхронизироваться иным путем. Подробно процедуры синхронизации времени в сети еще будут рассматриваться. Если для домашних пользователей это не имеет существенного значения, то для сети отсутствие синхронизации времени на ее компьютерах может привести к плачевным последствиям.

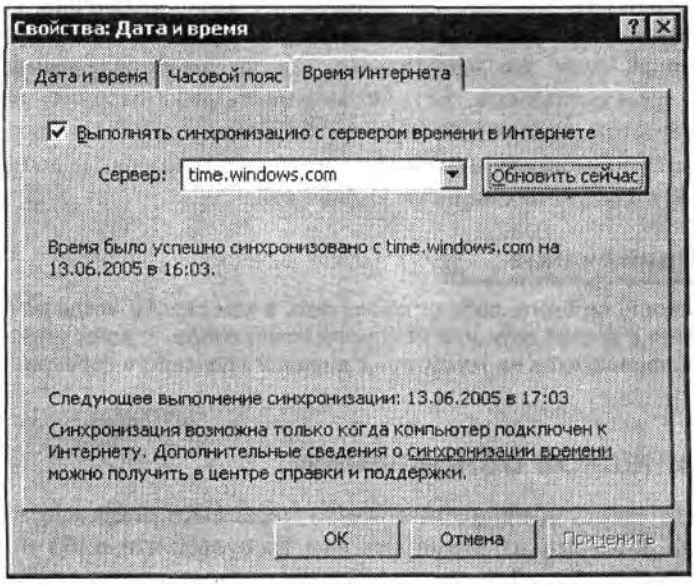


Рис. 2.7. Окно **Свойства: Дата и время**, вкладка **Время Интернета**

Автоматизация разнообразных процедур в сети требует привязки моментов их выполнения к определенному графику, соблюдения определенной их последовательности. Если время на компьютерах сети не синхронизировано, то возможны ситуации, когда выполнение запланированных процедур невозможно, или их выполнение приведет к порче информации.

Межсетевой экран

Это средство имеет несколько названий, самыми известными из которых стали Firewall (огненный вал, передний край) и брандмауэр, что, по сути, похоже, — это стена, предохраняющая от пожара. На самом деле роль межсетевого экрана не имеет отношения к пожарам, но он предназначен для защиты компьютера от внешних атак и проникновений. Если еще несколько лет назад, подключая компьютер к сети Интернет, можно было надеяться на установленные антивирусные средства и не очень беспокоиться о вторжениях извне, то теперь ситуация иная. При подключении к Интернету через высокоскоростной канал без средств защиты от вторжения из сети можно потерять контроль над операционной системой через несколько секунд после соединения. Только физическое отключение от Интернета может спасти компьютер от полного развала системы. Но нам требуется работоспособное и удобное подключение к Интернету, следовательно, нужны средства защиты. И эти средства уже встроены в операционную систему. Доступ к настройкам брандмауэра проходит через **Панель управления | Брандмауэр Windows**. Брандмауэр Windows позволяет настраивать защиту достаточно гибко, разрешая, если это необходимо, доступ по определенным портам и закрывая по всем остальным. Есть возможность даже оградить себя или сеть от любых попыток взаимодействия со стороны определенных IP-адресов. Это позволяет полностью перекрыть значительную часть потока спама и попытки атак с отдельных адресов Интернета.

Примечание

Возможность оградить себя от спама есть в том случае, когда почтовый сервер находится в вашей сети или на вашем компьютере. В иных случаях борьба со спамом переносится на территорию внешнего почтового сервера.

Автоматическое обновление

Учитывая, что средства нападения всегда несколько опережают средства защиты (такова диалектика), периодически требуется что-либо подправлять в системе или добавлять. Для того чтобы изменения производились вовремя, Windows XP содержит средство автоматического обновления системы. Настройка этого средства доступна по пути **Панель управления | Автоматиче-**

ское обновление. Многие домашние пользователи пренебрегают этим средством. Конечно, оно заставляет расходовать трафик при подключении к Интернету. Если настроен полностью автоматический режим обновления, то оно будет происходить почти без участия пользователя. Все же не стоит пренебрегать этим средством. Можно настроить его так, что пользователь будет извещен о наличии обновлений, а решение об их установке можно принять, когда это будет возможно. Состав обновлений также можно уточнять и загружать только самые необходимые компоненты. К самым необходимым можно отнести так называемые *критические обновления*. От них зависит возможность поддержания системы в защищенном состоянии. Рядовой пользователь локальной сети может надеяться и на администратора. В обязанности системного администратора входит поддержание защищенности сети уже на самом пороге с Интернетом. До компьютеров сети не должны добираться атаки из Интернета. Тем не менее, и компьютеры сети следует обновлять, но получать обновления они должны из вашей сети, а не из Интернета. Это позволит сэкономить трафик. Возможность загрузки обновлений без их установки предоставлена корпорацией Microsoft на том же сайте, через который происходят и автоматические обновления.

Если вы до сих пор работали с более старыми операционными системами, то, надеюсь, уже нашли для себя привлекательные стороны новой ОС, несмотря на краткость обзора. На самом деле привлекательных сторон у Windows XP много, и обнаруживаются они уже в процессе работы с системой.

Для тех же, кто уже имеет опыт работы с Windows XP, покажем особенности Windows 98, которая часто встречается в сетях, но все реже у отдельных пользователей. Кое-кто, возможно, даже и не сталкивался с этой системой практически, начав знакомство с Windows уже с версии XP.

Windows 98

Ограниченные возможности этой системы не позволяют считать ее полноценной сетевой операционной системой. Но в организациях, которые имеют давно работающие сети, эта ОС до сих пор широко применяется. Администраторам таких сетей приходится учитывать особенности этой системы, которые связаны, прежде всего, с отсутствием надежных средств защиты и разграничения прав пользователей. Если Windows XP не позволяет войти в систему без авторизации, то Windows 98 можно очень просто обмануть, отменив саму авторизацию. Это заставляло некоторых пользователей устанавливать пароли на уровне BIOS, что тоже не очень хорошо. Стоило забыть такой пароль, и уже никакой администратор не в состоянии был войти в систему. Это вызывало организационные проблемы, но для злоумышленника, который хотел получить доступ к данным, не представляло труда сбросить пароль в BIOS или подключить винчестер на другой машине. Нет в

этой ОС и встроенного межсетевого экрана, других серьезных средств защиты информации. Все же Windows 98 применяется до настоящего времени. Здесь так же, как и в ОС Windows XP, можно использовать управление с клавиатуры, причем сочетания клавиш для всех версий Windows одинаковы.

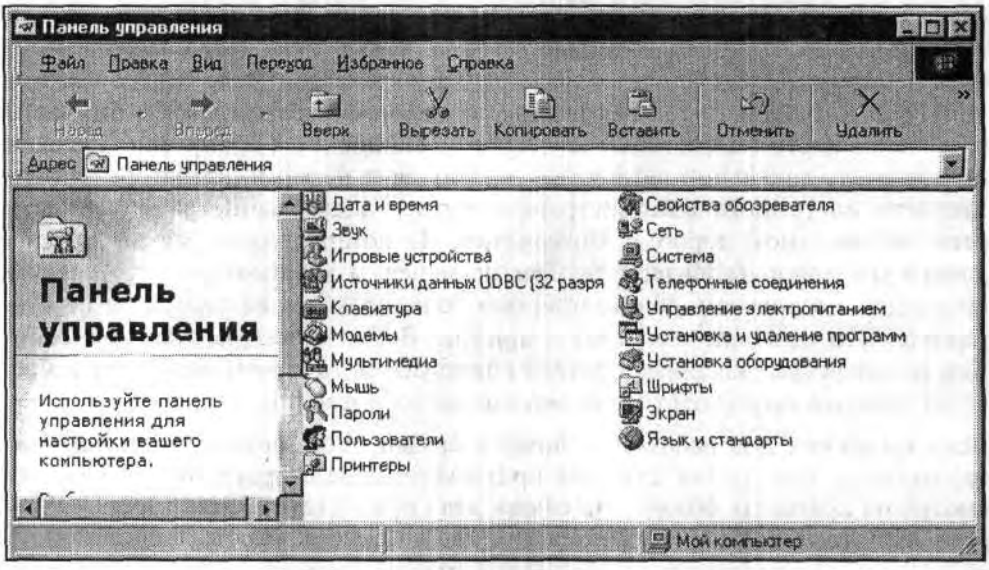


Рис. 2.8. Окно **Панель управления** в Windows 98

Доступ ко всем основным настройкам осуществляется так же, как и в Windows XP, через **Панель управления** (рис. 2.8). Но возможностей здесь существенно меньше, чем в Windows XP.

Файловая система

Windows 98 не может работать с новыми файловыми системами. Если на диске есть раздел NTFS, то эта операционная система его просто не увидит. Основной файловой системой для этой ОС является FAT32. В то время, когда эта файловая система была новой, у нее было много преимуществ перед ее предшественниками FAT12 и FAT16. В большинстве случаев пользователям не приходилось выбирать файловую систему при работе с различными дисковыми накопителями. ОС Windows 98 сама определяла вариант FAT, необходимый для форматирования накопителя определенного объема. Преимуществом FAT перед NTFS можно считать только возможность доступа из DOS. С любой загрузочной дискеты, содержащей MS-DOS, можно прочитать FAT-разделы, а из MS-DOS 7 и более новых версий можно получить доступ к разделам FAT32.

Примечание

Для доступа к файловой системе NTFS тоже существуют загрузочные дискеты различных разработчиков. Но стабильность работы программ на этих дискетах оставляет желать лучшего. Microsoft предлагает только комплекты дискет, позволяющие загрузить саму операционную систему или средство ее восстановления.

Надежность файловой системы, применяемой в Windows 98, не достаточно высока. Это заставляло разработчиков создавать программы восстановления файлов и самой файловой системы, а пользоваться ими приходилось довольно часто. Администраторы обязательно имели под рукой несколько вариантов аварийных дискет.

Тем не менее, при незначительных нагрузках на файловую систему, когда не часто переустанавливаются программы, не очень много информации записывается и стирается ежедневно на диск, Windows 98 может работать месяцами и годами без сбоев. Такой режим работы системы обеспечивается при работе в сети, когда информация хранится в сетевых каталогах, а программы редко заменяются.

Работа в сети

В основном работа в сети для этой ОС не отличается от работы из новых операционных систем. Но доступ к сети, авторизация при выполнении программ, требующих определенных прав пользователя, в Windows 98 выполняются иначе. Если Windows XP позволяет выполнять программы и открывать файлы от имени другого пользователя, то здесь необходимо войти в систему именно с той учетной записью, у которой есть права на выполнение этих операций. В большинстве случаев для рядового пользователя офисной сети это не вызывает проблем или неудобств, но для администратора это неудобно. Защищенность Windows 98 по сравнению с Windows XP не высока. Без применения специальных средств защиты эта операционная система в открытой сети подвержена заражению вирусами и атакам хакеров. Только защищенность самой локальной сети, ответственность пользователей сети и бдительность сетевых администраторов позволяют работать компьютерам с этой операционной системой в современных сетях, имеющих историю, начавшуюся до появления Windows 2000 и Windows XP. Но если есть возможность, лучше переводить компьютеры локальной сети на новые операционные системы. Это связано не только с лучшей их защитой, но и с единообразием их строения. Администрировать сеть с компьютерами, которые позволяют стандартизировать большинство операций по их обслуживанию, проще, и затраты времени на администрирование меньше.

Еще одна область применения Windows 98 — домашние сети. Здесь невозможно заставить пользователя поменять операционную систему на старом

компьютере, который используется совместно с новым, и включен в домашнюю сеть. Но и проблем, связанных со старыми ОС, в таких сетях меньше. Для администратора домовой сети, к которой подключены сети квартир и отдельные компьютеры жильцов, не имеет существенного значения версия ОС на компьютерах пользователей. Пользователям предоставляется некоторый сервис, даны рекомендации по его использованию, а если ваша операционная система не имеет необходимых возможностей, то вам решать, — установить дополнительные программы или заменить операционную систему, чтобы эти возможности были доступны. Например, все чаще доступ к Интернету предлагается через виртуальную частную сеть (Virtual Private Network, VPN). Если Windows XP имеет в своем составе все необходимое для подключения к такой сети, то Windows 98 требует дополнительного программного обеспечения, а некоторые возможности виртуальных сетей вообще недоступны для этой ОС, поскольку программы для работы в таких сетях разрабатывались только для новых операционных систем. К таким программам относится OpenVPN — программа, позволяющая создать удобную и простую виртуальную сеть, полезную для системных администраторов.

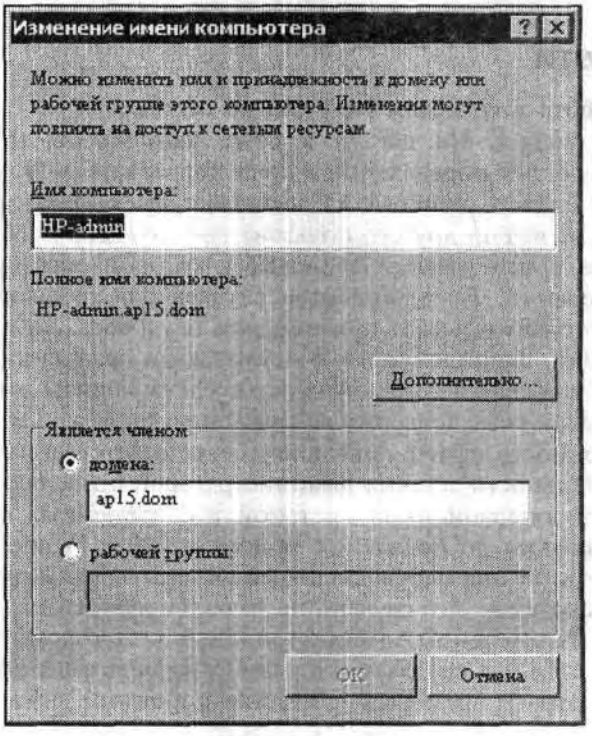


Рис. 2.9. Окно **Изменение имени компьютера** в ОС Windows XP

При регистрации в сети, содержащей домены на основе Active Directory — современной службы каталогов, предложенной Microsoft для сетей на основе Windows, компьютеры под управлением старой ОС вообще не регистрируются.

Если Windows XP позволяет указать принадлежность компьютера к домену и зарегистрировать его в нем, указав соответствующие данные в окне **Изменение имени компьютера** (рис. 2.9), доступного по пути **Панель управления | Система | Имя компьютера | Изменить**, то Windows 98 имеет лишь возможность указания принадлежности к домену, чтобы обеспечить возможность идентификации компьютера в сети сервером имен (DNS). Это делается в окне свойств протокола TCP/IP (рис. 2.10).

Невозможность полноценной регистрации в домене приводит к невозможности указания прав в сети для компьютера. Рабочие станции под управлением Windows XP могут сами иметь определенные права в сети (или определенные запреты). Это позволяет более гибко управлять локальной сетью и делает сеть безопасной. В Windows 98 такие возможности отсутствуют.

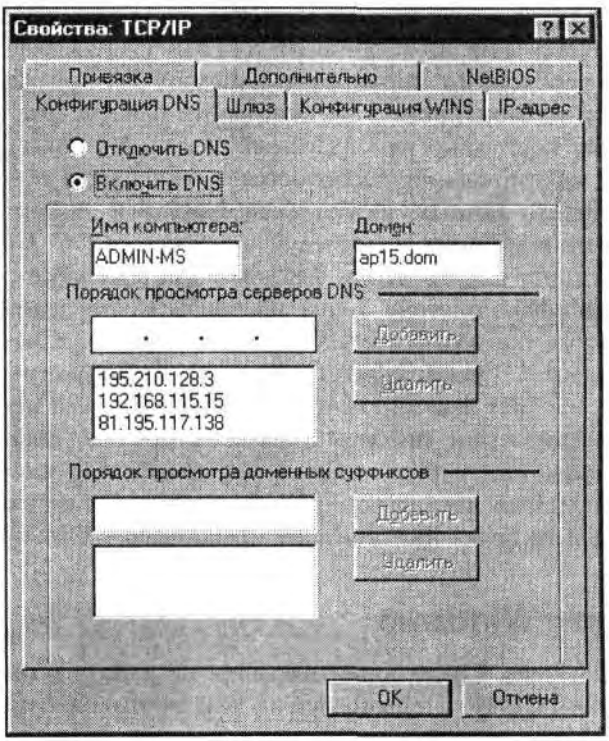


Рис. 2.10. Окно **Свойства: TCP/IP** в ОС Windows 98 (вкладка **Конфигурация DNS**)

Linux

Мала вероятность, что в локальной сети предприятия с Windows-сервером окажутся машины с такой операционной системой. Но в домашних сетях при каких-то экспериментальных работах, возможно, вам придется столкнуться и с Linux. Эта операционная система достаточно популярна у домашних пользователей ввиду своей бесплатности. Одну из современных версий (а их много) этой системы — Fedora — можно приобрести менее, чем за триста рублей. В отличие от ранних, последние версии Linux все более напоминают по интерфейсу Windows. Работа с ними становится понятной не только программистам, но и обычным домашним пользователям. Даже новые компьютеры нередко продаются с предустановленной ОС Linux. Но за внешней схожестью интерфейсов Fedora, например, и Windows XP скрываются очень большие отличия в устройстве самих операционных систем.

Файловая система

Различия между Linux и Windows начинаются на уровне файловой системы. В Linux применяется ext3. В отличие от NTFS и FAT32, разделы этой файловой системы необходимо монтировать каждый раз при запуске операционной системы и размонтировать по окончании работы. Эта операция автоматизирована для постоянно используемых разделов в новых версиях Linux. Коротко смысл монтирования заключается в том, чтобы обеспечить максимальную сохранность данных, целостность файловой системы. При неожиданном выключении питания и последующем запуске ОС Linux автоматически запускает утилиту для проверки файловой системы. Все предполагаемые изменения в файловой системе Linux предварительно записывает в LOG-файл. Только после проверки правильности внесенных изменений запись в LOG-файле стирается. Это позволяет сохранить информацию об исправном состоянии системы при аварийном завершении работы с целью восстановления при возникновении проблем. Такое устройство файловой системы позволяет серверам под управлением Linux работать с высокой надежностью. Но персональный компьютер с ОС Linux в руках не слишком грамотного пользователя не более надежен, чем компьютер с Windows.

Работа в сети Windows

Изначально все версии Linux ориентированы на работу в сетях с применением протоколов TCP/IP. Первоначально эти протоколы применялись для работы в сети Интернет, что определило категорию пользователей, применяющих Linux, — в основном это грамотные пользователи, регулярно посещающие Интернет. Но сети Microsoft Windows тоже стали использовать

TCP/IP. Соответственно, применение ОС Linux возможно и в сетях Microsoft Windows.

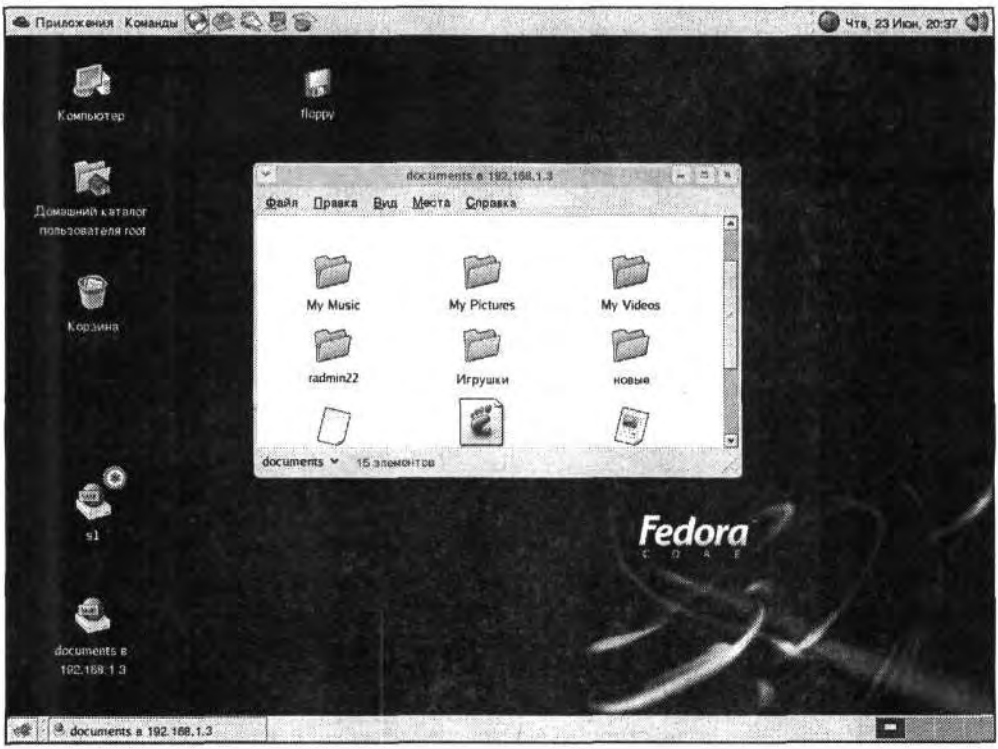


Рис. 2.11. Рабочий стол Linux с открытой сетевой папкой на нем

Но различие в архитектуре операционных систем накладывает определенные ограничения. Мне не удалось, например, получить данные с сайта, на котором использовалась технология получения данных на Web-странице через XML-файлы (Extensible Markup Language — расширенный язык разметки[1]), расположенные на другом сервере. Все доступные мне и моим знакомым компьютеры под Windows нормально видели эти страницы, а доступный мне Linux Fedora наотрез отказался получать данные через XML. Это не говорит об ущербности Linux — это говорит о том, что сеть должна быть однородной, если необходимо выполнять общие сетевые задачи. Вероятно, что задачи, созданные для Linux, не смогут быть решены системой

[1] Подробнее об этом языке можно прочитать по адресу в Интернете **http://www.codenet.ru/webmast/xml/**.

Windows. Система Linux не понимает и доменов Active Directory от Microsoft. Это значит, что с такой рабочей станции невозможно войти в сеть Microsoft Windows под управлением Active Direktory. Но в сети с рабочими группами работать можно вполне. На рис. 2.11 показан вид сетевой папки, расположенной на компьютере с Windows, к которой подключен компьютер с Linux.

Развитые средства для работы в Интернете позволяют подключаться к каталогам компьютеров Windows, как к Web-папкам (рис. 2.12). И такая настройка доступа не вызывает затруднений.

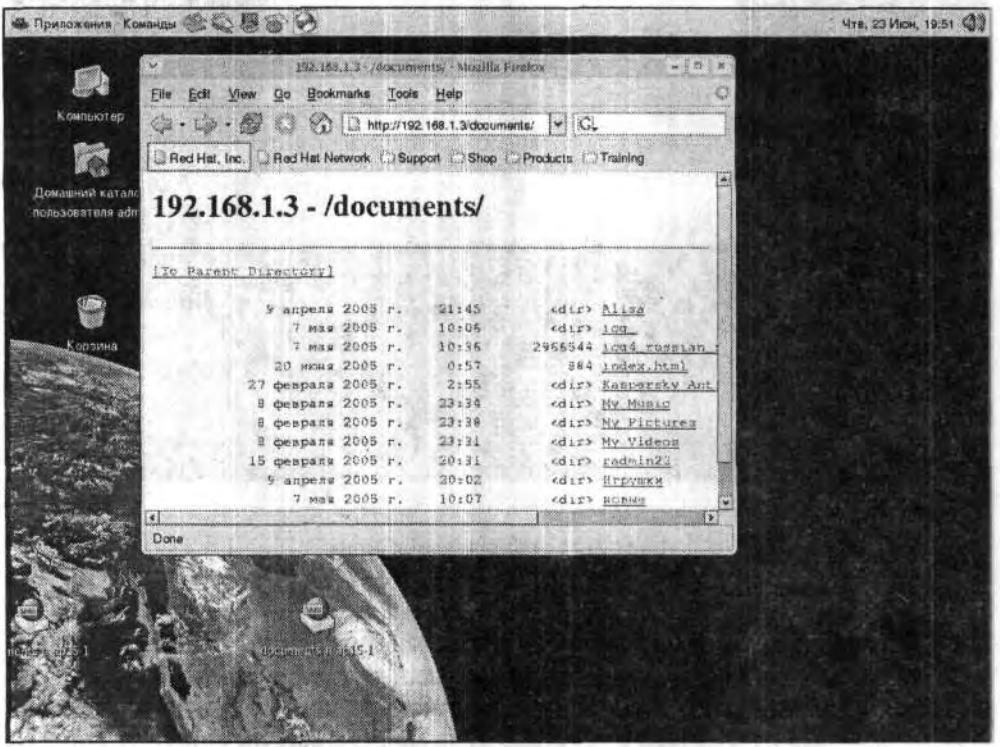


Рис. 2.12. Рабочий стол Linux с сетевой Web-папкой

Для домашней сети, сети квартиры эта операционная система вполне подходит. Обладая развитыми возможностями для работы в Интернете и средствами для работы с документами, она может быть хорошим бесплатным выбором для домашнего офиса. Серьезная же работа в сети с этой операционной системой возможна только при условии, что вся сеть построена на основе Linux и UNIX.

Кроме того, полноценное администрирование этой операционной системы невозможно без использования консоли (командной строки). Именно из командной строки доступно большинство ее настроек, включая сетевые. Знатоки Linux говорят, что для досконального освоения этой системы нужны годы. Что, в общем-то, можно сказать и о Windows, учитывая разнообразие версий и вариантов применения.

В книге более не будет упоминаний об этой операционной системе. Здесь приведено это небольшое описание только для того, чтобы познакомить читателей с ее возможностями при работе в сети Windows. Надеюсь, что этот обзор снимет хотя бы некоторые вопросы относительно данной операционной системы. Часто, ориентируясь на слухи, начинающие администраторы локальных сетей считают, что Linux намного совершеннее Windows, существенно стабильнее, и к тому же бесплатна, и почти не подвержена действию вирусов. Такие утверждения могут быть справедливы, но только при условии, что администраторы Linux-систем люди опытные. Сети под Linux это отдельная область человеческой деятельности и знаний. Но "нельзя объять необъятное". Мы же будем заниматься сетью под Windows. Поэтому рассмотрим одну из важнейших на сегодняшний день ОС Windows Server 2003.

Windows Server 2003

Эта операционная система вобрала в себя все лучшее, что было создано для Windows к 2003 году. Она похожа по структуре на Windows 2000 Server, но содержит множество новых возможностей, а по интерфейсу близка к Windows XP.

Поскольку это серверная операционная система, в ней по умолчанию настроен режим максимальной безопасности. Это позволяет надеяться на то, что в процессе первоначальной настройки сети не произойдет существенных неприятностей, связанных с настройками безопасности. Тем не менее, по собственному опыту могу сказать, что перед подключением к Интернету компьютера с этой операционной системой следует обязательно настроить брандмауэр и другие средства безопасности, связанные с доступом к компьютеру из Интернета. Эти настройки невозможны по умолчанию ввиду разнообразия вариантов подключения компьютеров к Интернету и задач обеспечения доступа к нему из глобальной сети. Во всяком случае, подключая такой компьютер к Интернету, ни в коем случае не включайте его в сеть в момент подключения. В наше время это относится не только к Windows Server 2003. Число и активность вирусов, изощренность методов сетевых атак достигли такого уровня, что компьютер, подключенный без средств защиты к Интернету, практически сразу сам становится переносчиком электронной заразы, становится опасным для сети, в которую он включен.

Файловая система

NTFS 5.0 — файловая система Windows Server 2003. Она имеет надстройку EFS (Encrypting File System — шифрующая файловая система), которая позволяет скрыть файлы пользователя от несанкционированного доступа шифрованием, которое прозрачно для владельца этих файлов.

Поддерживается работа с динамическими дисками, которые позволяют объединять несколько физических дисков в один том, и при этом отказоустойчивость системы значительно повышается[2].

Поддерживается работа с распределенной файловой системой (Distributed File System, DFS). При этом файлы и каталоги реально могут находиться в любом месте сети, но для пользователя они организованы в виртуальную структуру каталогов.

В то же время есть возможность работы и с самыми обычными дисками, и с традиционными файловыми системами. При этом можно объединять диски в массивы, позволяющие значительно повысить надежность файловой системы за счет резервирования и дублирования информации на дисках.

Возможности системы

Windows Server 2003 разработана и предназначена для работы именно на сервере компьютерной сети. Поэтому предусмотрена возможность работы с большим объемом оперативной памяти и на многопроцессорных компьютерах.

Windows Server 2003 позволяет организовать сети различных уровней сложности, начиная от сети с обычной рабочей группой до сложной сети из нескольких доменов, объединенных в лес.

Небольшая локальная сеть обычно не требует создания нескольких доменов. Но и для малой сети возможности Windows Server 2003 позволяют организовать ее надежное администрирование.

Система имеет несколько средств удаленного администрирования. Это и зарекомендовавший себя в компьютерных сетях Telnet, и средства удаленного управления посредством консоли управления, средства терминального доступа (которые по аналогии со средством в Windows XP называются *удаленным доступом к рабочему столу*), а также Web-интерфейс для управления сервером через Интернет или по локальной сети.

---

[2] Подробности о динамических дисках по адресу в Интернете **http://mdforum.dynu.com/article638.html**.

Собственно сервер терминалов, который может быть развернут на базе Windows Server 2003, позволяет в сети применять рабочие станции в качестве терминалов, на которых не устанавливаются программы, необходимые для работы пользователей, а используются ресурсы сервера в виде нескольких сеансов удаленных подключений. Такой вариант использования Windows Server 2003 требует приобретения дополнительных лицензий для пользователей терминального доступа.

Система может выступать и в роли сервера сертификации. До настоящего времени этот вариант организации доверительных отношений и авторизации в сетях еще не очень широко распространен. Но его можно с успехом применять в различных ситуациях, когда использование обычного пароля недостаточно.

Единый каталог ресурсов сети — Active Directory — позволяет создать доступную всем пользователям сети базу данных ее ресурсов. Причем доступ к этим ресурсам может быть строго разграничен в соответствии с правами учетных записей пользователей и компьютеров.

Встроенные средства маршрутизации и удаленного доступа позволяют организовать безопасное взаимодействие сетей, в том числе и безопасное подключение к Интернету. При этом применяется сетевое преобразование адресов (Network Address Translation, NAT), что позволяет при наличии одного-единственного выделенного организации или малой сети IP-адреса предоставить возможность работы в Интернете всем пользователям сети.

В системе встроены серверы SMTP, POP3, Web. Это значит, что можно снабдить каждого пользователя сети персональным почтовым ящиком, а саму организацию или сеть обеспечить собственным сайтом или страницей в Интернете. Свою страницу при желании может иметь каждый пользователь сети.

Возможно применение Windows Server 2003 и как Web-сервера с предоставлением пользователям доступа к данным и документам, хранящимся на сервере.

Стабильность работы системы такова, что она может работать месяцами без перезагрузки. Остановка системы иногда все же требуется, но для проведения профилактических работ на компьютере, который исполняет роль сервера.

Аналогично Windows XP, Windows Server 2003 имеет службу автоматического обновления. Но здесь следует соблюдать осторожность и меру. Если сервер работает круглосуточно, то недопустимо бесконтрольное автоматическое выполнение обновлений. Эти процедуры лучше проводить вручную, тем более, что иногда после обновлений требуется перезагрузка.

Возможности применения на персональном компьютере

Возможности Windows Server 2003 так широки, что некоторые пользователи пытаются применять эту систему в качестве персональной. Интерфейс подобен Windows XP, возможности намного шире, чем у Windows XP. На самом деле для персональной системы эти возможности чаще всего излишни. Но если они вам необходимы, то можно использовать Windows Server 2003 на рабочей станции. Правда, придется, во-первых, смириться с ценой этой ОС, а во-вторых, с ее средствами защиты. Для установки некоторых приложений придется покопаться в локальных политиках, чтобы снять мешающие ограничения. Но, насколько мне известно, есть случаи применения этой ОС даже на ноутбуках.

Если вы решились на установку Windows Server 2003 на вашу рабочую станцию, то последуйте рекомендациям, приведенным далее. Они помогут привести систему в необходимое вам состояние, и вы получите очень стабильную, обладающую невероятно широкими возможностями рабочую систему.

Настройка Windows Server 2003 для рабочей станции

Прежде всего, можно отключить окно **Управление данным сервером** (рис. 2.13), которое открывается каждый раз при запуске системы. Для этого надо отметить флажок **Не показывать эту страницу при входе в систему** (Don't display this page at logon). Вообще говоря, для начинающего администратора это окно может быть полезно. Но на рабочей станции оно может раздражать, да и администратор может запустить эту программу иначе — **Администрирование | Управление данным сервером**.

Известно, что работа под учетной записью администратора компьютера или сервера в общем случае не рекомендуется. Поэтому и на рабочей станции под управлением Windows Server 2003 должна проходить под обычной учетной записью рядового пользователя. Такую учетную запись (а лучше не одну) необходимо создать. Это можно сделать через диалоговое окно **Локальные пользователи и группы** (Local Users and Groups) (рис. 2.14).

Данное окно можно вызвать через меню **Пуск | Выполнить | lusrmgr.msc**.

Созданным учетным записям следует назначить права, соответствующие задачам этих учетных записей.

При каждой перезагрузке или выключении сервер требует, чтобы указали причину этого события. На сервере сети это полезно. Но мы готовим рабочую станцию. Здесь придется обратиться к **Редактору групповых политик**

(Group Policy Object Editor). Окно этого редактора (рис. 2.15) можно вызвать через **Пуск | Выполнить | gpedit.msc**.

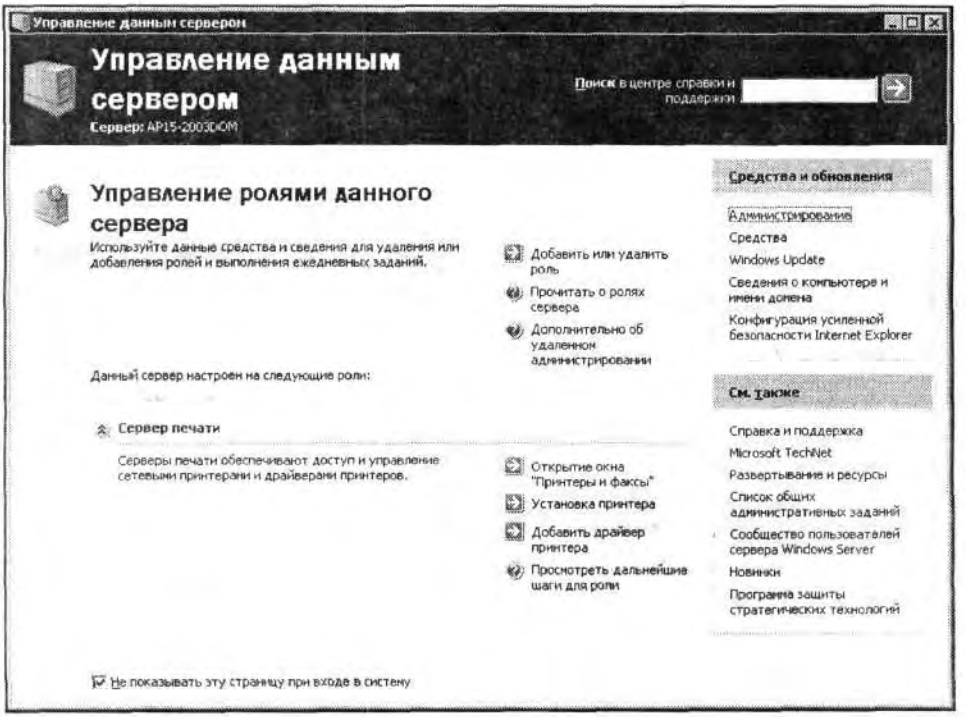


Рис. 2.13. Окно **Управление данным сервером** (Manage Your Server)

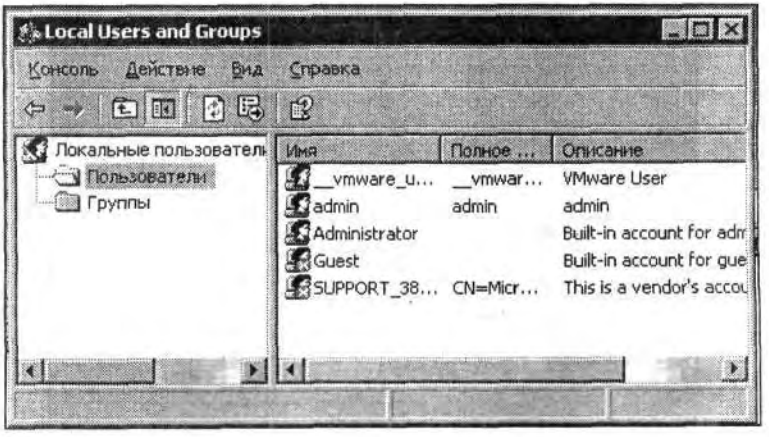


Рис. 2.14. Окно **Local Users and Groups**

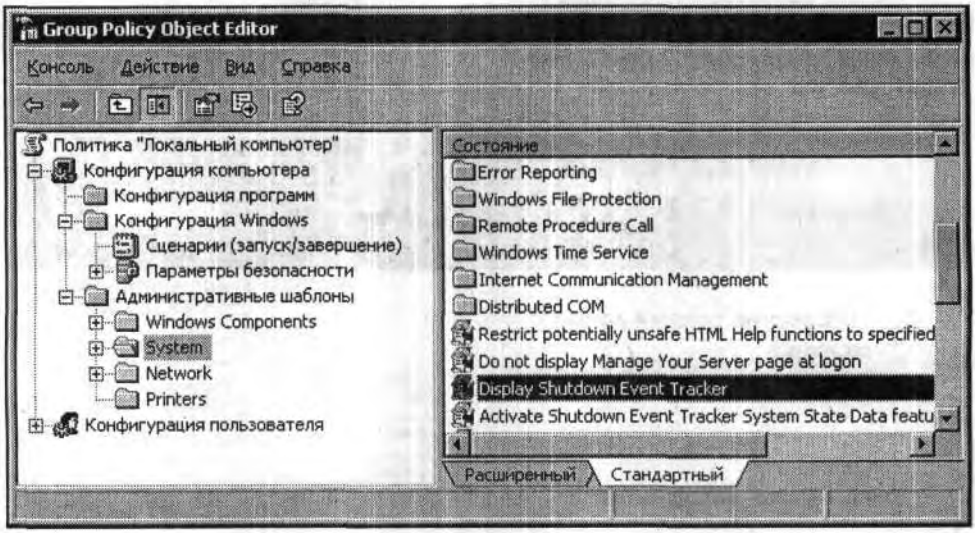


Рис. 2.15. Окно **Group Policy Object Editor**

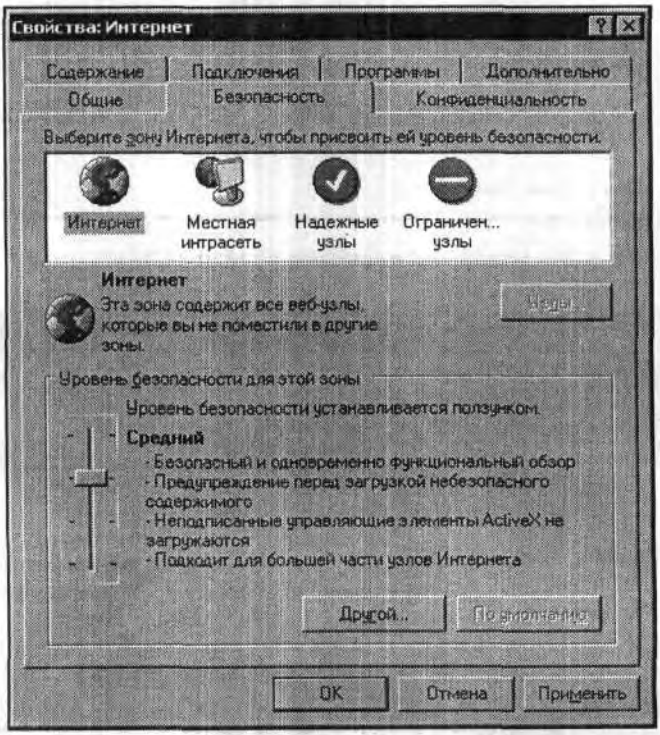


Рис. 2.16. Окно **Свойства: Интернет**, вкладка **Безопасность**

Пройдите по дереву объектов **Политика "Локальный компьютер" | Конфигурация компьютера | Административные шаблоны | System**.

В правой части окна найдите строку **Display Shutdown Event Tracker** (Отображать диалог слежения за завершением работы). В свойствах этого объекта установите состояние **Отключено**.

Internet Explorer в Windows Server 2003 по умолчанию настроен на высокий уровень безопасности. И это правильно. На сервере в Интернет можно выходить только для обновления программного обеспечения. На рабочей станции хотелось бы больше свободы.

Нажмите **Пуск | Выполнить | control** — откроется **Панель управления**. В ней находим **Свойства: Интернет** и открываем вкладку **Безопасность** (рис. 2.16).

Здесь, как и в обычной ОС, известные нам возможности настройки безопасности по зонам Интернета. Для зоны **Интернет**, в которой не определены какие-либо узлы с известными нам свойствами, уровень безопасности не может быть установлен ниже среднего. Но если вам необходимо его несколько снизить, можно нажать кнопку **Другой**.

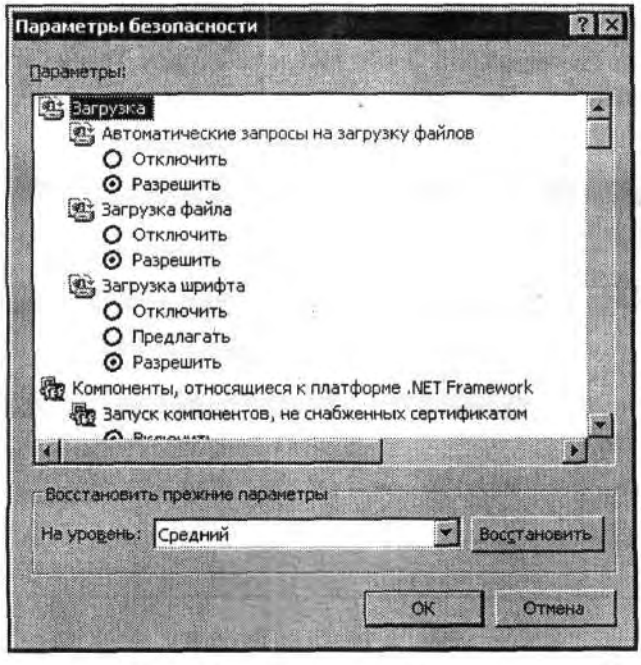


Рис. 2.17. Окно **Параметры безопасности**

Откроется окно **Параметры безопасности** (рис. 2.17), где можно выбрать наиболее подходящие для вас значения параметров. Интересно, что при изменении этих параметров на вкладке **Безопасность** пропадет изображение движка до восстановления стандартной настройки безопасности.

Для нормальной работы рабочей станции желательно включить аппаратное ускорение для видео- и аудиоустройств. Для его включения откройте **Пуск | Выполнить | dxdiag.exe**, это известное вам средство диагностики DirectX. На вкладках **Дисплей** и **Звук** включите необходимые кнопки и установите уровни ускорения.

Примечание

Вид вкладок зависит от конкретного оборудования, установленного на вашем компьютере.

На сервере оформление рабочего стола должно быть экономным с точки зрения потребления ресурсов компьютера. По моему мнению, на рабочей станции системного администратора также не должно быть "излишеств". Но на вкус и цвет товарищей нет. Если вам необходимы темы рабочего стола, следует пройти в **Пуск | Выполнить | services.msc**.

Откроется окно **Services** (рис. 2.18). Найдите службу **Themes** и в ее свойствах (рис. 2.19) установите **Тип запуска** в состояние **Авто**.

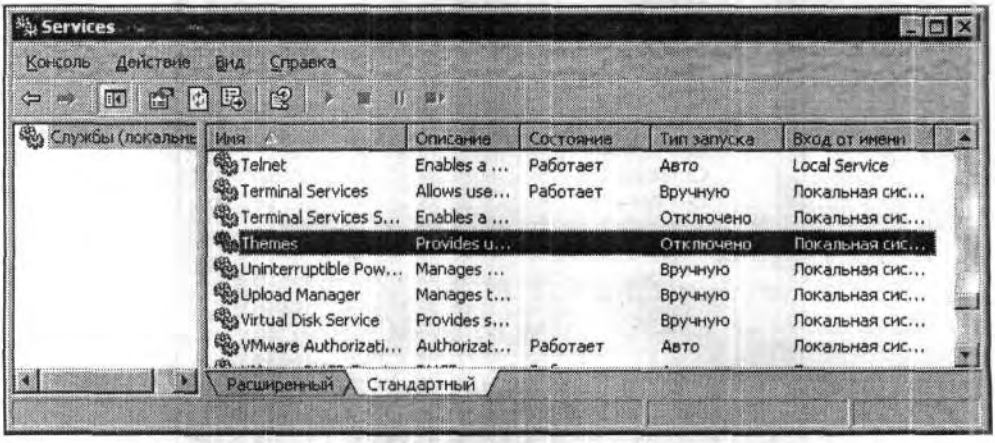


Рис. 2.18. Окно **Services**

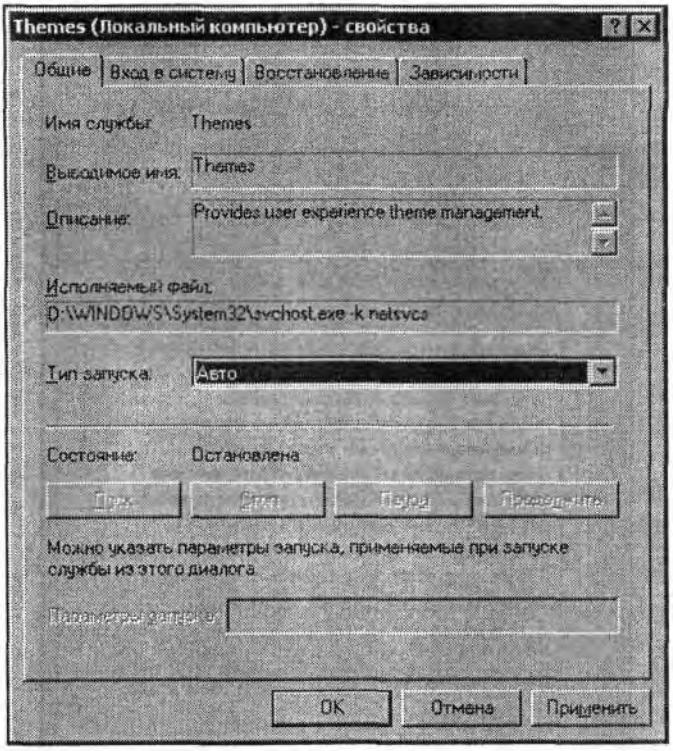


Рис. 2.19. Окно **Themes (Локальный компьютер) — свойства**

Примечание

В процессе работы в сети вам часто придется обращаться к свойствам служб (services), установленных на компьютере. Кроме пути, приведенного здесь, окно **Services** можно открыть через **Панель управления | Администрирование | Службы**.

Можно поправить и некоторые настройки в свойствах системы **Панель управления | Система** на вкладке **Дополнительно | Быстродействие | Параметры** (*окно* **Параметры быстродействия**).

На вкладке **Визуальные эффекты** (рис. 2.20) можно установить такое сочетание эффектов, которое вы предпочитаете. На вкладке **Дополнительно** (рис. 2.21) можно также оптимизировать работу процессора и памяти для программ, что для рабочей станции предпочтительнее. Но при использовании компьютера в качестве сервера эти параметры лучше оставить как есть.

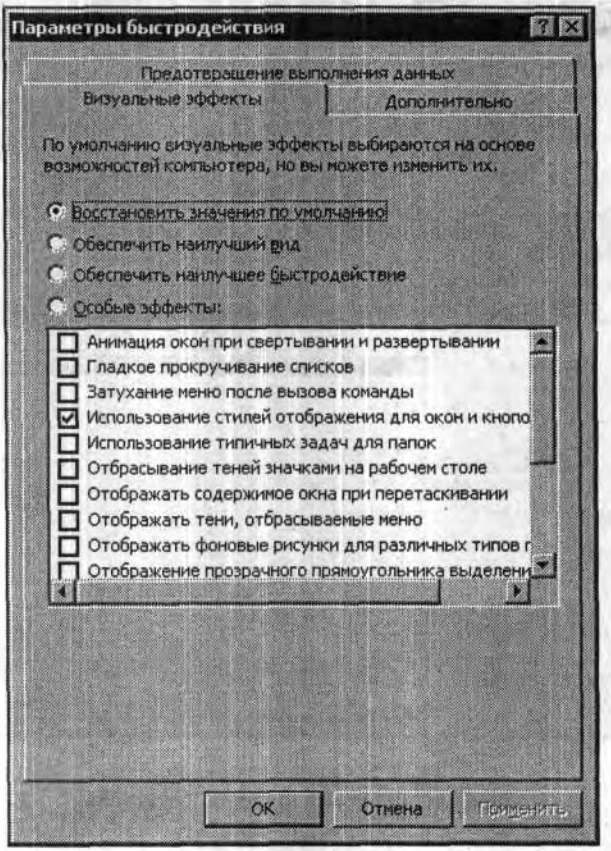


Рис. 2.20. Окно **Параметры быстродействия**

В окне свойств системы **Панель управления | Система** на вкладке **Дополнительно** есть еще кнопка **Отчет об ошибках**, при нажатии которой откроется одноименное окно (рис. 2.22). Если ваша система будет работать в режиме рабочей станции, то само собой разумеется, что необходимости посылать в Microsoft отчеты о незапланированных выключениях системы не имеет большого смысла. Возможно, что вы решите вообще отключить отчеты об ошибках.

Вот, собственно и все. Если вас не устраивает еще что-нибудь в работе системы, можно пройтись еще раз по всем настройкам, внимательно посмотрев на возможности их изменения.

Вполне возможно, что некоторые окна и параметры по умолчанию в вашей системе выглядят несколько иначе. Сделайте обновление системы до Service

Pack 1. Windows Update предложит вам это обновление, когда вы запустите данную программу, подключившись предварительно к Интернету.

Кое-что из предложенных настроек, возможно, вы выполните и на сервере, если уже его используете или собираетесь применить в сети. Меня раздражает, например, необходимость отчитываться перед сервером каждый раз, когда необходимо перезагрузить компьютер, который работает в качестве сервера в сети из трех компьютеров. Это домашняя (квартирная) сеть. Никто кроме меня не изменяет настройки этого сервера. И уж если что и сделаю не так, то я не буду рассматривать LOG-файл с записью выключений и перезагрузок. Единственное, что не стоит изменять, это уровень безопасности Internet Explorer. У нас все-таки сервер.

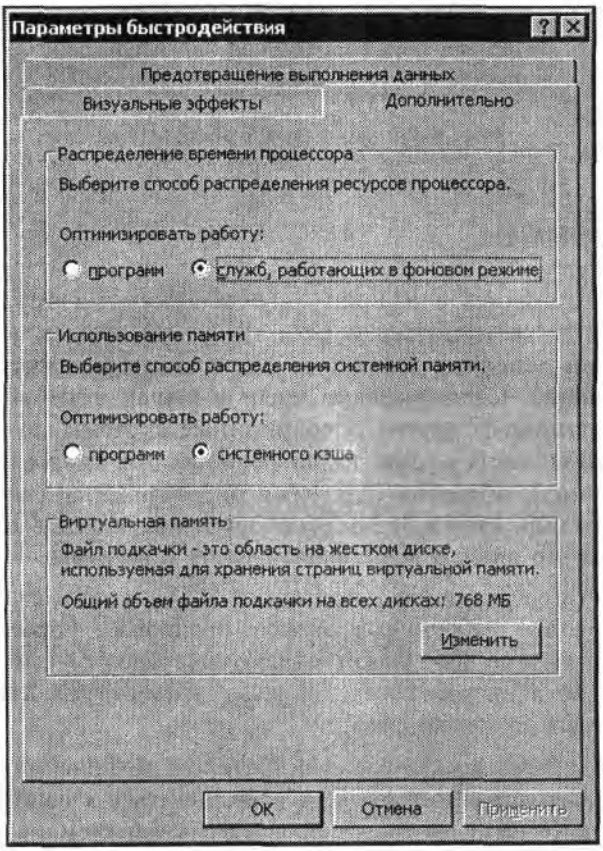


Рис. 2.21. Окно **Параметры быстродействия**, вкладка **Дополнительно**

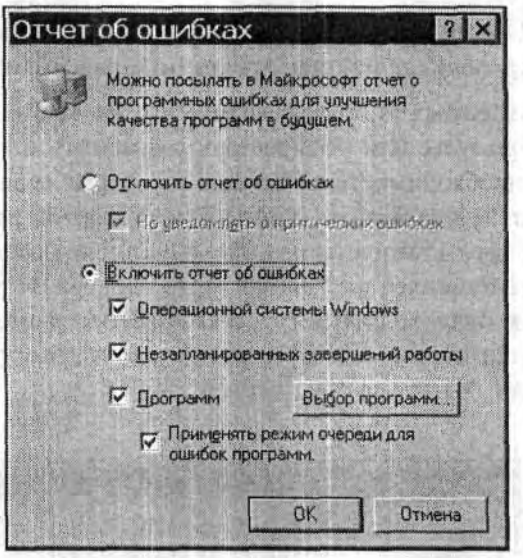


Рис. 2.22. Окно **Отчет об ошибках**

В заключение

Вот мы и познакомились с основными особенностями операционных систем, которые могут встретиться в сети. Конечно, это не исчерпывающий список. Но наша основная задача состоит в поддержании работы сети на основе ОС Windows. Следовательно, если в вашей сети это допустимо, и пользователи применяют другие операционные системы, вы можете возникающие у них проблемы оставить для решения им самим. В то же время, если вы имеете опыт общения с другими операционными системами и можете оказать помощь пользователю, который по тем или иным причинам применяет ее, то это плюс к вашему авторитету и имиджу.

Несмотря на все мое уважение к компании MTU, я не могу относиться положительно к словам работников службы поддержки Стрим, когда вместо помощи при настройке модемов и маршрутизаторов D-Link вы услышите, что эти модели не поддерживаются. В то же время огромное число пользователей применяют эти устройства.

Так и в случае с системным администратором небольшой сети. Если вы сможете подсказать пользователю, как подключиться к вашей сети, используя, например PTS DOS, который был предустановлен на его компьютер при покупке, ваш авторитет в глазах пользователей не упадет. Не упадет он, и когда вы квалифицированно объясните, какими ограничениями обладает ОС пользователя в вашей сети, если эти ограничения существуют.



Глава 3

Физическая сеть

В этой главе будут рассмотрены варианты физической организации сети, требования к компьютерам, оборудованию, его размещению, требования к кабельной системе. Насколько бы совершенно не было программное обеспечение, мастерство пользователей и администратора сети, сеть не будет работать нормально, если в ее составе плохие компьютеры, нестабильный сервер, кабели проложены наспех без соблюдения норм для кабельных сетей.

Что мы имеем?

Разговор у нас о модернизации и поиске неисправностей в сети. Но с чего начинается модернизация? Конечно, с того, что уже что-то существует и работает. А что за сеть работает у вас? К сожалению, невозможно получить единогласный ответ на этот вопрос. Кто-то из вас имеет лишь два компьютера, соединенные перекрестным кабелем, у кого-то уже серьезная сеть, в которой более десяти машин, а кто-то вообще только собирается организовать сеть. Одни имеют сеть дома, другие начали работу в качестве системного администратора в какой-либо организации. Старт у всех разный, но все прошли через момент рождения их сети или момент первого практического знакомства с ней. Естественно, что все началось с двух компьютеров, даже если они и были уже в большой сети.

Вот и мы начнем с двух компьютеров. Первой модернизацией будем считать уход от перекрестного кабеля. Перекрестный кабель соединяет два и только два компьютера. Для такого подключения вполне мог подойти и нуль-модемный кабель для LPT- или COM-порта. Такие соединения иногда удобно применять при наличии всего двух компьютеров, когда необходимо перенести большой объем информации с машины на машину, но они требуют специально переделанного кабеля. В наше время появилось множество других способов соединить два компьютера. Это и инфракрасные порты, и

USB-соединители, и Wi-Fi- или Blue Tooth-подключения. Но обычно эти способы подключения имеют мало общего с локальными сетями, как и передача посылки через знакомого проводника имеет не много общего с работой почтовой службы.

Но перед началом модернизаций желательно определиться с требованиями к модернизированной сети. Каждый проект начинается с технического задания. В то же время каждый проект опирается на некоторые общие требования, ГОСТы, технические условия и т. п. Не пугайтесь — мы не будем изучать нормативные акты, ГОСТы, СНиПы... Оставим это специализированным фирмам, для которых организация сетей — их бизнес. Тем не менее, определенные требования ко всем составляющим нашей сети необходимо установить.

Требования к компьютерам — рабочим станциям

Даже когда у нас всего два компьютера, для обеспечения их взаимодействия между собой и другим сетевым оборудованием они должны быть одной архитектуры. В большинстве случаев мы даже не задумываемся над этим, поскольку подавляющее большинство компьютеров, которые нам встречаются — IBM-совместимые машины с процессорами Intel или AMD. Это наиболее распространенный тип компьютеров в нашей стране и во всем мире ввиду их относительно невысокой цены, простоты обслуживания и распространенности программного обеспечения различного назначения для них. Но бывает, что у пользователей встречаются компьютеры Macintosh производства Apple Computer Inc. К сожалению, компьютеры Macintosh включить в одну сеть с IBM-совместимыми сложно. Такие компьютеры в нашей стране находятся обычно в индивидуальном использовании. В нашей сети должны быть только IBM-совместимые компьютеры. Соответственно и все оборудование, применяемое в сети, IBM-совместимое. Это требование выполнить проще всего, поскольку другое оборудование, если и продается, то не везде и по высоким ценам.

Но среди IBM-совместимых компьютеров, встречающихся в наше время у пользователей, есть машины очень старые. Раньше уровень совершенства компьютера определялся применяемым процессором. Вот линейка компьютеров в соответствии с прогрессом в их развитии: i386, i486, Pentium, Pentium Pro, Pentium II, Pentium III, Xeon, и Pentium IV и их аналоги фирм AMD, Cyrix, VIA, IDT. Были и i286, но их применение в наше время практически невозможно, учитывая требования программного обеспечения, применяемого пользователями. Для более или менее комфортной работы с современным программным обеспечением требуется компьютер не ниже, чем Pentium III. В отдельных случаях могут применяться и Pentium II. Те-

перь устаревшие модели компьютеров могут встречаться у домашних пользователей. Приобретя новую машину, ввиду морального устаревания старой, избавиться от последней не удается, а выбрасывать просто так жалко. Если компьютер имеет сетевую карту, то его вполне можно применить в домашней сети для выполнения задач, не требующих значительных ресурсов от компьютера.

Таким образом, сформировалось второе требование — компьютер должен иметь сетевой адаптер. Для пользователей ПК с некоторым стажем это требование совершенно очевидно, но для начинающих может быть не совсем понятным. Во всяком случае организаторы домовых сетей, объединяющих индивидуальных пользователей, имеют запас сетевых адаптеров для установки в компьютеры пользователей. Современные компьютеры часто имеют встроенные в материнскую плату сетевые адаптеры, но возможно применение и отдельно поставляемых сетевых карт (рис. 3.1). Сетевые адаптеры производятся различными фирмами и обладают различными возможностями. Но для нас важно, чтобы адаптер поддерживал работу в сети со скоростью передачи данных 10 или 100 Мбит в секунду.

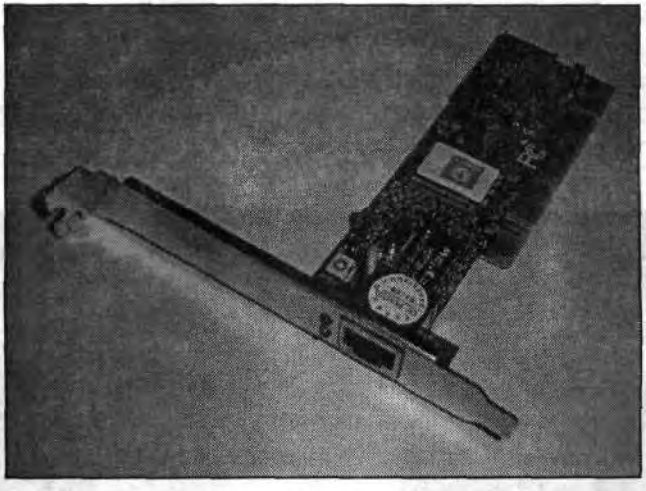


Рис. 3.1. Сетевой адаптер

Следующее требование не очень сильно связано с работой сети, но для офисных сетей от выполнения этого требования может зависеть успешность работы коллектива, использующего сеть. Каждый компьютер должен быть защищен от неблагоприятных воздействий со стороны питающей сети. Броски напряжения в питающей сети могут привести к выходу из строя компьютера или отдельных его составляющих. Обычный сетевой фильтр (рис. 3.2), защищающий от перенапряжений в сети, может уберечь ваш компьютер.

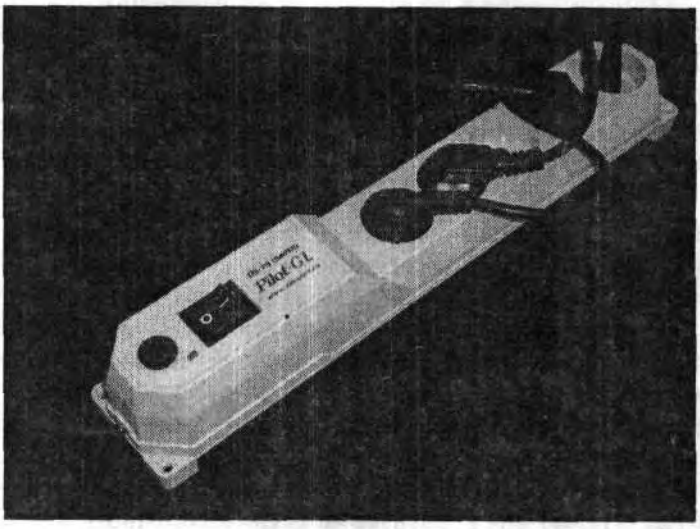


Рис. 3.2. Сетевой фильтр

Но для более ответственных рабочих мест может потребоваться и источник бесперебойного питания (рис. 3.3). Эти устройства позволяют продлить работу компьютера во время перебоев в электроснабжении, хотя бы для того, чтобы не потерять информацию, корректно завершив работу и сохранив данные.

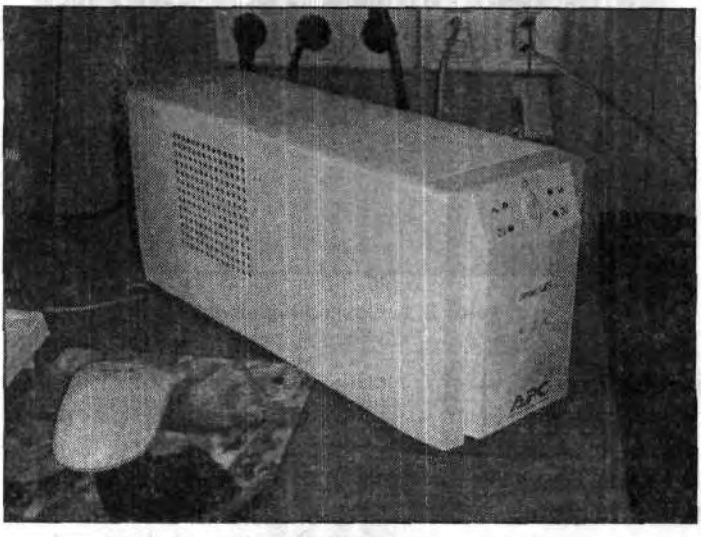


Рис. 3.3. Источник бесперебойного питания

Само собой, что компьютеры должны иметь установленную операционную систему, позволяющую работать в сети. Существуют различные операционные системы, предназначенные для работы в компьютерных сетях. Но нас интересуют ОС, предназначенные для работы в сетях Microsoft. В отдельных случаях на рабочих станциях и даже серверах сети может быть установлена одна из версий Linux. Но это допустимо тогда, когда не предполагается активный обмен информацией в сети. ОС Linux Fedora, например, позволяет создавать документы как текстового, так и графического формата, позволяет работать в Интернете, имеет множество средств для разработки программ, мониторинга сети, содержит программы как для рабочей станции, так и для сервера, весьма стабильна и к тому же бесплатна. Но в настоящее время эксплуатация сети на основе Linux требует довольно серьезной подготовки администратора. Даже установка этих ОС часто весьма трудоемка, а результат зависит от мастерства пользователя. Если вы не достаточно хорошо знаете Linux, то не стоит ориентироваться на применение этой ОС. Тем не менее, в домашней сети, где невозможно ограничить пользователя в желании использовать ту или иную ОС, Linux может применяться без вашего "благословения". В этом случае есть смысл оговорить с пользователями сети некоторые границы ваших возможностей в обеспечении работы не-Windows операционных систем. Для них вы наверняка можете обеспечить выход в Интернет, работу электронной почты, но специальные сервисы, включая доступ к серверу Windows Server 2003, использование возможностей Active Directory вы гарантировать не можете. То же относится и к другим не-Windows операционным системам. Есть, например, любители DOS различных версий. DOS тоже имеет некоторые привлекательные для отдельных пользователей возможности. На основе DOS могут быть созданы даже серверы, предоставляющие Web, FTP и некоторые другие сервисы. Рабочие станции с этими ОС могут содержать программное обеспечение, позволяющее просматривать Web-страницы в Интернете, работать с графикой, видео, звуком, электронными таблицами и др. Но и это, как говорят, отдельная песня. К сожалению для одних и счастью для других наиболее распространенными на рабочих станциях стали ОС Windows 98, Windows 2000, Windows XP. Именно эти системы могут поддерживаться вашей сетью полноценно. Но и Windows 98 уже имеет некоторые ограничения для работы в современных сетях. Поэтому для работы в офисе остаются только Windows 2000 и Windows XP. Причем последняя предпочтительней. Следует также отметить, что применение в государственных и коммерческих организациях Window XP Home Edition не допустимо. Это связано с условиями лицензирования Microsoft.

Относительно лицензирования операционных систем и программного обеспечения можно сказать, что лицензии должны быть. Ответственность за использование нелицензионного программного обеспечения может лежать на руководителе предприятия, системном администраторе, конечном пользова-

теле или на всех сразу в зависимости от конкретной ситуации. Более подробно о необходимости использования лицензионного ПО можно узнать на странице
http://www.microsoft.com/Rus/Antipiracy/Partner/Action/News/Default.mspx.

Никаких специальных требований к сборке компьютеров мы предъявлять не будем. Это дело пользователей или администрации организаций, которые приобретают компьютеры. Если вы уверены в работоспособности и надежности компьютера, а его характеристики вас устраивают, то не имеет значения, кто его собирал. Во всяком случае имя фирмы-производителя не может повлиять на возможность работы компьютера в сети. Возможно, что вам нравится самостоятельно собирать компьютеры для вашей сети. В этом случае вы должны хорошо представлять себе все особенности каждой машины сети, и в случае возникновения проблем с железом вы быстро сможете сориентироваться в причинах и решить их в кратчайшие сроки. Есть смысл иметь резерв запасных частей, таких как блоки питания, видеокарты (если применяются невстроенные), сетевые карты, платы оперативной памяти, винчестер. Чем однороднее состав компьютеров, тем меньше придется иметь запасных частей для оперативного восстановления их работоспособности в сети.

Требования к серверу

Если в сети применяется сервер, то к нему тоже можно предъявить некоторые требования. Конечно, многое зависит от материальных возможностей, но лучше, если этот компьютер имеет именно серверную конфигурацию. Серверу приходится работать без остановки сутками, следовательно, надежность его должна быть существенно выше, чем у обычной рабочей станции. Технические характеристики сервера зависят от задач, которые на него возлагаются. В домашней сети или сети малого офиса вполне может работать сервер не новый, например, на основе материнской платы Intel L440GX+. Его возможности для работы с ресурсоемкими приложениями по нашему времени несколько ограничены, но операционная система Windows Server 2003 на нем вполне прилично работает. Можно, конечно, применить в качестве сервера и обычную рабочую станцию. Но здесь уже вам решать. Устанавливать сервер желательно так, чтобы к нему был обеспечен свободный доступ в случае необходимости, но чтобы он не мешал окружающим. В случае если это сервер относительно большой сети, то его лучше устанавливать в отдельном помещении — серверной.

Сетевое оборудование и кабельная система

Это компоненты сети, без которых она не может существовать. О кабелях мы говорили в *разд. "Среда передачи данных" главы 1.* Но важно не только

какой кабель применяется, но и как он проложен к рабочим местам, как размещены коммутаторы или концентраторы, как осуществлена коммутация кабельной системы. Конечно, при наличии всего двух компьютеров, находящихся в одном помещении, не возникает серьезных проблем в прокладке кабеля. Но все же и здесь есть определенные требования, которые следует соблюдать.

Переходя от перекрестного кабеля к подключению через коммутатор, следует продумать место, где этот коммутатор будет находиться. Эта задача кажется простой, но, столкнувшись с ней впервые, вы можете обнаружить несколько проблем. В квартире или в офисе появление дополнительных предметов не всегда одобрительно воспринимается жильцами или работниками. Лучше всего, если вы найдете место на стене, где можно подвесить устройство с помощью предусмотренных для этого отверстий в корпусе и шурупов, завернутых в стену. Это позволит не только исключить загромождение полезной площади столов, но и обезопасит коммутатор от случайных неблагоприятных воздействий. Никто не уронит его на пол, не положит на него ворох бумаги (это может привести к перегреву и выходу коммутатора из строя). При большом числе компьютеров коммутаторы могут помещаться в специальные коммутационные шкафы. Кабель должен прокладываться по такому маршруту, который исключит случайные его повреждения ногами, предметами мебели, дверными полотнами, оконными створками. Не должно быть свисающих участков кабеля, за которые можно случайно зацепиться и выдернуть кабель из коммутатора, розетки или из сетевого адаптера.

Как бы проста не была сеть, все коммутации, маршруты кабеля, места размещения коммутаторов следует спланировать.

Давайте рассмотрим вариант нашей модернизированной простейшей сети в свете обозначенных требований (рис. 3.4).

На рисунке вы можете насчитать девять шнуров и кабелей, которые необходимо проложить и подключить к компьютерам и дополнительным устройствам, не считая шнуров к мониторам, клавиатурам и устройствам, которые на рисунке не показаны (принтеры, например). Для того чтобы обеспечить защиту подключений от случайных механических воздействий, кабели от коммутатора проложены по стенам и оканчиваются розетками. По сути, мы получили коммутационный центр сети, состоящей пока только из двух компьютеров. Организацию каждого рабочего места мы рассматривать не будем, поскольку для этого существуют стандартные решения в виде компьютерных столов на любой вкус и потребности.

В растущей сети появляется необходимость в дополнительном оборудовании, организующем сеть и позволяющем компактно разместить необходимые устройства. При расширении сети требуется предусмотреть и рабочее место для ее администратора.



Рис. 3.4. Сеть из двух компьютеров

Рабочее место администратора локальной сети

Несмотря на то, что сеть может занимать 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 к серверу, если необходимо срочно предпринять какие-либо меры. Как бы надежно не 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 случаи выключения или перезагрузки сервера невозможно, но время проведения этих операций и их количество должны быть минимизированы.

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, например, требуются не чаще одного раза в месяц, а сам перерыв длится три-четыре минуты. Если учесть, что для выполнения таких процедур выбирается время, когда большая часть пользователей сети не работает, то у этих пользователей складывается ощущение, что 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 к серверной от компьютеров сети, коммутаторов, расположенных в сети, от других сетей, возможно, взаимодействующих с вашей, приходит значительное число кабелей. Часто начинающие администраторы считают, что когда возникнет необходимость, можно переделать подключения, переложить кабели, заменить оборудование. На самом деле, если заранее не предусматривать возможности расширения сети, наступит момент, когда сеть будет неработоспособна продолжительное время, которое может составлять не один день, а вам, даже после восстановления ее работоспособности, придется еще завершать начатые работы не одну неделю. Лучше заранее готовиться к будущим проблемам. Естественно, что такая подготовка потребует определенных 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 убедить руководство, 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. 3.5 показан ввод кабелей в серверную и их подключение к коммутирующим устройствам в наименее затратном (на момент проведения работ) варианте.

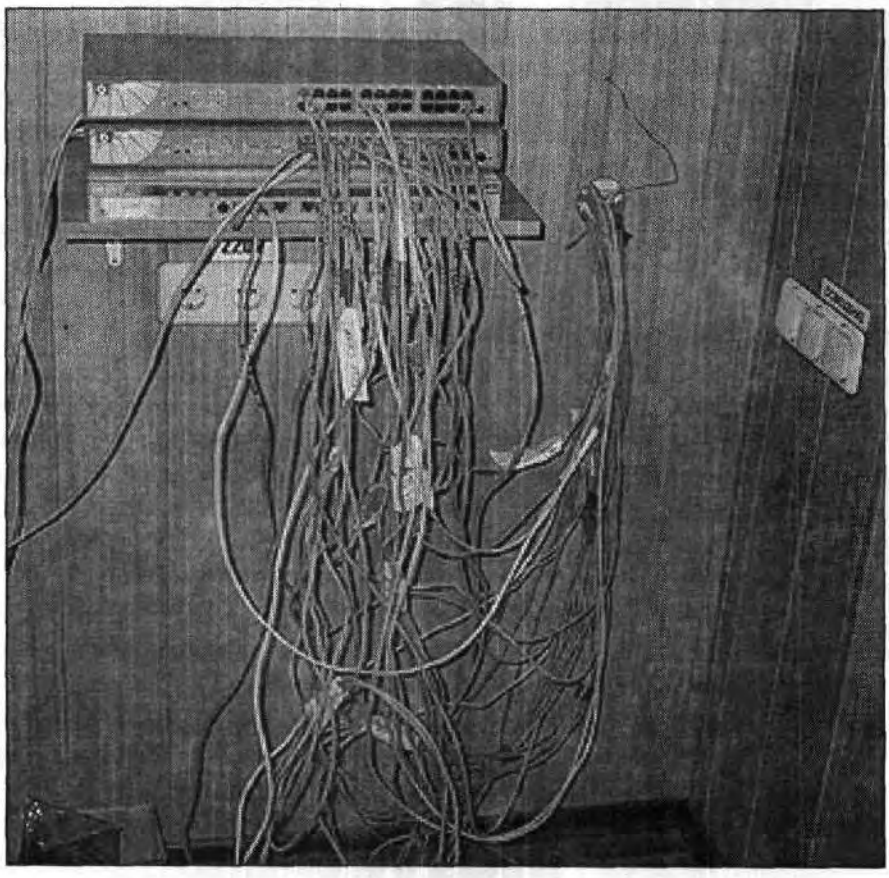


Рис. 3.5. Упрощенная коммутация кабелей и размещение оборудования

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 не велики, а работ по переподключению этих кабелей не пришлось бы выполнять, если бы сразу был применен другой вариант их организации при вводе в серверную. Такой вариант показан на рис. 3.6.

Теперь нет некрасиво и опасно расположенных кабелей, они аккуратно скрыты в коробах, а их подключение осуществлено через, специально для этого предназначенные патч-панели с организаторами кабеля. Часть ак-

тивного оборудования осталась здесь же в настенном коммутационном шкафу (рис. 3.7).

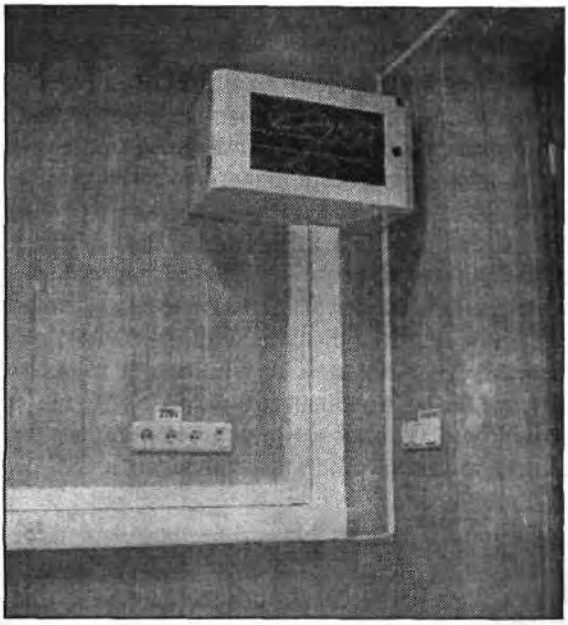


Рис. 3.6. Нормальная коммутация кабелей и размещение оборудования

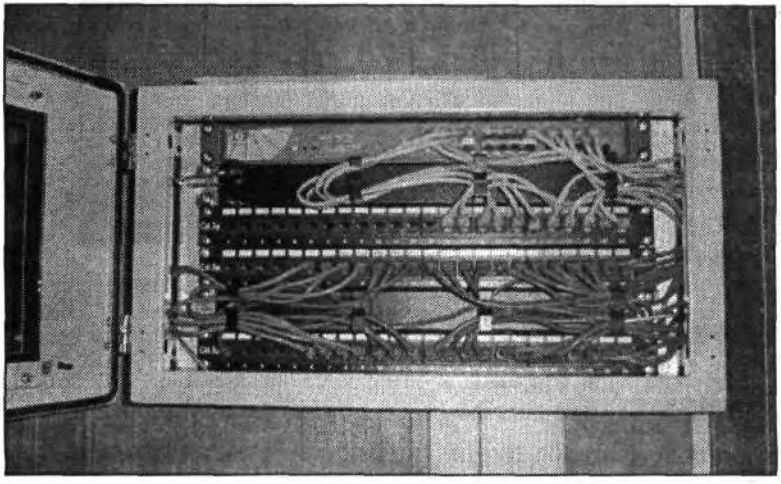


Рис. 3.7. Коммутационный шкаф с открытой дверцей

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

Конечно, самостоятельно вы вряд ли сможете установить такой шкаф. Для этого лучше пригласить специалистов, которых смогут вам порекомендовать там, где вы будете приобретать оборудование. 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. 3.8 показаны включенные в одинаковые гнезда компьютерной розетки телефонный провод и патч-корд, соединяющий с сетью компьютер.

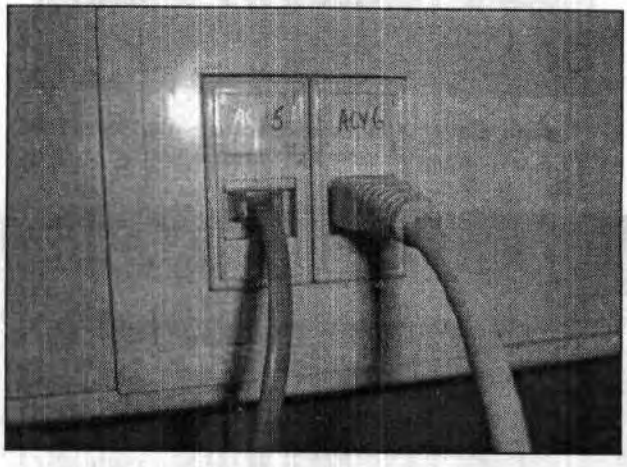


Рис. 3.8. Телефонный и компьютерный кабели подключены в одинаковые гнезда

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

Если телефон или компьютер не подключен к такой розетке, то ее гнезда закрываются подпружиненной заслонкой, что исключает попадание в них посторонних предметов и загрязнение (рис. 3.9).

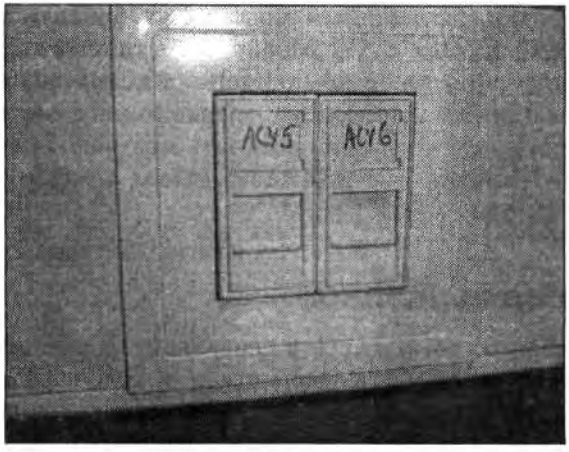


Рис. 3.9. Гнезда розеток, закрытые заслонками

Мы не указываем здесь конкретные типы кабельных каналов и коммутационных шкафов, вы сможете выбрать подходящее вам оборудование из вариантов, предложенных торгующими такими товарами организациями.

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. Во многих случаях вам не придется выезжать к месту, где находится ваша сеть для оперативного решения проблем, требующих вашего вмешательства. Можно иметь, конечно, и дома настроенный соответствующим образом компьютер, 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 стан-

цию, он должен иметь встроенный модем. Как ориентир, можно указать на 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 Professional, которую нужно 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, хабы (от англ. "hub"), 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, могут быть 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 при скромном списке применяемых устройств на столе лучше поместить монитор, мышь и клавиатуру. Все остальные устройства лучше разместить в специальной стойке — шкафу (рис. 3.10). 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.

Уже те описания организации подключений в сети, которые вы прочитали, говорят о необходимости значительного объема предварительной работы перед модернизацией или добавлением новых участков сети. Для того чтобы упростить работу по составлению планов модернизации и развития сети,

можно воспользоваться услугами автоматизированного составления проектов локальной сети.

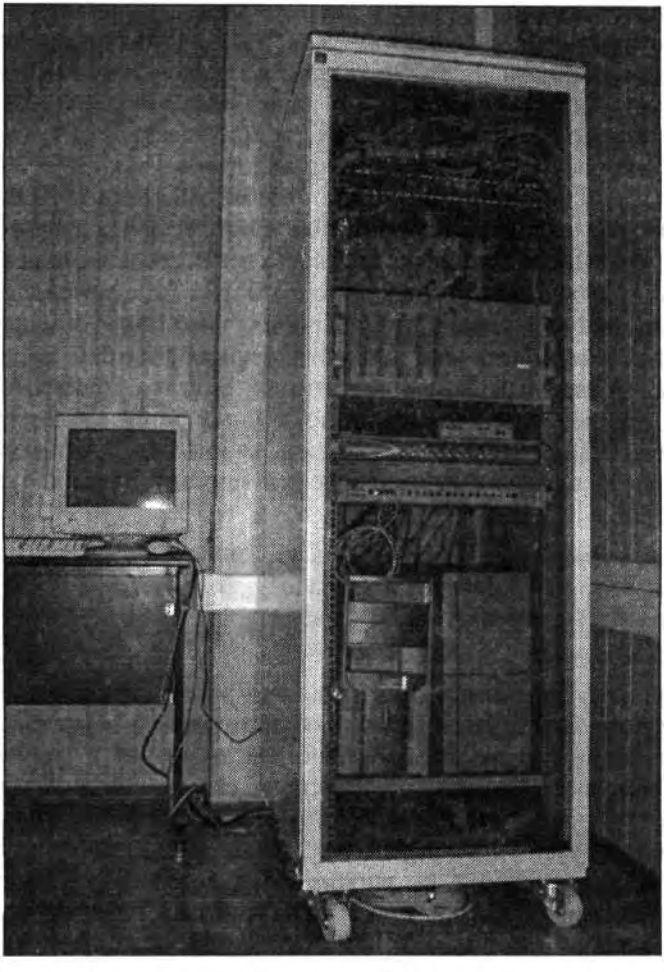


Рис. 3.10. Компьютерная стойка с оборудованием

Автоматическое проектирование сети

Развитие средств автоматического проектирования привело к тому, что теперь каждый пользователь ПК, имеющий доступ в Интернет, может получить проект будущей сети буквально за считанные минуты. Такую возможность предоставляет компания "Тауэр-Сети и Технологии" с помощью своей

разработки — системы интерактивного проектирования информационных систем (**www.netwizard.ru**). С момента ее появления в 2000 г. в доступном через Интернет для любого желающего варианте я не нашел аналогичных сервисов, предоставляемых другими компаниями. "Тауэр-Сети и Технологии" *бесплатно* осуществляет разработку эскизных проектов информационных систем любой сложности. Все консультации по вопросам выбора, монтажа и использования сетевого оборудования, кабельных систем и вычислительной техники проводятся *бесплатно*. Наиболее сложные проекты, также *бесплатно*, получают экспертную оценку у специалистов в Presales Center 3Com. Недостатком системы проектирования на настоящий момент является отсутствие предложений новых операционных систем для серверов и рабочих станций. Но это, учитывая экономию времени и средств на разработку проекта, мелочь, которую можно откорректировать самостоятельно. Оборудование, предлагаемое системой, поставляется фирмами, поддерживающими проект. Но для нас важно, что автоматически созданный проект позволяет определить качественный и количественный состав оборудования, материалов и работ, что без опыта создания локальных сетей сделать трудно. Если вы собираетесь самостоятельно проводить работы по расширению или созданию локальной сети, то автоматический проектировщик окажет существенную помощь.

В начале работы над проектом можно выбрать версию автоматического проектировщика, который проведет всю работу. Этих версий доступно уже три. Попробуем получить проект несложной сети с помощью этого прогрессивного метода.

Войдя на страницу компании, нам придется зарегистрироваться, внеся сведения о себе в предлагаемые формы. После ответа на вопросы программы о наших требованиях к будущей сети начинается расчет и формирование документации. Проект содержит структурную схему, спецификацию и техзадание. Конечно, проект поддерживается определенными фирмами и рекомендует использовать оборудование этих фирм. Но, даже если у вас уже есть бóльшая часть оборудования, вы вполне можете дополнить его, руководствуясь спецификацией. Некоторые элементы система навязывает, не спрашивая вас, но вы можете подойти к проекту рассудительно и использовать только необходимое оборудование. В спецификации приведены как цены на оборудование, так и расценки на работы по прокладке кабеля и монтажу сети. Даже приблизительно составленный этой системой проект поможет вам сориентироваться в ценах и определить ваши возможности. Предположим, что будущая сеть состоит из шести рабочих мест, расположена компактно на одном этаже, расстояние между машинами и хабом около десяти метров. Операционная система — Windows 98.

Примечание

Текущая версия проектировщика не имеет в своем составе ОС Windows XP.

Автоматический проектировщик самостоятельно предлагает включить в состав сети сервер и указывает конкретный тип и характеристики машины. Даже если вы не собираетесь пока устанавливать сервер, вы можете ознакомиться с его характеристиками и ценой, чтобы в будущем принять решение на основании уточненных знаний. Но рассмотрим результаты расчета по порядку.

Прежде всего, приводятся *характеристики сети*. Указаны ее некоторые конструктивные особенности. Количество коммуникационных центров в нашем варианте сети соответствует количеству коммутаторов. Все компьютеры подключены к одному устройству, позволяющему им связываться друг с другом и с сервером. Каждый ПК подключен к сети через свой порт. Поэтому в проекте указано, что количество активных портов — 6. Каналы для рабочих станций выделенные. Это значит, что каждая станция имеет свой адрес и может быть связана с сервером параллельно с другими станциями.

Далее следует описание *главного коммутационного центра*. В нашем случае — это вся компактно расположенная сеть. В больших сетях с несколькими серверами могут применяться несколько коммутационных центров. Среди них есть главный и подчиненные центры, осуществляющие связь как с компьютерами главной сети, так и с машинами других сетей, которые могут быть связаны с главной. Для упрощения проекта при "заказе" мы отказались от управления активным оборудованием (например, можно управлять коммутаторами), а также от его резервирования. Но источник бесперебойного питания предложен проектировщиком без нашей просьбы, иначе сеть не будет иметь достаточной, по мнению программы, надежности. Указано общее количество портов — 12. Это весьма разумно, т. к. допускает развитие сети. Никто не может сказать, что произойдет завтра и какие резервы понадобятся. Но если появилась потребность развития сети, а резервов нет, проблем у вас возникнет достаточно.

Следующий раздел — *серверы коммуникационного центра*. Он описывает единственный сервер сети, которого может и не быть. Точнее, в сети выделенного сервера может и не быть, но программа считает, что он необходим. Сервер — это не только машина, но и программное обеспечение, предоставляющее рабочим станциям некоторые дополнительные возможности. Мы предполагали, что в нашей сети потребуется электронная почта для всех станций и файловый сервис, позволяющий всем машинам использовать дисковое пространство сервера. Все станции на равных правах могут пользоваться сервером электронной почты и файловым сервером, физически находящимися в одной машине. В нашем случае это сервер 1-го уровня Аквариус: AquaServer E200, его характеристики приведены далее.

Эта модель относится к серверам начального уровня, рекомендованного изготовителем для использования в качестве файлового и принт-сервера в рабочих группах или сервера электронной почты. В базовой конфигурации

он поставляется с одним процессором Intel Pentium III 500, ОЗУ 128 Мбайт ECC SDRAM, Ultra Wide SCSI-винчестером емкостью 9,1 Гбайт, накопителем CD с 40-кратной скоростью и сетевым адаптером Fast Etherlink III 3C905B-TX. Легко наращиваемый, неприхотливый и простой в обслуживании сервер прослужит вам долгие годы. Повышенная надежность в работе и разумная цена — вот основные отличительные особенности AquaServer E200. По желанию заказчика серверы могут комплектоваться и другим оборудованием.

Далее приведены базовые конфигурации моделей серии AquaServer E.

- AquaServer E200.
- Процессор Intel Pentium III, 500 МГц, 512 Кбайт кэш-памяти.
- Системная плата Soyo SY-D6IBA(-2)/MicroStar MS-6120.
- Системная шина 100 МГц.
- Оперативная память 128 Мбайт ECC SDRAM.
- Жесткие диски 9,1 Гбайт UWSCSI.
- Порты ввода/вывода 4 PCI, 3 ISA, 1 порт AGP2x, 2 Ultra2 Wide SCSI, 2 UDMA.
- Сетевой адаптер 3C905B-TX/IntelPro100/B.
- Видеоконтроллер SVGA, 2 Мбайт AGP.
- CD-ROM 40x.
- Стандартный дисковод для гибких дисков 1,44 Мбайт, 3,5 дюйма.
- Корпус Big Tower.
- Внутренние отсеки для жестких дисков 3×5,25", 3×3,5".
- Отсеки для съемных накопителей 3×5,25", 4×3,5".
- Источник питания 300 Вт.
- Поддерживаемые операционные системы MS Windows 2000/NT 4.0 Server, UNIX, Novell Netware 5.1, Red Hat Linux 6.2.

В этом сервере можно установить до двух процессоров Intel Pentium II/III. Он содержит 4 разъема PCI, 3 ISA, 1 порт AGP и два интерфейса Ultra Wide SCSI. В корпусе Big Tower могут разместиться до четырех 3,5-дюймовых и до трех 5,25-дюймовых устройств. Системные платы SY-D6IBA (-2) с набором микросхем i440BX поддерживают процессоры до Pentium III 600 МГц; максимальный объем оперативной памяти — 1 Гбайт. Дисковая подсистема рассчитана на 4 жестких диска Ultra Wide или Ultra2 SCSI (на системной плате SY-D6IBA-2).

В разделе "Сервер № 1", в графе "Тип операционной системы сервера" стоит "NO". Дело в том, что свойства сети, которые мы хотим получить, поддер-

живаются сервером с Windows 2000 Server, а мы пока рассчитываем обойтись версией ОС для рабочей станции.

Завершает описание параметров сети раздел "Персональные компьютеры главного коммуникационного центра". Предложено использовать Aquarius Standard. Далее приводятся характеристики базовой модели этого компьютера.

- Оперативная память наращивается до 512 Мбайт; возможна установка до 4 дисков IDE.
- Ultra-DMA. Слоты расширения (4 PCI) позволяют разместить необходимое количество устройств.
- Три 5,25-дюймовых отсека предназначены для внешних устройств. Дают возможность установки нужных накопителей. Компьютеры этой серии оборудованы двумя портами универсальной последовательной шины (USB) для подключения периферийных устройств новейших стандартов.
- Процессор Intel Celeron с тактовой частотой 466—600 МГц.
- Системная шина 66/100 МГц.
- Кэш-память 2-го уровня 128 Кбайт.
- Набор микросхем базовой логики Intel 810/440ZX.
- ОЗУ минимум 32 Мбайт с возможностью расширения до 512/768 Мбайт, 2—3 разъема для модулей DIMM.
- Жесткий диск от 4,3 до 20 Гбайт Ultra DMA; поддерживается до 4-х жестких дисков.
- Флэш-BIOS, 4 Мбит флэш-памяти для системной BIOS, SCSI и видео-BIOS.
- Слоты расширения 3—4 PCI/0-2 ISA.
- Каналы ввода/вывода, последовательный и параллельный порт, 2 порта USB, порт IrDA, разъемы PS/2 для клавиатуры и мыши.
- Внутренние отсеки для жестких дисков. Два 3,5-дюймовых отсека для съемных накопителей.
- Источник питания 250 Вт.
- Стандартный дисковод для гибких дисков 1,44 Мбайт, 3,5 дюйма.
- CD-ROM 40x.
- Видеоконтроллер Video i810/AGP-видеоплата.
- Видеопамять. Динамическое выделение памяти из ОЗУ (i810)/4—32 Мбайт.
- Поддерживаемые операционные системы MS-DOS, MS Windows 9x/NT/2000, Red Hat Linux 6.2.

- Корпус Middle Tower (ATX)/Mini Tower (microATX).
- Габариты корпуса Middle Tower (высота × ширина × глубина) 400×210× ×420 мм, Mini Tower 365×185×400 мм.
- Сертификат соответствия качества стандарту РИСО 9002, сертификат соответствия РОСС RU ME06.B00193.
- Гигиенический сертификат № 12РЦ-128. Сертификат надежности № RINC.RU.E003.C00002. Сертификат на совместимость с ОС Windows 98 и Windows NT.

Примечание

В настоящее время существуют более новые, более быстрые модели компьютеров. Но в нашем проекте это не много меняет. Важно, что мы видим состав комплектующих.

Структурная схема компьютерной сети

Структурная схема сети показана в табл. 3.1—3.6[1].

Таблица 3.1. *Параметры сети*

Параметр	Величина или свойство
Количество коммуникационных центров	1
Количество активных портов	6
Каналы для рабочих станций	Выделенные

Таблица 3.2. *Главный коммуникационный центр*

Параметр	Величина или свойство
Количество активных портов	6
Управляемость активным оборудованием	Нет
Резервирование источников питания активного сетевого оборудования	Нет
Резервирование центрального сетевого устройства	Нет
Резервирование управления	Нет

[1] Данный отчет построен с помощью системы NETWIZARD (**www.netwizard.ru**) © 2000. Компания Тауэр.

Таблица 3.2 *(окончание)*

Параметр	Величина или свойство
Средняя длина кабельных каналов, м	10
Способ прокладки кабеля	Короб
Крепление розеток СКС	На плоскую поверхность
Количество портов UTP	12
Нужны источники бесперебойного питания для активного сетевого оборудования	Да

Таблица 3.3. *Серверы коммуникационного центра*

Серверы уровня 1	Распределение пользователей по серверам	
	Сервер эл. почты (кол-во клиентов)	Файловый и принт-сервер (кол-во клиентов)
Сервер 1	6	6

Таблица 3.4. *Сервер № 1*

Параметр	Величина или свойство
Процессор	Обычный
Объем ОЗУ (Мбайт)	384
Объем дискового пространства (Гбайт)	18
Желаемый тип корпуса сервера	Rack
Отказоустойчивость	Нет
Наличие устройства для резервного копирования данных (стримера)	Нет
Тип операционной системы сервера	Нет
Источник бесперебойного питания	Требуется
Количество связей	1
Технология связи	10Base-T
Скорость передачи, Мбайт/с	10
Среда передачи	Витая пара (Twisted Pair)
Характеристика связи	Неэкранированная витая пара (UTP)

Таблица 3.5. *Персональные компьютеры главного коммуникационного центра*

Параметр	Величина или свойство
Количество	6
Станции стандартной конфигурации	Да
Тип процессора	Celeron
Частота процессора, МГц	600
Объем ОЗУ, Мбайт	64
Объем видео-ОЗУ, Мбайт	4
Объем жесткого диска, Гбайт	10
Диагональ монитора, дюймов	15
Наличие мультимедиа	Нет
Наличие источников бесперебойного питания	Да
Операционная система	Windows 98
Количество лицензий ОС	6
Офисное ПО	MS Office 2000 Standard
Количество лицензий офисного ПО	6

Таблица 3.6. *Связи персональных компьютеров*

Параметр	Величина или свойство
Количество	6
Тип связи	Коммутируемая
Технология	10Base-T
Скорость передачи, Мбайт/с	10
Среда передачи	Витая пара (Twisted Pair)
Характеристика	Неэкранированная витая пара (UTP)

После описания общих характеристик сети предлагается спецификация, в которой вы найдете ответы на все "Что?", "Сколько?" и "Почем?" В разделе "Активное сетевое оборудование" предлагается использовать двенадцатипор-

товый коммутатор SuperStack 3 Baseline 10/100 Switch 12 port 10/100Base-TX и сетевую плату Fast EtherLink XL PCI 10/100 TX M.

Коммутаторы SuperStack II Baseline 10/100 применяются в любой сети, где требуется высокая производительность, но нет необходимости в управлении. Они могут, во-первых, использоваться как агрегирующие устройства при подключении других коммутаторов и хабов (концентраторов), во-вторых, предоставлять недорогое, быстродействующее решение для соединения с рабочими станциями пользователей. Коммутаторы 3Com SuperStack II Baseline не имеют функций управления, они готовы к работе сразу же после включения.

Ключевые особенности устройств:

- автоматическое определение скорости передачи и возможность установки полудуплексного или дуплексного режимов для каждого порта удваивают скорость соединения до 200 Мбит/с;
- таблицы MAC-адресов дают возможность поддерживать до 4000 устройств локальной вычислительной сети;
- функция управления потоком IEEE 802.3x (Flow Control) гарантирует отсутствие потери пакетов в высокоскоростных дуплексных соединениях во время пиков трафика;
- размер устройства упрощает установку в стойку с помощью поставляемого комплекта для монтажа, устройство может также использоваться автономно;
- диагностические индикаторы (LED) показывают состояние сети и статус каждого порта, облегчая поиск ошибок и проверку статуса индивидуального порта;
- подключение резервной системы питания Advanced Redundant Power System (улучшенная резервная система питания) обеспечивает надежную защиту от простоев сети.

Если у вас есть хаб и сетевые платы иного, чем здесь описано, типа — вы можете использовать их. Но в последнее время вместо хабов все чаще применяют коммутаторы, передающие сигнал не на все компьютеры сразу, а только в тот сегмент, где находится нужный компьютер. Это позволяет делать более сложные (топологически) сети. Источники бесперебойного питания, безусловно, вещь нужная и полезная, но если сумма $1607,92 не приводит вас в восторг и электрическая сеть работает стабильно, напряжение не меняется более чем на 10% и не выключается в неподходящий момент, то какое-то время можно обойтись без них.

Спецификация

Спецификация для проекта приведена в табл. 3.7[2].

Таблица 3.7. *Спецификация*

Артикул	Наименование товара	Ед. изм.	Кол-во	Цена, $	Сумма, $
Активное сетевое оборудование					**778,44**
3C16464B	SuperStack 3 Baseline 10/100 Switch 12 port 10/100Base-TX	шт.	1	424,24	424,24
3C905C-TX-M	Fast EtherLink XL PCI 10/100 TX M	шт.	7	50,60	354,20
Источники бесперебойного питания					**1607,93**
SU1000INET	Smart-UPS 1000	шт.	1	452,90	452,90
BK650MI	Back-UPS 650MI	шт.	6	192,50	1155,02
Кабельные каналы					**87,10**
NCT1050	Короб 100×50	м	6	9,88	59,28
NCI1050	Соединитель 100×50	шт.	1	1,69	1,69
NJC1050	Заглушка на шов 100×50	шт.	1	1,69	1,69
NAF1050	Плоский угол 100×50	шт.	2	5,68	11,36
NWP1050	Заглушка внутренняя 100×50	шт.	3	2,86	8,58
PVH_GOFR_20_P	Труба ПВХ гофрированная 20 мм с протяжкой	м	18	0,25	4,50
Серверы и рабочие станции					**6136,00**
QEV-1G6670131091NINN	Aquarius Server E100 133	шт.	1	1 351,00	1351,00
DIMM 256 Мбайт	SDRAM ECC 100 MHz	шт.	1	315,00	315,00
Monitor15	Monitor 15 LITE-ON TCO95	шт.	7	198,00	1386,00
QSI-C600064100-FNNS2	Aquarius Std MC600 (C600/64/VINT/H10/KM-SB)	шт.	6	514,00	3084,00

[2] Данный отчет построен с помощью системы NETWIZARD (**www.netwizard.ru**) © 2000. Компания Тауэр.

Таблица 3.7 (продолжение)

Артикул	Наименование товара	Ед. изм.	Кол-во	Цена, $	Сумма, $
Программное обеспечение					**1738,64**
730-01011	Windows 98 Russian Disk Kit CD /Upg Second Edtn	шт.	1	20,08	20,08
730-01196	Windows 98 Russian DocKit Second Edtn	шт.	1	16,05	16,05
730-01629	Windows 98 Russian VUP OLP NL	шт.	6	67,62	405,72
021-02771	Office 2000 Win32 Russian Disk Kit CD	шт.	1	20,08	20,08
021-02770	Office 2000 Win32 Russian DocKit	шт.	1	16,05	16,05
021-03881	Office 2000 Win32 Russian OLP NL	шт.	6	210,11	1260,66
Пассивное сетевое оборудование					**760,83**
27.1B.241.A005G	19" Patch Panel, 24xRJ45 KATT with cover, 568B, UTP, Power Cat, 1U, Graphite	шт.	1	169,89	169,89
25.A017G	19" Ring Run (Jumper) Panel, 1U, Graphite	шт.	2	23,49	46,98
45.0B.011.D022E	Patch Cord RJ45, 568B-N, UTP stranded, PowerCat, 1 m, Grey	шт.	6	5,09	30,54
45.0B.011.D024E	Patch Cord RJ45, 568B-N, UTP stranded, PowerCat, 3 m, Grey	шт.	6	7,64	45,84
39-504-PS	UTP PVC Cable PowerCat 4-pair	м	120	0,42	50,10
17.1B.011.A0042	Euromod 1xRJ45, M1 Straight, 568B, UTP, PoweCat, White	шт.	12	5,14	61,68
42-501-32	Розеточная коробка для установки на плоскую поверхность Surface Box UK 1G 32 mm	шт.	6	1,94	11,64

Таблица 3.7 (окончание)

Артикул	Наименование товара	Ед. изм.	Кол-во	Цена, $	Сумма, $
Пассивное сетевое оборудование					**760,83**
17-0111-02	Лицевая панель розетки Labelled Single Gang Wall-plate, United Kindom, 86×86×10 mm, White	шт.	6	2,84	17,04
DR3016604	CageNuts/Washers/6mm Screws (50)	шт.	1	16,09	16,09
DR3006106	W/M Cab. Acrylic Door. 600w×400d×6U	шт.	1	311,03	311,03
Работы по монтажу сети					**582,50**
MUTP5	Прокладка кабеля UTP	м	120	0,30	36,00
MKOROB	Монтаж короба	м	28	2,00	56,00
MKOROBB	Монтаж короба на бетонной стене	м	3	2,50	7,50
MROZ1	Установка розетки RJ-45	шт.	11	10,00	110,00
MROZ1B	Установка розетки RJ-45 на бетонной стене	шт.	1	15,00	15,00
MRACK	Установка шкафа	шт.	1	150,00	150,00
MPATCH	Монтаж патч-панели, 1 порт	шт.	12	4,00	48,00
TUTP	Тестирование UTP/STP-порта	шт.	12	5,00	60,00
MDOC	Подготовка документации на СКС	шт.	1	100,00	100,00
	ИТОГО				**11 691,44**

В спецификации перечислены почти все "мелочи", о которых недосуг задуматься, когда мечтаешь об организации сети и представляешь ее работу. Кабели должны быть аккуратно уложены и защищены от случайного смещения половой тряпкой, от повреждения передвигаемой мебелью и от других неблагоприятных воздействий. В спецификации приведены детали кабельных каналов с указанием цен, размеров и необходимого количества.

Вполне возможно, что у вас уже есть какие-либо иные средства для прокладки кабеля, или вы упростите систему прокладки из-за архитектурных особенностей строения, где будет находиться сеть. Но в любом случае, изучив спецификацию, вы не упустите незаметные с первого взгляда, но важные моменты в процессе организации сети. В разделе "Пассивное сетевое оборудование" перечислены кабели, разъемы, розетки, панели для монтажа разъемов и подключения кабелей. Для удешевления проекта при малых размерах сети от этих элементов можно отказаться, проводя подключения компьютеров к хабу напрямую, без использования промежуточных панелей, а также управляя питанием от сети переменного тока с помощью выключателей на сетевых фильтрах. Их применение при отсутствии источников бесперебойного питания очень желательно. И, наконец, в спецификации приведен перечень работ по монтажу сети. Для небольшой сети, монтируемой своими руками, вся стоимость работ может быть равна нулю. Налицо существенная экономия по сравнению с затратами при вызове специалистов.

Техническое задание на разработку проекта компьютерной сети

Последний важный документ, который нам позволяет получить автоматический проектировщик, это *техническое задание*. Ни один серьезный проект не воплощается без предварительного составления технического задания. В нем отражены все особенности сети и требования к ней. По сути, это не последний, а первый документ, на основе которого проект может детализироваться и рассчитываться. По техническому заданию, составленному автоматическим проектировщиком, вы можете оценить, соответствует ли проект вашим представлениям о предполагаемой сети. Если обнаружены какие-либо неточности, несоответствия вашему замыслу, то проект можно пересчитать за несколько минут, внеся необходимые коррективы при вводе первичной информации. Изменения могут повлиять и на состав оборудования, и на затраты, связанные с монтажом сети.

Общие положения

Данное техническое задание составлено на основе анализа ответов на вопросы, заданные системой NETWIZARD в интерактивном диалоге через сеть Интернет. Многие параметры проектируемой сети установлены в соответствии с экспертной оценкой системы.

Описание задачи

1. Основные параметры[3].

   Компьютерная сеть проектируется для 1-го этажа здания, в котором необходимо обеспечить взаимодействие 6-ти персональных компьютеров. Кабельная инфраструктура строится на базе одного главного коммуникационного центра. Проектируемая сеть должна обеспечить решение следующих задач:

   - сетевое хранение файлов и сетевая печать;
   - электронная почта.

2. Распределение персональных компьютеров по коммуникационным центрам.

   Главный коммуникационный центр — 6 штук.

3. Активное сетевое оборудование.

   Программой предлагается активное сетевое оборудование фирмы 3Com, но каждый вправе выбирать.

4. Параметры производительности:

   - полоса пропускания канала связи с рабочими станциями должна составлять не менее 10 Мбит/с;
   - необходимо выделять эту полосу пропускания для каждой рабочей станции (коммутируемая сеть);
   - магистраль должна обеспечивать пропускную способность не менее 33% от максимального трафика коммуникационного центра.

5. Управление трафиком.

   Средства эффективного управления трафиком в сети не требуются.

   Параметры межузловых каналов связи проектируемой сети представлены в табл. 3.8.

Таблица 3.8. *Параметры межузловых каналов*

Назначение канала	Скорость канала, Мбит/с	Кол-во каналов	Объединять каналы
Связи с ЛВС другого здания	100	1	–

6. Структурированная кабельная система:

   - для связи с серверами необходимо использовать кабель типа "неэкранированная витая пара";

---

[3] Техническое задание составлено с помощью системы NETWIZARD (**www.netwizard.ru**) © 2000. Компания Тауэр.

- для связи с рабочими местами необходимо использовать кабель типа "неэкранированная витая пара";
- для связи с ЛВС другого здания применяется кабель типа "неэкранированная витая пара";
- на каждом рабочем месте необходимо установить 2 порта кабельной системы.

7. Параметры кабельной системы главного коммуникационного центра:
   - среднее расстояние от коммуникационного центра до рабочего места составляет 10 м;
   - среднее расстояние между главным и этажным коммуникационными центрами составляет 10 м;
   - монтаж кабельной системы в комнатах должен быть выполнен в узком коробе;
   - бетонные стены составляют 10%.
8. Программное обеспечение:
   - должно быть представлено продукцией фирмы Microsoft;
   - в качестве операционной системы персональных компьютеров необходимо применять Windows 98, при этом предпочитаемый язык интерфейса — русский;
   - в качестве офисных приложений для персональных компьютеров должен использоваться программный продукт MS Office 2000 Standard, при этом предпочитаемый язык интерфейса приложения — русский.
9. Центральные серверы и персональные компьютеры.

   Для центральных серверов проекта должно быть выбрано оборудование группы Aquarius:
   - количество центральных серверов должно равняться 1;
   - распределение приложений и пользователей по серверам приведено в табл. 3.9.

Таблица 3.9. *Распределение по серверам*

Серверы уровня 1	**Распределение пользователей по серверам**	
	Сервер электронной почты (кол-во клиентов)	**Файловый и принт-сервер (кол-во клиентов)**
Сервер 1	6	6

10. Необходимая конфигурация сервера № 1:
    - тип процессора: обычный;
    - количество процессоров в сервере: 1;
    - объем оперативной памяти (ОЗУ) сервера 384 Мбайт;
    - необходимый объем дискового пространства 18 Гбайт;
    - желаемый тип корпуса: монтируемый в стойку (RackMount);
    - количество линий связи сервера: 1;
    - скорость передачи линии связи должна составлять 10 Мбит/с.
11. Источники бесперебойного питания.

    Требуется обеспечить бесперебойным питанием следующие компоненты компьютерной сети:
    - активное сетевое оборудование;
    - серверы;
    - рабочие станции.

    Для организации бесперебойного питания активного сетевого оборудования и серверов необходимо использовать распределенную систему бесперебойного питания.

    Время работы от батарей должно составлять не менее 7 мин.

Проанализируйте созданный проект, замените операционные системы на те, которые применяются в вашей сети, замените оборудование на доступное вам. У вас получилась заготовка реального проекта, который не трудно, при наличии некоторых знаний компьютерной техники, превратить в настоящий проект, если это необходимо.

Однажды зарегистрировавшись на сайте **www.netwizard.ru**, вы можете пересчитывать свою сеть столько раз, сколько будет необходимо. За это с вас платы не возьмут, кроме платы за время, проведенное в Интернете. Расчет, подобный приведенному ранее, длится около 5 минут. Более сложные задания, возможно, потребуют большего времени. Обращение к такому помощнику избавит вас от большого количества ошибок при разработке сети.

Конечно, для модернизации сети из двух компьютеров при переходе с перекрестного кабеля на подключение через коммутатор не требуется такой объемный проект. Все же, процедура его подготовки занимает немного времени. Попробуйте рассчитать свою сеть с помощью автоматизированного проектировщика. Независимо от вашего желания система предложит вам сеть с сервером, поместит коммутационное оборудование, состоящее из одного коммутатора, в шкаф. И с точки зрения подготовки проекта для офиса или сети в организации она абсолютно права. Для простейшей сети в вашей квартире коммутационный шкаф и сервер пока можно исключить.

Поиск и устранение неисправностей в кабельной сети

Обычно правильно проложенная сеть работает нормально, не вызывая проблем со стороны физического функционирования. Тем не менее, кроме сетевых кабелей по тем же трассам могут проходить множество других проводов. Обслуживанием этих линий занимаются люди, никак не связанные с вашей сетью. При проведении работ по обслуживанию указанных линий или обычных строительных работ компьютерный кабель может быть поврежден. Возможно также неблагоприятное воздействие климатических условий, например, повышенной влажности, на разъемные соединения. Случается это не часто, но при неготовности администратора сети к проблемам подобного рода он может долго ломать голову над причинами неудовлетворительной работы сети, не находя реальных причин.

Рассмотрим ситуации из жизни.

Очевидная проблема

Вот пример проблемы, решение которой удалось найти довольно быстро. В трехэтажном здании, в котором работала компьютерная сеть, проводился косметический ремонт. Сеть простиралась на все три этажа. На первом этаже находился офис, сотрудники которого после выходного дня обнаружили невозможность связи с сервером сети. В выходные дни бригада строителей-отделочников занималась заменой облицовки стен коридора первого этажа. Электрики или телефонисты никаких работ не проводили. Кабель на этом участке сети прокладывался давно и проходил под облицовкой стен. Обход доступных открытых участков сегмента сети ни к чему не привел. Повреждений обнаружено не было. Вскрытие нового участка облицовки стены позволило обнаружить участок кабеля, который был прижат облицовочными панелями к деревянной обрешетке. В результате сильного сжатия была нарушена изоляция жил кабеля. Произошло обычное короткое замыкание. До ожидающейся скорой реконструкции сети решили не менять кабель, а, вырезав поврежденный участок, сделать вставку.

На этот раз проблема была решена оперативно, сеть продолжила работу. Но, вообще говоря, наличие таких вставок, да еще и закрытых для свободного доступа, не рекомендуется. Эти участки в какой-то момент могут проявить себя не с лучшей стороны, когда замыкания не будет, проверка кабеля на обрыв с помощью доступных средств результатов не даст, но сеть будет работать плохо, или вообще работать не будет. Хорошо еще, если эту вставку делали вы сами и знаете о ее наличии.

Проблема менее очевидная

Но бывают ситуации, когда, случайно повредив кабель, работники, не имеющие отношения к компьютерной сети, восстанавливают обрыв собственными силами, чтобы не предавать огласке проблему. Появляются вставки и скрутки, о наличии которых вы не подозреваете. Через некоторое время начинаются жалобы пользователей о проблемах с сетевыми приложениями, "торможении" компьютера при входе в сеть, неожиданных потерях данных при попытке сохранить в сетевой каталог. Работы на линии несколько ранее проводились приглашенным телефонистом, о приходе которого уже успели забыть. Все же это не катастрофический случай. Вы явно видите проблемы в сети. Проведение теста с помощью команды `ping` (верного помощника администратора) должно выявить ухудшение связи. Остается предположить, что есть повреждение, и искать его. К сожалению, оборудование для поиска таких неисправностей достаточно дорого. Есть смысл его приобретать, когда приходится часто иметь дело с прокладкой кабельных линий и поиском неисправностей в них. Некоторые средства для обнаружения проблем на линии могут оказаться у ваших знакомых телефонистов. Портативные генераторы и щупы, применяемые ими, позволяют обнаружить явный обрыв или замыкание. Но в данном случае нет ни того, ни другого. Сеть работает, но плохо. Может помочь прямой осмотр всей линии. Если никаких строительных работ не проводилось, то, скорее всего, причина проблемы обнаружится на открытом участке. На длинном участке с ограниченным доступом к кабелю найти проблемный участок может быть очень трудно. Но, как это бывает в приключенческих фильмах и рассказах, помощь может прийти совершенно неожиданно. Опытным администраторам известно, что плохой контакт при соединении кабеля, а также плохой контакт в разъемном соединении вызывают радиопомехи во время работы сети. Достаточно организовать активный обмен информацией между компьютерами по этому участку сети и пройти по трассе кабеля с портативным радиоприемником. В каком диапазоне хорошо "слушать" помехи, лучше определить экспериментально для вашего приемника, создавая искусственно "повреждение" на экспериментальном участке сети, в виде временного кабеля от коммутатора к компьютеру.

Помехи

Иногда по трассе вашего кабеля прокладываются другие коммуникации. Это могут оказаться силовые кабели высокого напряжения. Обычно такое соседство мешает при протяженности сетевого кабеля более 20 метров. Если сеть новая, и кабель только предполагается укладывать, необходимо рассмотреть все возможные варианты маршрута кабеля, чтобы исключить соседство с силовыми кабелями и в настоящем, и в будущем. Но это удается не всегда. В какой-то момент соседом вашего кабеля может оказаться силовой кабель.

Если это повлияло на работу сети, то лучший выход из положения — проложить кабель по новому маршруту. Иногда новый маршрут не настолько удобен, как старый, но зато безопасен.

Вот небольшая невымышленная история из жизни реально работающей 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 несложно 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 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 когда был подключен осциллограф 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 та 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 ценой 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...

Вот так. Иногда сведения из соседних областей знаний помогают решить не совсем стандартные задачи. Но сообразительность и логические выводы не помогут решить проблемы, если нет материальных средств для их осуществления.

Инструменты, материалы и оборудование

К таким средствам можно отнести инструменты, материалы, оборудование, необходимое для выполнения работ, связанных с ремонтом кабельных линий. Далее приведено описание самых необходимых инструментов, материалов и оборудования, которое реально помогало при поиске неисправностей в сети.

Кабель "витая пара" — основной материал при создании и модернизации сети. Неэкранированная витая пара (рис. 3.11) или кабель UTP (Unshielded Twisted Pair) представляет собой кабель, состоящий из двух или более пар скрученных между собой проводников, покрытых изоляцией и заключенных в общую защитную полимерную "рубашку". Каждый проводник в таком кабеле имеет свою уникальную расцветку и номер. Маркировка кабеля обычно содержит сведения о его категории "CATEGORY 5 UTP".

Подключение кабеля к концентраторам и компьютерам осуществляется через разъемы RJ-45. Внешний вид этих разъемов представлен на рис. 3.12.

Для закрепления коннекторов на конце кабеля требуется специальный обжимной инструмент. Такие приспособления выпускаются различными фирмами и могут иметь какие-либо особенности, но в любом случае этот инструмент будет похож на изображение рис. 3.13. Это важнейший из инструментов. Без него невозможно восстановить линию, имеющую кон-

нектор хотя бы на одном конце, если необходимо заменить или добавить такой кабель. При отсутствии подобного инструмента придется обращаться к помощи специалистов, имеющих его, но их помощь обычно не бесплатна.



Рис. 3.11. Кабель "витая пара"

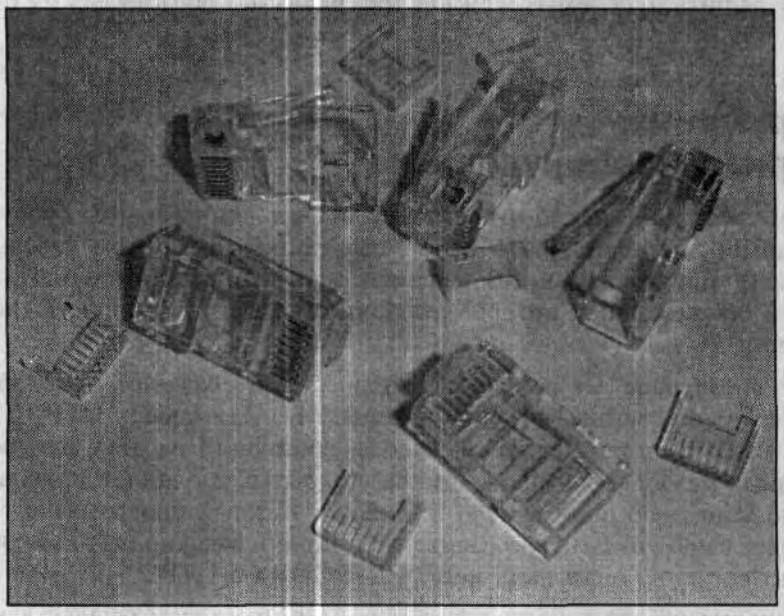


Рис. 3.12. Разъемы RJ-45

В целом ряде случаев кабель оканчивается не разъемом, а розеткой.

Компьютерные розетки выпускаются в самых разнообразных вариантах внешнего оформления, а часто и внутреннего устройства. Они могут отличаться способом крепления жил кабеля к контактам розетки. Иногда для

крепления жил приходится применять дополнительные приспособления — ключ KRONE, например (рис. 3.13). Но при незначительном числе розеток, что обычно имеет место при ремонте, можно обойтись и подручными средствами — отверткой, например, с тонким жалом.

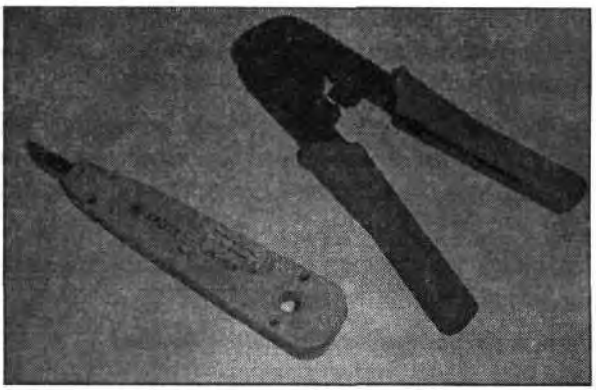


Рис. 3.13. Обжимной инструмент

Часто встречающийся тип розетки изображен на рис. 3.14.

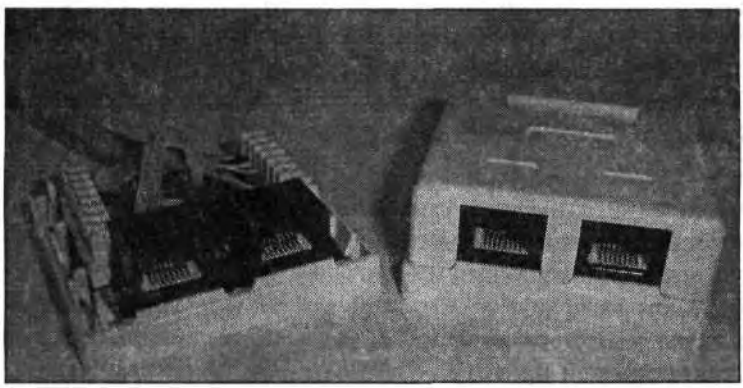


Рис. 3.14. Розетка

Восстанавливая подключение, при необходимости замены коннектора или розетки обязательно запишите порядок подключения жил кабеля. Существует, конечно, стандарт для распайки кабеля в разъемах и розетках, но нередки случаи, когда соединения выполнялись без соблюдения стандартов. Ведь для работоспособности кабеля важно только соблюсти пары сигнальных жил. Одна пара должна соединять контакты 1 — 1, 2 — 2, а другая 3 — 3,

6 — 6. Номера контактов на розетках обычно нанесены с внутренней стороны, а на коннекторах начало отсчета номеров контактов слева, если разъем держать контактами кверху и к себе.

Для определения повреждений кабеля можно использовать приспособления, применяемые телефонистами. Генератор и щуп, который определяет наличие сигнала генератора в проводе, позволяют находить линии с обрывом или замыканием. Возможно применение "прозвонок", которые изготавливают для себя электрики-слаботочники и телефонисты.

Есть специализированное оборудование для тестирования кабельных соединений в ЛВС. Но в обычной практике администрирования сети можно обойтись и без него. Впрочем, если вам его предложат бесплатно — отказываться не стоит.

По следующим ссылкам вы можете найти дополнительную информацию о монтаже разъемов на кабель.

- **http://www.pkinform.ru/newspaper/2004/06/rj45.html**
- **http://cad.ntu-kpi.kiev.ua/~netlib/Nets/RJ45**
- **http://www.ixbt.com/comm/lanfaq/1422.html**

Дополнительная информация о кабельной сети в квартире есть по ссылке

http://www.smart-house.ru/raschet/tip2.php

Там вы увидите сеть, предназначенную не только для компьютеров, но и для различной электронной техники, требующей кабельных коммуникаций. Она предназначена для создания "Умного дома". Эта тема в последнее время все более интересует состоятельных людей. Есть фирмы, которые по заказам населения создают такие "дома" в квартирах или коттеджах.

Наша тема — сеть компьютерная, в которую при желании можно включить любое оборудование, которое может работать в сети. Во всяком случае, если вы начнете основательно проводить кабельные коммуникации в квартире, предусмотрите по одному лишнему порту на каждом рабочем месте. Это позволит в будущем включать в сеть дополнительные устройства. В офисной сети дополнительный порт на рабочем месте может использоваться для подключения телефона или принтера с встроенным принт-сервером.

Неисправности в физической сети и их устранение

Анализируя собственный опыт работы в сети, прихожу к выводу, что описать все возможные неисправности почти невозможно. Разнообразие типов оборудования и способов прокладки кабеля, различные местные условия

могут приводить к неисправностям, возможность появления которых заранее трудно было бы предугадать.

Тем не менее, можно выделить некоторый круг "стандартных" проблем, которые возникают в работе администратора в связи с эксплуатацией физической сети.

Довольно полно эти проблемы оказались описаны в письме одного из начинающих администраторов, который работает сразу с двумя сетями. В вашей сети проблемы могут быть очень похожи на те, что возникли у этого администратора. Имена и адреса в этом письме удалены, незначительно отредактирован текст. Некоторые проблемы выходят за рамки физических, но это и понятно. Физическая сеть существует не ради себя самой, а для обеспечения работы программ на ее компьютерах.

Вопросы начинающего администратора

1. Есть ЛВС. Сервер Windows 2003 Server SP1. Клиенты Windows XP Pro SP2 (Celeron 1700/128). Используется коммутатор DLink DES 1226G. При обмене информацией между компьютерами происходят потери данных 18—20%. Перезагрузка сервера и компьютеров не помогает. Укажите, пожалуйста, возможные ПРИЧИНЫ этого.
2. Есть сеть из 40—50 компьютеров. ОС Windows 2000, Windows XP или Windows 98. С одного на другой компьютер отправляют письмо программой The Bat!, но ОНО НЕ ДОХОДИТ ДО АДРЕСАТА. Почему? Укажите, пожалуйста, возможные ПРИЧИНЫ этого.

Ответы

Для подробного анализа причин ваших проблем недостаточно информации. Поэтому анализ проблем и рекомендации по их устранению будут носить общий характер.

По **первому вопросу** существует несколько вариантов причины проблемы и, соответственно, несколько вариантов ее устранения.

1. Вы не указали основные характеристики сети. Скорее всего, это витая пара. Причем возможно, что все или отдельные линии (сегменты) выполнены четвертой категорией кабеля, который не поддерживает 100 Мбит. Для поддержки 100 и даже 1000 Мбит должен быть кабель не хуже UTP 5E.
2. Возможно, что был некачественно выполнен обжим коннекторов. Иногда при самостоятельном обжиме путают жилы кабеля. Необходимо, чтобы

парам контактов с номерами 1 и 2, 3 и 6, 4 и 5, 7 и 8 соответствовали скрученные пары проводников с одинаковым распределением их цвета с обеих сторон кабеля.

3. Возможны скрутки кабеля (не хватало длины, например), что неблагоприятно сказывается на его работе, особенно при небрежном их выполнении.
4. Возможно, что превышена длина сегментов (100 м).
5. Возможны проблемы с самим коммутатором. Это самый неприятный вариант, но будем надеяться, что он не подтвердится.
6. Возможно, что требовалась скорость 1000 Мбит, а сетевые карты не поддерживают этот режим (как вариант, возможно, что требовалась скорость 100 Мбит, а сетевые карты не поддерживают этот режим).

Для выяснения истинных причин проблемы требуется диагностика сети.

Диагностика и устранение неисправностей:

1. Выбираем плохо работающую линию. Современные сетевые адаптеры обычно могут автоматически определять скорость связи в линии и подстраиваться под нее. Перенастройте порт коммутатора на скорость 10 Мбит или убедитесь, что он был настроен на 1000 Мбит, и перенастройте на 100. Процедура настройки через Web-интерфейс должна быть описана в документации к коммутатору. Если у вас нет инструкции для вашего коммутатора, вы можете ее получить по адресу в Интернете (**ftp://ftp.dlink.ru/pub/Switch/DES-1226G/Description/**).

   После выполнения настройки проверяем качество связи. Если заработало на 100 Мбит, то проблема решена. Если заработало на 10 Мбит или не заработало совсем, проверяем дальше.
2. Исключаем коммутатор из сети. Отключаем от него два кабеля — тот, что идет от сервера, и от одной рабочей станции. Естественно, что в это время сеть работать не будет или будет работать неправильно. Если сервер отключать от сети нельзя, то выберите две рабочие станции, кабели от которых приходят к коммутатору. Берем сдвоенную наружную розетку и соединяем контакты ее гнезд так, чтобы получить перекрестное соединение между компьютерами, включенными через нее (1 — 2, 2 — 1, 3 — 6, 6 — 3, остальные один к одному). Включаем в нее вынутые из гнезд коммутатора кабели и проверяем связь. Если заработало на 100 Мбит (определяется по состоянию подключения), то проблема, вероятнее всего, в коммутаторе.
3. Если не заработало, переключаем сетевые адаптеры на 10 Мбит (в свойствах) и проверяем качество связи. Если заработало, то просматриваем качество кабеля (возможно, что надо заменить четвертую категорию на пятую) и качество обжима, пробуем переобжать кабели. Снова проверя-

ем. Если заработало, снова включаемся через коммутатор — должно работать. Если работает на 10 Мбит и нет возможности в данное время заменить кабель или переобжать его, временно переводим сеть на 10 Мбит, перенастроив все задействованные порты коммутатора, до устранения *причин*.

4. Если без коммутатора все работает, а настройки коммутатора не приводят к положительному эффекту, то перезагружаем коммутатор (скорее всего это вы уже делали). Если не работает, пробуем поменять его на любой самый дешевый. Убеждаемся, что все заработало и отправляем в ремонт не самый дешевый или пробуем сначала найти последнюю прошивку для него (**ftp://ftp.dlink.ru/pub/Switch/DES-1226G/Firmware/**).
5. Если не на всех линиях наблюдается проблема, то перед всем описанным ранее пробуем переключить дефектные линии на другие порты коммутатора и смотрим на результат. Возможна неправильная работа отдельных портов.
6. Если есть очень длинные сегменты, следует в разрыв такого сегмента включить дополнительный хаб или коммутатор в качестве усилителя (повторителя). К нему можно будет подключать дополнительные линии, если позволяет общая топология.

Надеюсь, что по этим общим рекомендациям вам удастся решить вашу проблему.

Второй вопрос также требует уточнения, но и здесь попытаемся определить направления наших действий.

1. Конкретно о The Bat! много не скажу, но разберемся в проблеме в целом. Почта требует наличия сервера. Его расположение не имеет значения, особенно для внутренней почты. Почтовый сервер состоит из двух серверов (программно) — SMTP, через который отправляем почту, и POP3 — через него почту получаем. (Есть и другие протоколы, но остановимся на этих, как самых распространенных.) Функции данных серверов могут выполняться множеством программ, в том числе и The Bat!. Но эта пара серверов должна быть в сети ОДНА. Иначе трудно будет настроить обмен.
2. Можно настроить работу почтового сервера для локальной сети с помощью бесплатной программы Courier Mail Server v.1.56 (**http://courierms.narod.ru/**).
3. Для успешной работы почтового сервера должна работать служба имен в сети, чтобы можно было по сетевому имени обращаться к почтовому серверу. Клиенты смогут отправлять и получать письма при определенных настройках программы не только между собой, но и через Интернет. Ес-

ли в качестве почтового сервера используется The Bat!, то все сказанное ранее верно, но описание настроек придется искать самостоятельно. Courier Mail Server подробно описан на сайте и в help по программе.

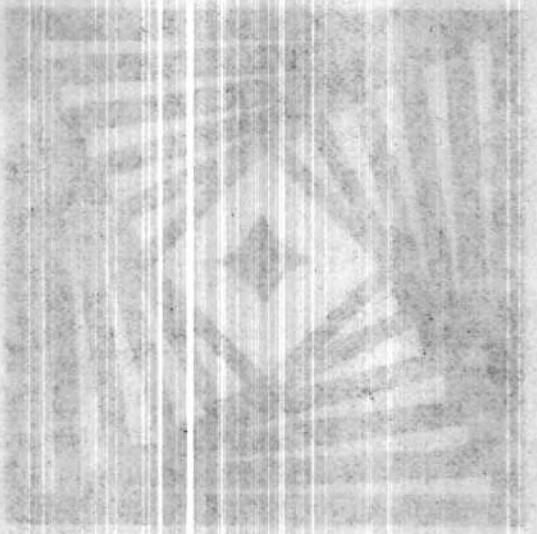
4. Для сети Windows 2003 Server вы можете настроить встроенный в эту систему почтовый сервер. Это лучшее решение для небольшой сети. В моей сети более 50 компьютеров и почта настроена именно так. Если есть реальный IP-адрес в Интернете, то можно, зарегистрировав доменное имя, заставить этот сервер быть и внешним, и внутренним (так у нас — без наворотов и надежно). Если связь требуется между двумя компьютерами, то все сказанное ранее остается в силе. Один компьютер должен выполнять функции сервера и клиента, а другой только клиента. Но The Bat! не всегда лучшее решение. Еще одна интересная ссылка — **http://spsmtp.net.ru/**. Это бесплатный SMTP-сервер для персонального компьютера. Установить его можно на любом компьютере сети.

По приведенному примеру вопросов и ответов видно, что для получения конкретного ответа на вопрос его необходимо формулировать как можно более конкретно, обязательно приводя дополнительные сведения о сети, которые имеют или могут иметь отношение к проблеме. Все же и при недостаточно четкой формулировке вопроса вы можете получить ответ на него, написав письмо по адресу **braginsky@comail.ru** либо задав его на сайте **www.okobox.narod.ru**.



ЧАСТЬ II

РАБОТА В ОДНОРАНГОВЫХ СЕТЯХ



Иметь физическую структуру сети, это не значит действительно иметь работающую сеть. Подключенные к сети компьютеры и другое оборудование должны быть настроены для работы в сети. В небольших сетях компьютеры с ОС Windows могут настраиваться с помощью программ-мастеров, имеющихся в самой операционной системе. Но эти программы позволяют провести настройки лишь в некоторых стандартных ситуациях. Любое отклонение условий задачи от стандарта приведет к невозможности настройки с помощью программы-мастера. Это значит, что думать надо самостоятельно. При этом результаты нашей работы могут быть существенно интереснее, чем результат автоматической настройки.



Глава 4

Настройка рабочих станций для работы в сети

Размеры сети почти не влияют на процедуры настройки этой сети. Другое дело, что в очень маленьких сетях могут не применяться какие-либо протоколы и методы работы. Для двух рядом стоящих компьютеров незачем организовывать связь по защищенному виртуальному каналу. Но организовать такую связь можно. Примеры, приведенные в книге, выполнены либо на основе реально работающих сетей, либо на основе минимально возможной конфигурации сети. Вам решать, применять описанные настройки или нет. Все зависит от конкретной ситуации.

Общие ресурсы

Общие ресурсы, это данные или программы, доступные всем пользователям сети. В общем случае к ним можно отнести и общие ресурсы Интернета, например, программу ICQ2GO (**http://www.icq.com/icq2go**), которая загружается на компьютер пользователя каждый раз, когда это необходимо (пейджер ICQ, доступный в виде Web-страницы или Java-программы). А данные с сервера ICQ доступны для пользователей любой версии программы. Но это Интернет. Нас пока интересуют общие ресурсы в одноранговой локальной сети. Наиболее часто используются общие ресурсы в виде файлов, доступных для всех или для части пользователей, а также общее подключение к Интернету. Несколько реже требуется доступ к рабочему столу рабочей станции. Это может быть необходимо для запуска программ, которые установлены только на этой рабочей станции или в целях администрирования.

Для того чтобы рабочие станции были доступны в сети, их необходимо, во-первых, соответствующим образом настроить, а во-вторых, входя в систему, обязательно авторизоваться. Последнее замечание имеет отношение в основном к ОС Windows 98, где возможно войти в систему, отменив ввод сетевого пароля.

Настройка Windows XP

Для начала убедитесь, что учетная запись администратора и учетная запись пользователя имеют пароли. Работая в сети без пароля, вы подвергнете компьютер опасности непрошенного вторжения со стороны сети.

Если ваша рабочая станция еще не работала в сети, то необходимо подготовить ее для работы в составе рабочей группы. Даже при наличии всего двух компьютеров в вашей сети они должны принадлежать некоторой рабочей группе. Это необходимо для того, чтобы компьютеры сети были видны в сетевом окружении и вам не приходилось их искать, используя средства поиска компьютеров, запоминая имена или IP-адреса.

Откройте **Панель управления | Система** на вкладке **Имя компьютера** (рис. 4.1).

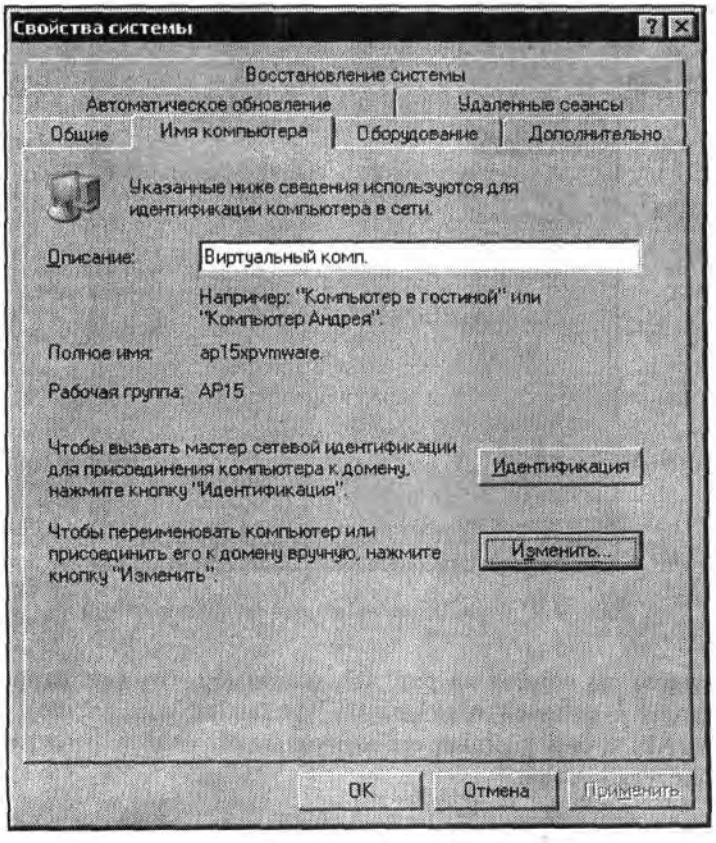


Рис. 4.1. Окно **Свойства системы**, вкладка **Имя компьютера**

Нажмите кнопку **Изменить**. Откроется окно **Изменение имени компьютера** (рис. 4.2).

В поле **Имя компьютера** необходимо ввести то имя, под которым ваш компьютер должен быть виден в сети, а в нижней части этого окна нужно указать, что компьютер является членом рабочей группы, и ввести ее имя. По умолчанию система предлагает имя WORGROUP или MSHOME. Если вы думаете, что в сети будет общий доступ к Интернету или позднее будет организована связь с другими сетями, то лучше изменить это имя. Если сеть будет состоять из нескольких рабочих групп, то имя должно содержать признак рабочей группы, например, номер подразделения, номер квартиры и т. п. Имя компьютера тоже должно быть информативным.

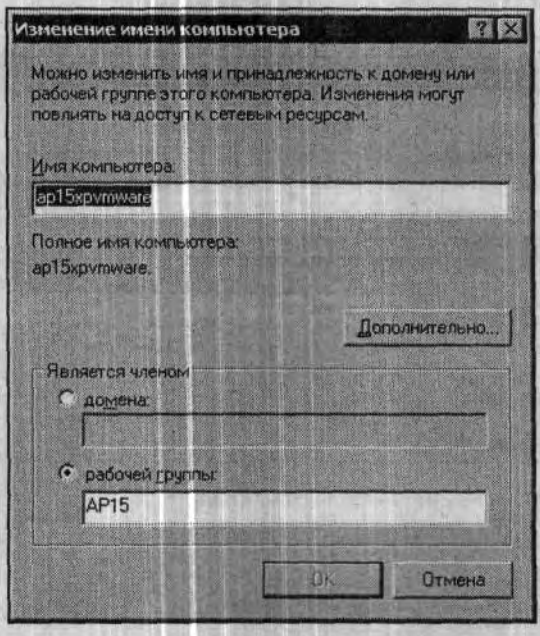


Рис. 4.2. Окно **Изменение имени компьютера**

То имя, которое вы видите на рис. 4.2, например, говорит о принадлежности компьютера к рабочей группе ap15, сообщает, что на нем установлена ОС Windows XP, а сам компьютер виртуальный, создан в виртуальной машине VMware Workstation.

Примечание

VMware Workstation — это программа, которая позволяет на своем компьютере или на сервере создать еще один или несколько компьютеров с одинаковыми

или различными операционными системами. Зарегистрировавшись на сайте программы (**http://www.vmware.com/vmwarestore/newstore/wkst_eval_login.jsp**), вы можете получить ее пробную версию (объем файлов более 50 Мбайт). На русском языке о программе VMware можно почитать по адресам **http://onix.opennet.ru/content/category/4/13/26/** и **http://www.computerra.ru/softerra/36340/**. Для виртуальных компьютеров только на основе Windows может быть использована виртуальная машина Microsoft Virtual PC 2004 (**http://www.microsoft.com/windows/virtualpc/default.mspx**). Эта программа также доступна в пробной версии.

Для сети не имеет значения, виртуальный компьютер подключается к ней или реальный. Все настройки для этих компьютеров идентичны.

Теперь откройте **Панель управления | Сетевые подключения** (рис. 4.3).

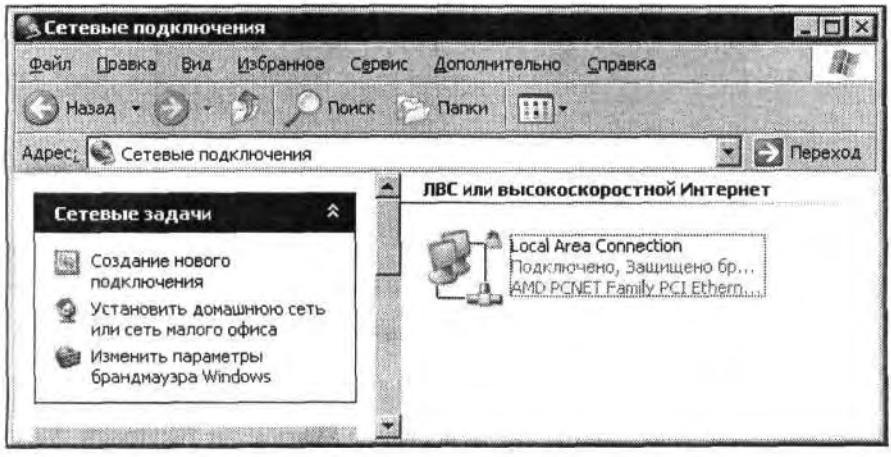


Рис. 4.3. Окно **Сетевые подключения**

В различных версиях Windows имя подключения может быть написано по-русски или по-английски. В данном случае мы видим `Local Area Connection`, что соответствует наименованию в полностью локализованной версии Windows XP — `Подключение по локальной сети`. Но нас не очень устраивает такое имя подключения. Позднее нам придется управлять подключениями из командной строки, где имена с пробелами надо помещать в кавычки, а русские буквы в отдельных случаях не читаются. При таком способе управления удобнее пользоваться наименованиями из одного слова и лучше латинскими буквами. Поэтому давайте переименуем наше сетевое подключение. Можно, как и в имени компьютера, применить осмысленные обозначения. Например, можно этому подключению дать имя `LocalConn15`. Теперь откройте свойства данного подключения (рис. 4.4).

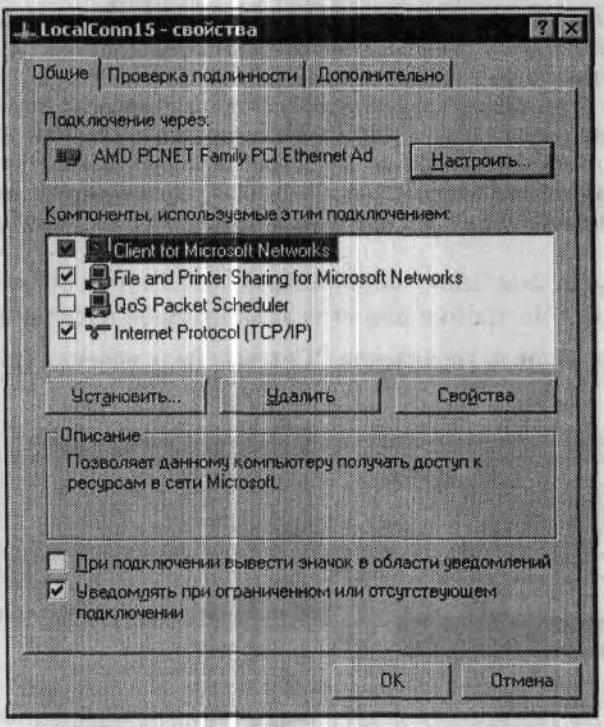


Рис. 4.4. Окно **LocalConn15 - свойства**

Необходимо поставить галочки напротив **Client for Microsoft Networks** (Клиент для сетей Microsoft) и **File and Printer Sharing for Microsoft Networks** (Служба доступа к файлам и принтерам для сетей Microsoft).

Также следует поставить галочку и напротив **Internet Protocol (TCP/IP)** (Протокол Интернета TCP/IP). Но кроме галочки для этого пункта необходимо установить свойства, доступ к которым открывается после нажатия кнопки **Свойства** (рис. 4.5).

Примечание

Если какого-либо протокола нет в перечне, то нажмите кнопку **Установить** и добавьте его в список.

По умолчанию это окно выглядит так, как показано на рис. 4.5. Операционная система сама будет назначать компьютеру IP-адрес. Вернитесь к окну **Сетевые подключения** и проверьте IP-адрес для подключения `LocalConn15`.

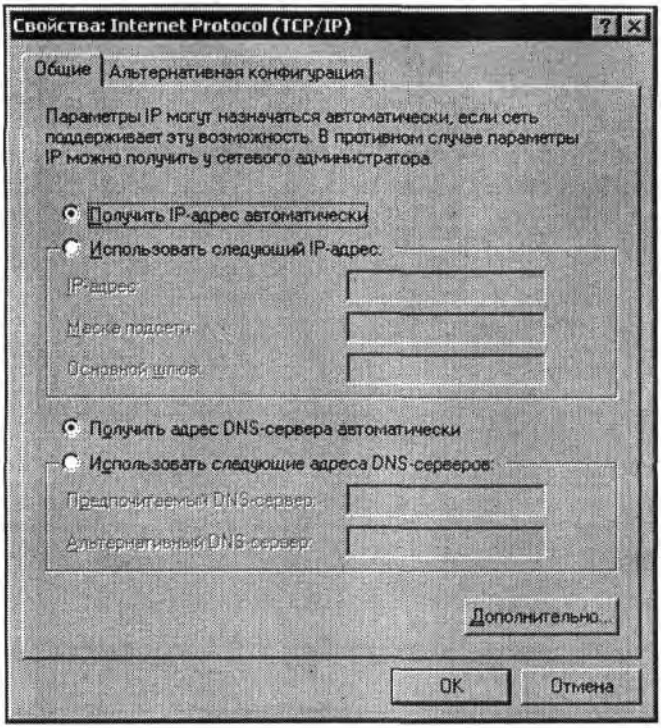


Рис. 4.5. Окно **Свойства: Internet Protocol (TCP/IP)**

Примечание

Вы можете использовать свои наименования объектов, поэтому следите за сопоставлением объектов в книге и ваших реальных объектов.

Для того чтобы проверить IP-адрес, присвоенный подключению, можно открыть окно **Состояние**, выбрав в контекстном меню этого подключения пункт **Состояние** (рис. 4.6).

IP-адрес, который вы увидите в этом окне, может иметь различные значения, зависящие от того, в какую сеть вы включили компьютер. Возможно, что IP-адрес не будет присвоен, если компьютер еще не включен в сеть. В любом случае, для первых компьютеров сети (а мы сейчас настраиваем самый первый компьютер, и других в сети просто нет) мы назначим адреса самостоятельно. Возможны различные соображения по распределению адресов в сети, поэтому мы не будем останавливаться на вопросе, почему выбран именно такой или другой IP-адрес. Вы можете назначить этот адрес почти произвольно. Но для уверенности в том, что дальнейшие опыты будут удачны, рекомендую назначить адрес из диапазона 192.168.1.2—192.168.1.254.

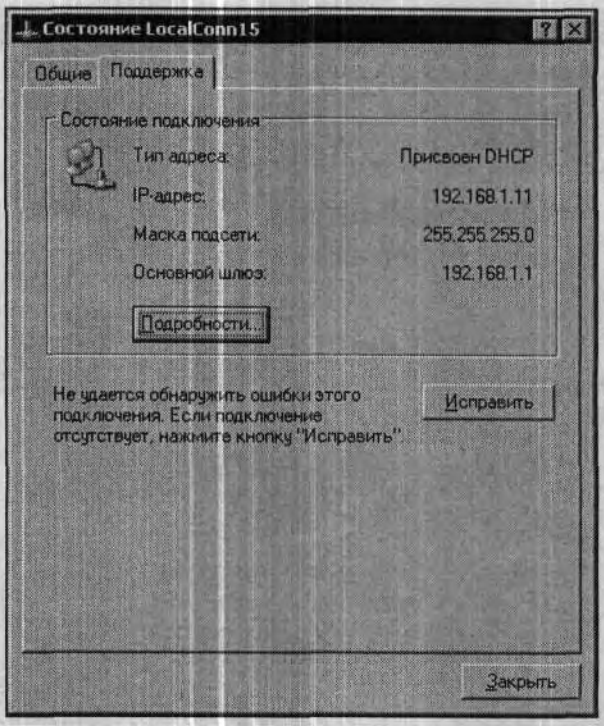


Рис. 4.6. Окно **Состояние LocalConn15**

Если вы изберете другой диапазон, пригодный для локальной сети, то все будет также работать, но в примерах книги будут адреса именно из этого диапазона.

Для того чтобы самостоятельно назначить IP-адрес, в окне свойств подключения отметьте опцию **Использовать следующий IP-адрес** и в поле IP-адреса введите его значения. В нашем примере это будет 192.168.1.101. Маску подсети при этом можно указать 255.255.255.0, а шлюз пока не указывать совсем. Именно эти значения вы теперь увидите при проверке состояния подключения.

Примечание

В окне состояния подключения на вкладке **Поддержка** есть кнопка **Подробности**. Среди сведений, которые открываются при нажатии этой кнопки, есть физический адрес сетевого адаптера.

Остается установить общий доступ к какому-либо каталогу, чтобы завершить первый этап настройки рабочей станции для работы в сети. Лучше всего на роль общедоступного каталога подходит каталог **Общие документы**.

Windows XP создает для каждого пользователя папку документов. Дополнительно автоматически создается папка **Общие документы**, доступная всем пользователям. Откройте окно свойств этого каталога (рис. 4.7). Поставьте галочки напротив пунктов **Открыть общий доступ к этой папке** и **Разрешить изменение файлов по сети**.

Вы можете создать любое необходимое число каталогов с доступом по сети. Причем, в отличие от папки **Общие документы**, вы сможете назначать произвольные сетевые имена каталогов.

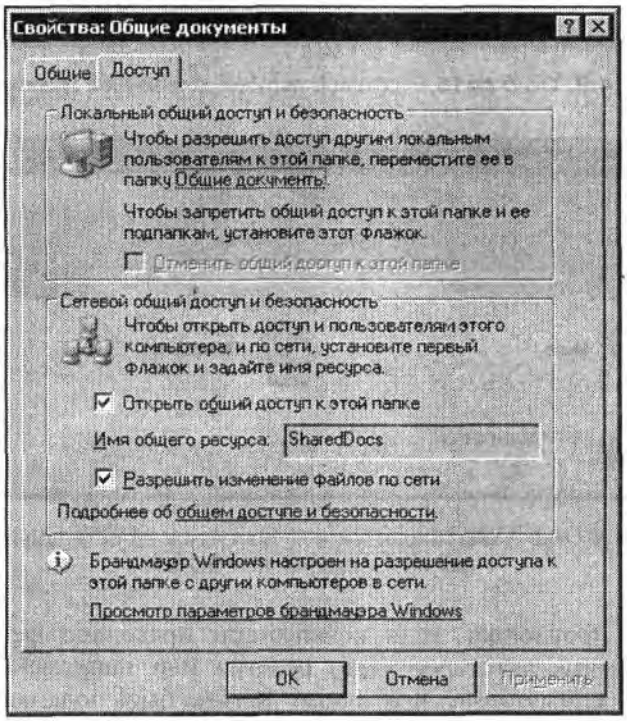


Рис. 4.7. Окно **Свойства: Общие документы**

Теперь остается повторить все настройки на втором компьютере сети. Подключая второй ПК, не забудьте, что IP-адреса компьютеров и имена должны быть уникальными. Второму компьютеру можно назначить IP-адрес 192.168.1.102, а имя — любое, на ваше усмотрение. Теперь, открыв сетевое окружение с любого из этих компьютеров, мы должны увидеть там их оба (рис. 4.8).

Откройте тот ПК, который является для вас удаленным. Вы увидите доступные по сети ресурсы этого компьютера (рис. 4.9).

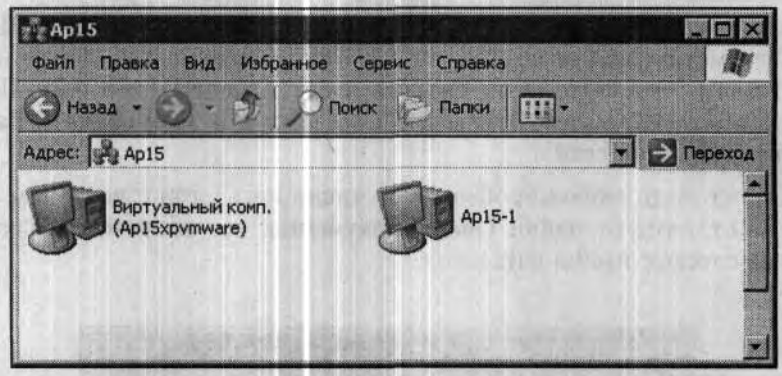


Рис. 4.8. Окно **Ap15** — сетевое окружение рабочей группы Ap15

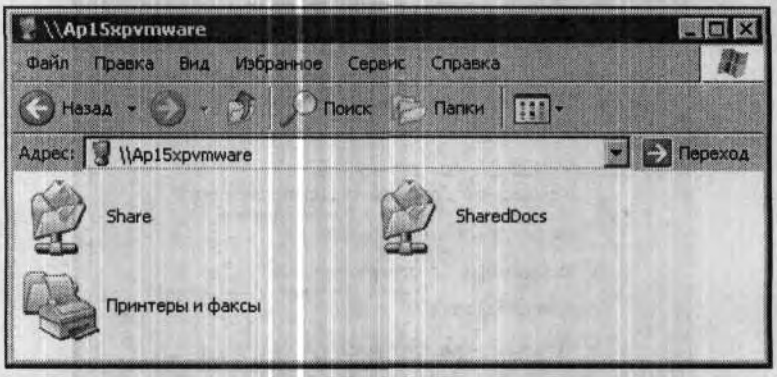


Рис. 4.9 Окно **\\Ap15xpvmware** — доступное по сети содержимое первого сетевого компьютера

Конечно, это произойдет, если компьютеры правильно включены в сеть. Кабели от сетевых адаптеров через розетки или напрямую должны быть подключены к коммутатору, к которому должно быть подключено питание.

Если не заработало

Вполне возможно, что результат не получился. В чем может быть проблема? Схема нашей сети проста (рис. 4.10).

Поэтому проанализировать ситуацию и найти причину не сложно. Но для начала попробуем сделать диагностику средствами операционной системы. Пока наша сеть не подключена к Интернету и другим сетям, можно отключить брандмауэр, который встроен в ОС Windows XP и по умолчанию включен. Может быть, что он не настроился автоматически, когда вы предостав-

ляли доступ к документам компьютеров, и теперь сигналы к компьютеру не могут пробиться через защиту.

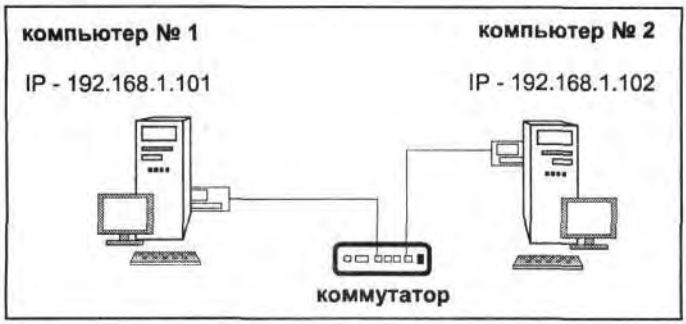


Рис. 4.10. Схема нашей сети

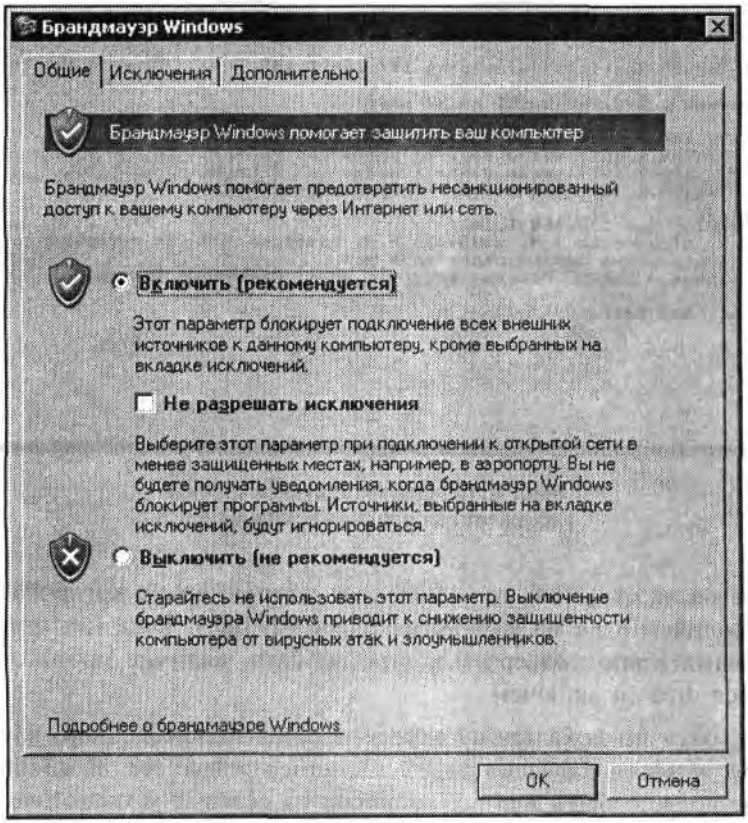


Рис. 4.11. Окно **Брандмауэр Windows**

Настройки брандмауэра находятся в **Панель управления | Брандмауэр Windows** (рис. 4.11).

Отключите брандмауэр, отметив соответствующую опцию, согласившись с тревожными предупреждениями операционной системы. Если сразу после этого все заработало, то на вкладке **Исключения** этого окна установите галочку напротив пункта **Общий доступ к файлам и принтерам**. После этого брандмауэр можно включить и начинать работать с сетью.

Если отключение брандмауэра не помогло, продолжаем диагностику. Откройте командную строку и наберите команду `ping 192.168.1.101`, если вы работаете с компьютером № 2, или `ping 192.168.1.102`, если с компьютером № 1. Результат выполнения команды должен быть подобен тому, что показан на рис. 4.12.

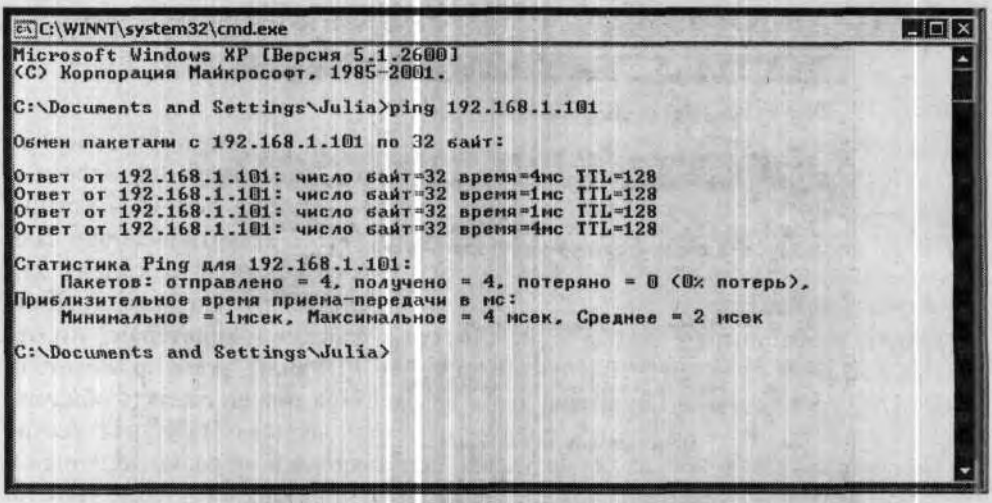


Рис. 4.12. Окно командной строки, результат выполнения команды `ping`

Если ответов на `ping` нет, то делаем тест компьютера, с которого проверяем сеть. Выполняем `ping` на локальный адрес 127.0.0.1. Если нет ответа на этот раз, то внимательно проверяем настройку сети, наличие протокола TCP/IP, убеждаемся, что он включен.

Если `ping`-тест по локальному адресу прошел положительно, то проверяем состояние сетевого адаптера через диспетчер устройств. В диспетчере устройств не должно быть желтых вопросов на сетевых устройствах. Если есть желтые вопросы, то переустанавливаем драйверы сетевого адаптера. Правильно установив верный драйвер, проверяем работу сети.

Если в диспетчере устройств все нормально, `ping` на локальный адрес 127.0.0.1 проходит нормально, то проводим аналогичную проверку на втором компьютере.

Если проблем с оборудованием не обнаружено, кабельную сеть заменяем временными, но заведомо исправными патч-кордами. Если все заработало, то ищем ошибки распределения жил кабелей в коннекторах и розетках. Если не заработало и на этот раз, то проблема в коммутаторе. Переключите кабели на другие порты коммутатора. Если заработало, то внимательно проверьте исправность портов коммутатора и отправьте его в ремонт, если дефект подтвердился. Но бывает, что дефект вызван не полным введением разъемов в гнезда, и при повторной проверке не подтверждается.

Если все заработало, то можно приступать к эксплуатации сети.

Если в сети компьютер с ОС Windows 98

Если в сети применяются рабочие станции с ОС Windows 98, то настройка сети проводится аналогично.

Для настройки сетевых протоколов следует открыть **Панель управления | Сеть**. В свойствах протокола TCP/IP указать требуемое значение адреса и маски подсети. Брандмауэра в этой операционной системе нет. Имя компьютера и рабочей группы устанавливается на вкладке **Идентификация**. Для обеспечения доступа к компьютеру из сети нужно установить клиент для сетей Microsoft и службу доступа к файлам и принтерам. На вкладке **Конфигурация** необходимо нажать кнопку **Доступ к файлам и принтерам**, а в открывшемся окне отметить оба пункта доступа — **Файлы этого компьютера можно сделать общими** и **Принтеры этого компьютера можно сделать общими**. На вкладке управления доступом следует отметить вариант **На уровне ресурсов**. Второй вариант доступа — **На уровне пользователей** — возможен только при наличии сервера, содержащего сведения о пользователях сети. Имена локальных пользователей не помогут получить доступ к ресурсам из сети.

В свойствах каталога на вкладке **Доступ** (рис. 4.13) устанавливаем **Тип доступа** и при необходимости **Пароли** для каждого типа доступа.

Для просмотра текущих настроек сетевого адаптера в Windows 98 можно применить команду `winipcfg`, введя ее в окне **Пуск | Выполнить**. В окне **Конфигурация IP** (рис. 4.14) можно узнать текущие IP- и физический адреса сетевого адаптера, выбранного в поле со списком формы.

Доступ с компьютеров под управлением Windows 98 к компьютерам с Windows XP возможен и в одноранговой сети, и в сети с сервером и установленным каталогом Active Directory. Windows XP позволяет разрешить доступ к каталогу для всех. Но доступ к серверу Windows Server 2003 в одноранговом варианте сети становится возможным только при создании учетных

записей пользователей с совпадающими именем и паролем на системах Windows 98 и Windows Server 2003. Именно под этой учетной записью следует входить в сеть на компьютере с Windows 98, если необходим доступ с него к файлам на компьютере с Windows Server 2003.

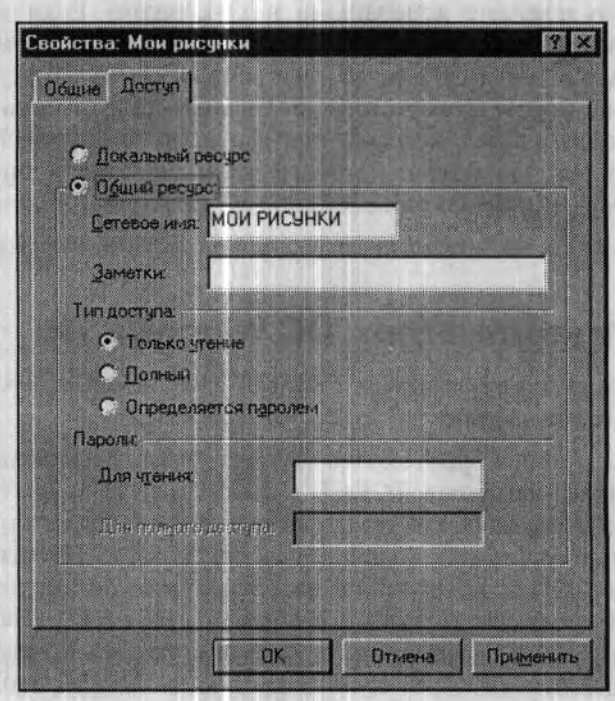


Рис. 4.13. Окно **Свойства: Мои рисунки** (каталог с общим доступом)

Операционная система Windows 98 прекрасно работает в сети с себе подобными машинами. Но в сети с Windows XP, при отсутствии каких-либо серверов имен, позволяющих идентифицировать компьютеры сети, Windows 98 может растеряться. Применяемый в Windows 98 протокол NetBEUI отсутствует в новых операционных системах. В то же время новые возможности работы через TCP/IP не вполне поддерживаются старой ОС. Для того чтобы компьютеры сети видели друг друга нормально, придется установить на рабочие станции с Windows XP протокол NetBEUI.

В Windows XP по умолчанию не поддерживается протокол NetBEUI. Для его установки потребуется диск с дистрибутивом операционной системы. В каталоге <*Буква диска*>:\VALUEADD\MSFT\NET\NETBEUI вы найдете файлы для этого протокола. Для его установки проделайте следующее:

1. Скопируйте файл nbf.sys в папку *%SYSTEMROOT%*\SYSTEM32\DRIVERS\.

2. Скопируйте файл netnbf.inf в папку *%SYSTEMROOT%*\INF\.
3. Откройте окно свойств сетевого подключения и нажмите кнопку **Установить** для того, чтобы добавить протокол NetBEUI.

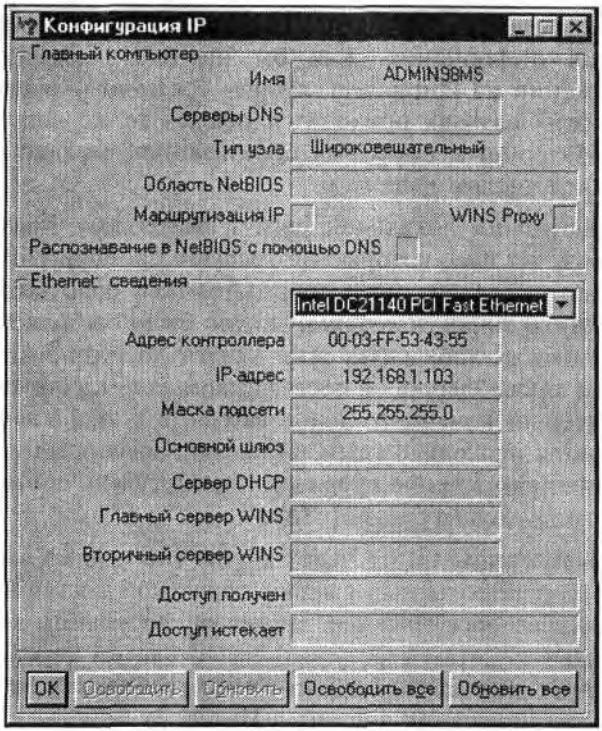


Рис. 4.14. Окно **Конфигурация IP**

Для совместимости со старыми компьютерами, работающими под управлением операционных систем Windows 9*x*, инсталлируйте также драйвер сетевого монитора, который появится в списке протоколов, еще доступных для установки, после добавления файлов протокола NetBEUI.

После добавления NetBEUI на компьютеры с Windows XP в сетевом окружении каждого компьютера сети будут видны все остальные ПК. Будет возможен также и доступ к разрешенным для этого ресурсам компьютеров.

Общее подключение к Интернету

Общие файлы в сети, возможность обмена файлами между компьютерами сети — это уже хорошо. Но практически сразу у вас возникнет вопрос под-

ключения вашей сети к Интернету. На собственном опыте знаю, что появление второго компьютера дома тут же заставило решать вопрос подключения его к Интернету. Тем более такая задача возникнет в сети офисной. Только особые условия работы сети могут запретить подключение к Интернету для рабочих станций, работающих в ней. Такое ограничение существует, например, в банках и других организациях, где по локальной сети передается секретная информация. Как бы ни были совершенны средства защиты от вторжений из Интернета, лучшее средство — отсутствие подключения. Но и в этих случаях приходится решать те же вопросы, поскольку для доступа в Интернет в подобных организациях создают еще одну сеть, правда, с меньшим числом клиентов.

Вариантов подключения локальной сети к Интернету может быть много. Мы рассмотрим те из них, которые не требуют приобретения дополнительного программного обеспечения и дорогостоящего оборудования. Интернет не имеет какой-либо точки, к которой можно было бы подключить кабель и через него выходить в глобальную сеть. Услуги доступа всегда предоставляются некоторым провайдером — поставщиком услуг. Для обеспечения доступа к сети Интернет конечного пользователя, т. е. нас с вами, в настоящее время применяются несколько технологий. Вот некоторые из них, получившие широкое распространение (порядок перечисления соответствует последовательности дальнейшего рассмотрения).

- Доступ по выделенной линии через другие компьютерные сети. Организация, имея широкополосный высокоскоростной доступ к сети Интернет через специальное оборудование, может предоставлять доступ пользователям и локальным сетям через свою сеть по витой паре, проведенной до клиента. В этом случае достаточно иметь свободный сетевой адаптер у компьютера для получения доступа в Интернет. Иногда требуется дополнительное программное обеспечение, применяемое с целью защиты от воровства трафика пользователя злоумышленником из сети.
- Коммутируемый доступ посредством аналогового модема через телефонную линию (dial-up). Для реализации доступа с одиночного компьютера требуется подключить модем к последовательному или USB-порту компьютера (зависит от конструкции модема). Возможно также подключение к недорогому маршрутизатору, который поддерживает работу с модемом, например, DI-824VUP+, к которому в свою очередь должна подключаться рабочая станция.
- Доступ по телефонной линии, но посредством цифрового модема. Наиболее распространен доступ через ADSL-модем, с несимметричной скоростью доступа в направлениях от и к абоненту. ADSL-модемы могут иметь как Ethernet, так и USB-интерфейс для связи с компьютером. Нас в большей степени должен интересовать вариант с Ethernet-выходом. ADSL-модемы могут поддерживать работу в двух режимах (конкретная

модель может поддерживать один из них) — режим моста (bridge) или маршрутизатора (router). Режим моста подходит для подключения к отдельному компьютеру, а режим маршрутизатора позволяет подключать модем к сети, где его смогут использовать несколько компьютеров.

Применение других более редких видов подключения будет аналогично одному из перечисленных вариантов. Отличие может состоять в типах применяемого дополнительного оборудования. Для подключения компьютера потребуется либо последовательный порт, либо USB, либо Ethernet-порт. Рассмотренные далее практические примеры подключений помогут сориентироваться в большинстве случаев.

Доступ по выделенной линии

Этот вариант доступа стал достаточно популярным ввиду высокой скорости соединения с Интернетом и отсутствия необходимости дозваниваться до провайдера. Интернет может быть подключен постоянно. Чаще всего с конечного пользователя взимается плата за использованный входящий трафик или абонентская плата.

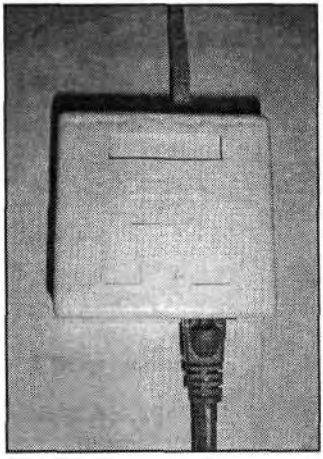


Рис. 4.15. Компьютерная розетка на стене

Кабель, введенный в квартиру, можно аккуратно провести до рабочего места и подключить к розетке, закрепленной на стене (рис. 4.15). С помощью патч-корда к розетке можно подключить сетевой адаптер компьютера или маршрутизатор. В данном примере подключается именно сетевой адаптер. На рис. 4.16 показано подключение к домовой сети квартирной или офисной сети из трех компьютеров.

IP-адрес адаптера, подключенного к кабелю, входящему в квартиру, указан условно, поскольку его должны предоставить поставщики услуги доступа к Интернету. Но вполне возможно, что в вашем случае он тоже будет начинаться с числа 10.

Один из компьютеров сети должен иметь два сетевых адаптера. В данном случае это компьютер № 1. Данный компьютер должен выполнять функции маршрутизатора и шлюза в Интернет для локальной сети. Операционная система Windows XP имеет для этого в своем составе все необходимое.



Рис. 4.16. Подключение к домовой сети

В последнее время для обеспечения лучшей защищенности доступа к Интернету применяют подключение через виртуальный канал. Этот канал соз-

дается в виртуальной сети. Данные сети можно создавать как внутри локальных сетей, так и в Интернете. Принятое в настоящее время общее наименование таких сетей — VPN (Virtual Private Network, виртуальная частная сеть). В Windows XP встроена поддержка работы в виртуальных сетях, соответственно есть возможность создания виртуального сетевого адаптера. Именно этот виртуальный адаптер будет связывать нашу сеть с Интернетом, а реальный (изображенный на схеме) свяжет нашу сеть с локальной сетью поставщика услуги.

Прежде всего, конечно, подключение нужно настроить на компьютере № 1. Этот компьютер имеет два физических сетевых адаптера. На рис. 4.17 показаны три сетевых подключения этого компьютера. Два из них (в нижней части окна) соответствуют реальным адаптерам. Настройка этих подключений должна производиться в соответствии с параметрами квартирной (офисной) и домовой сети. Подключение виртуальной частной сети можно создать с помощью мастера **Создание нового подключения**, который запускается из меню **Сетевые задачи** в левой части окна **Сетевые подключения**.

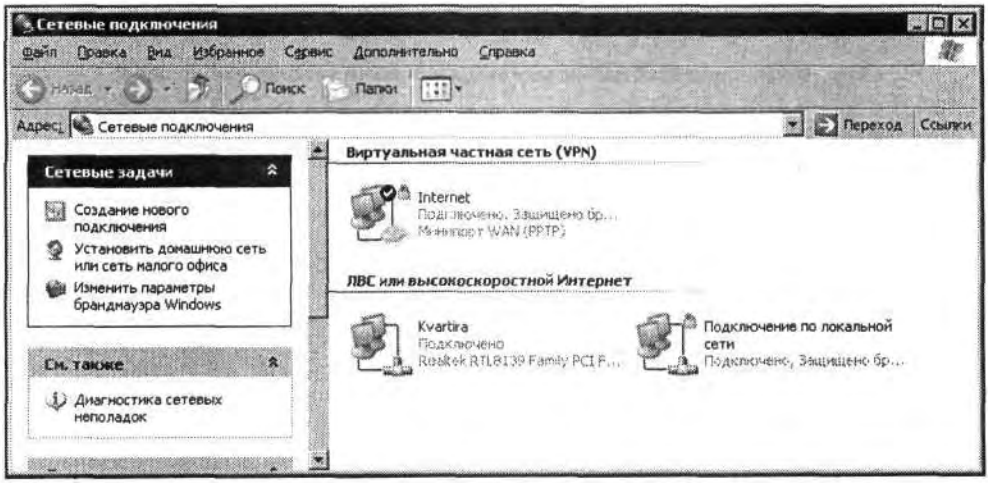


Рис. 4.17. Окно **Сетевые подключения**

Создавая VPN-подключение, мы подключаемся к виртуальной, но уже существующей сети. Причем не просто к сети, а к удаленному компьютеру. Поэтому по ходу работы мастера выбираем **Подключить к сети на рабочем месте** (рис. 4.18).

На следующем шаге выбираем способ подключения (рис. 4.19).

Имя для подключения (рис. 4.20) можно указать совершенно произвольно.

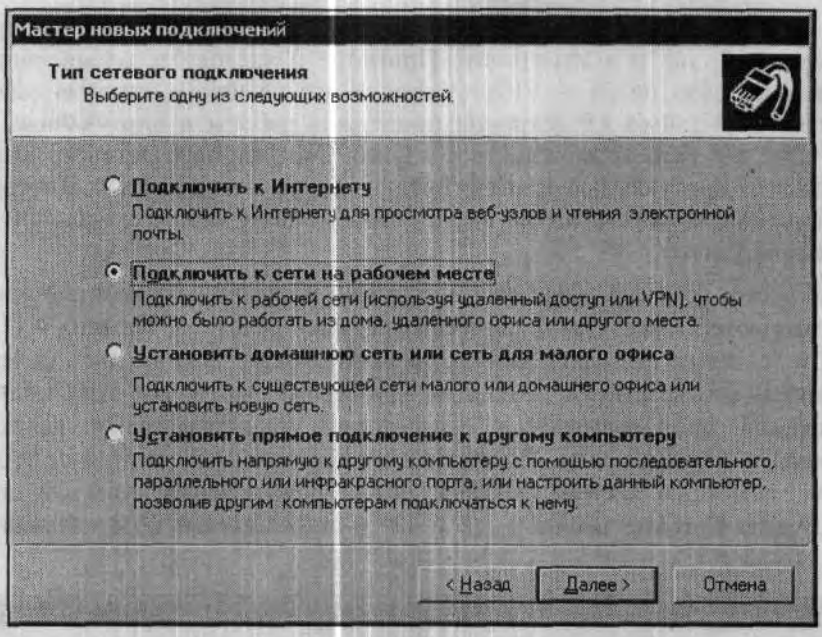


Рис. 4.18. Окно **Мастер новых подключений** (подключить к сети)

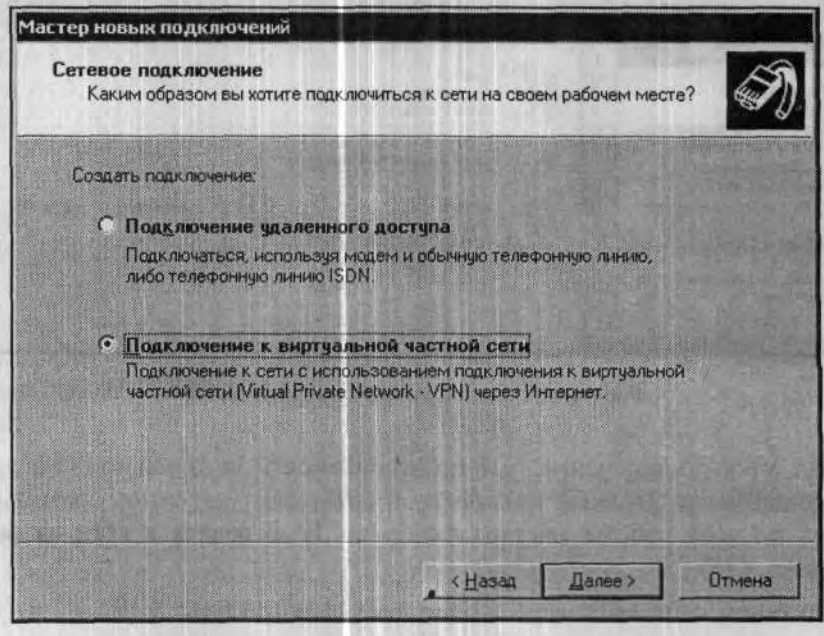


Рис. 4.19. Окно **Мастер новых подключений** (подключение к виртуальной сети)

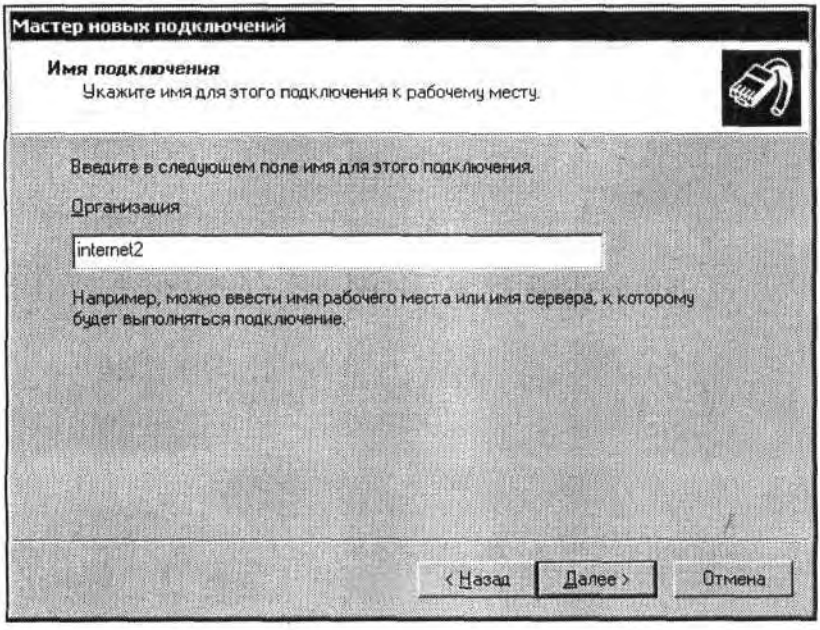


Рис. 4.20. Окно **Мастер новых подключений** (имя подключения)

VPN-подключения и другие подключения к удаленному компьютеру могут требовать предварительного набора номера. Но в нашем случае предварительное соединение уже установлено по локальной сети провайдера. Поэтому выбираем **Не набирать номер для предварительного подключения** (рис. 4.21).

Номер набирать не требуется, но адрес VPN-сервера нужно указать. Этот адрес должен предоставить провайдер (рис. 4.22).

Далее мастер подключений покажет нам окно ввода имени пользователя и пароля, необходимых для подключения к VPN (рис. 4.23).

Данные параметры можно занести сразу или вводить каждый раз при подключении. Учитывая, что этим подключением должны пользоваться другие компьютеры сети, лучше сразу ввести их и отметить опцию **Сохранять имя пользователя и пароль**.

В свойствах созданного подключения скорее всего потребуется указать дополнительные параметры. Для этого, открыв свойства созданного подключения на вкладке **Безопасность** (рис. 4.24), нажмите кнопку **Параметры**. Откроется окно **Дополнительные параметры безопасности** (рис. 4.25). Сведения о необходимых установках предоставит провайдер. На рис. 4.25 показаны типичные параметры для подключения к Интернету.

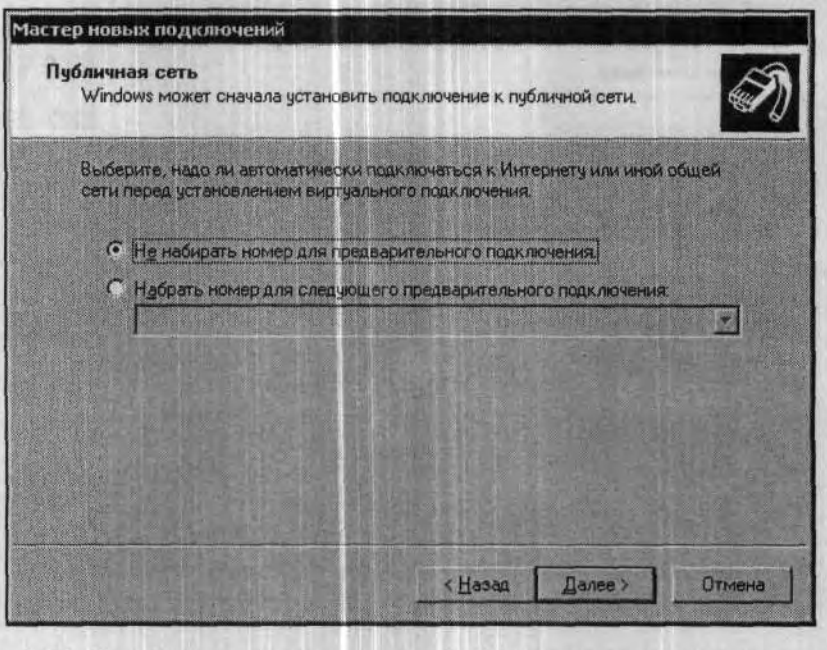


Рис. 4.21. Окно **Мастер новых подключений** (предварительное подключение)

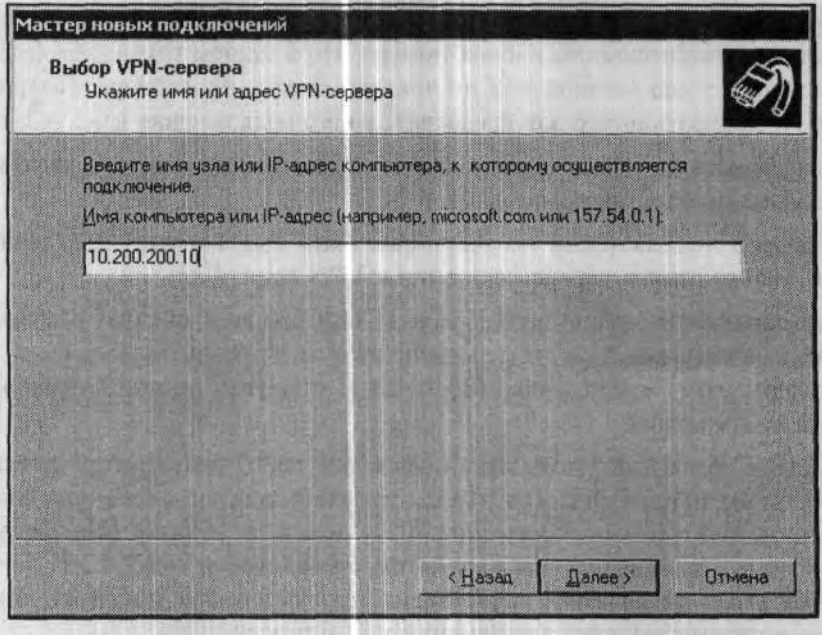


Рис. 4.22. Окно **Мастер новых подключений** (Адрес VPN-сервера)



Рис. 4.23. Окно **Подключение: Internet2**

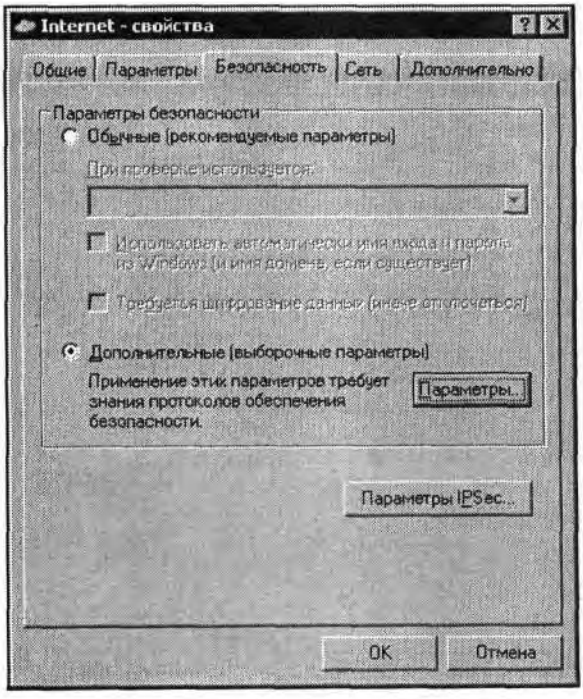


Рис. 4.24. Окно **Internet - свойства**, вкладка **Безопасность**

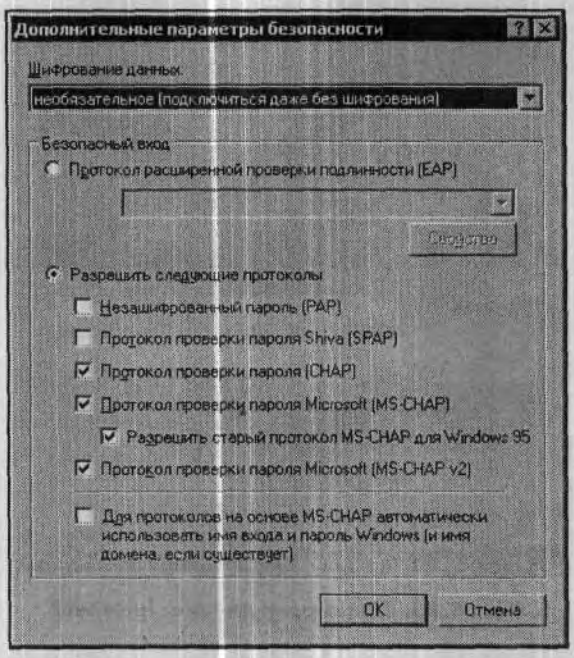


Рис. 4.25. Окно **Дополнительные параметры безопасности**

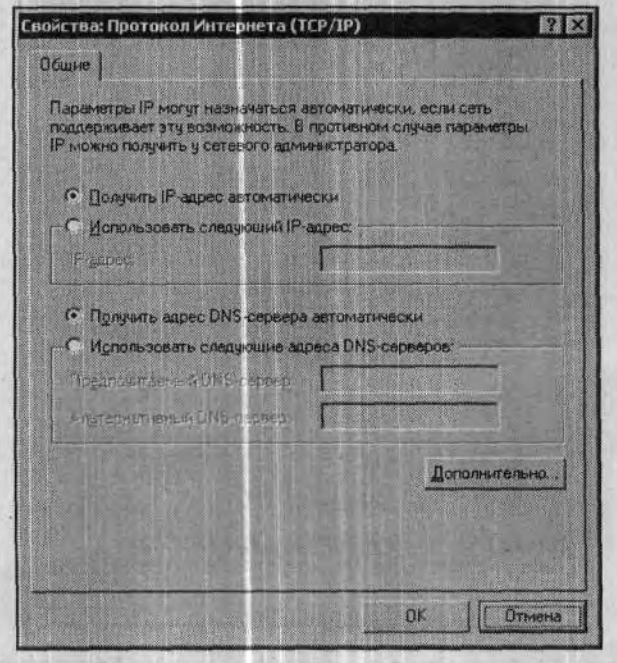


Рис. 4.26. Окно **Свойства: Протокол Интернета (TCP/IP)**

Как и любой другой вид подключения к Интернету, наше подключение использует протокол TCP/IP. В свойствах этого протокола (рис. 4.26) ничего менять не надо — IP-адрес и адрес DNS-сервера получаются автоматически. Но необходимо, нажав кнопку **Дополнительно**, установить дополнительные параметры протокола (рис. 4.27).

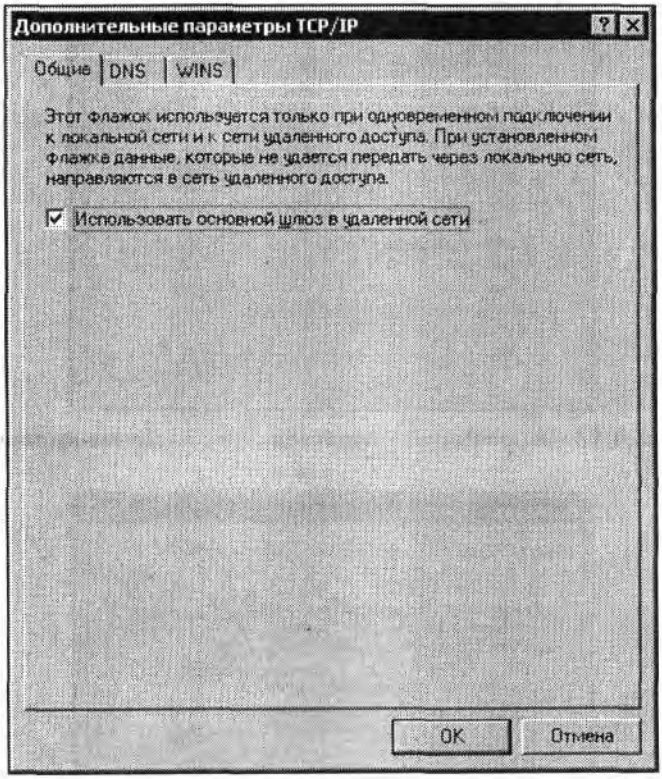


Рис. 4.27. Окно **Дополнительные параметры TCP/IP**

На вкладке **Общие** должен быть установлен флажок **Использовать основной шлюз в удаленной сети**.

Вернувшись к окну свойств подключения, переходим на вкладку **Дополнительно** (рис. 4.28). В этом окне необходимо **Разрешить доступ другим пользователям сети использовать подключение к Интернету данного компьютера**, установив соответствующий флажок. В поле со списком **Подключение домашней сети** нужно выбрать подключение, которое ведет к квартире или офису, но не к домовой сети (сети провайдера) (рис. 4.29).

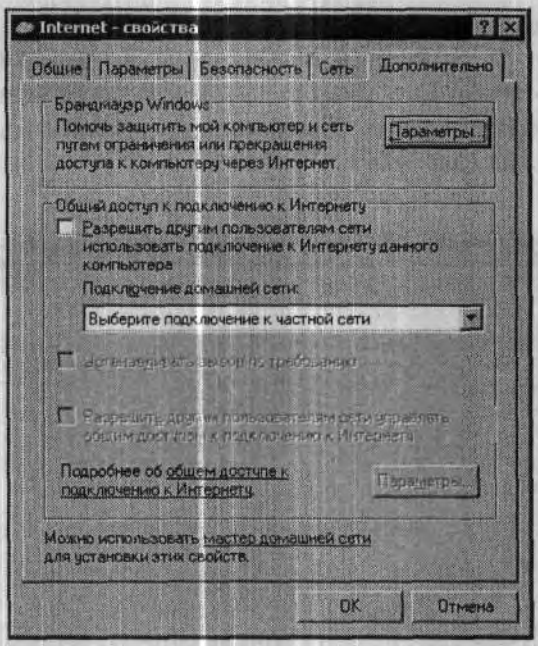


Рис. 4.28. Окно **Internet - свойства**, вкладка **Дополнительно**

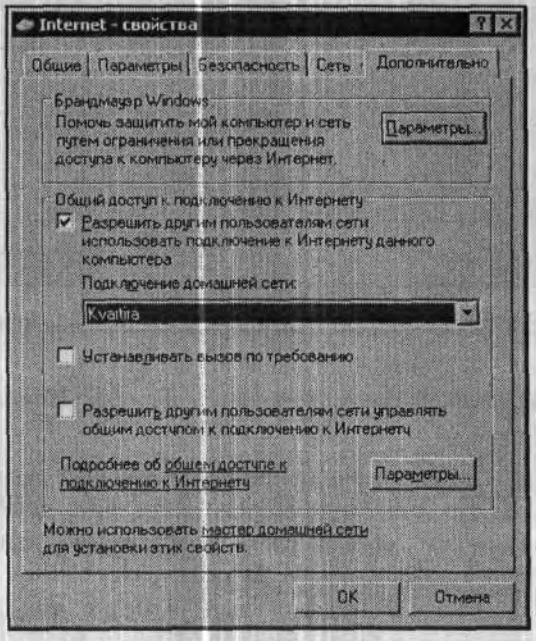


Рис. 4.29. Окно **Internet - свойства**, вкладка **Дополнительно** (выбрано подключение к локальной сети)

Любое подключение может быть отключено по техническим причинам. Для того чтобы его легко было восстановить при подключении пользователей, можно отметить флажок **Устанавливать вызов по требованию**.

Определив последние параметры и нажав кнопки **ОК** необходимое число раз, вместо ожидаемого начала работы этого подключения вы увидите сообщение, приведенное на рис. 4.30.



Рис. 4.30. Окно **Сетевые подключения** с сообщением

Дело в том, что по замыслу разработчиков Windows, в локальной сети квартиры или офиса компьютер, через который предоставляется доступ в Интернет, должен иметь IP-адрес 192.168.0.1. А если вы не согласны с этим, подключение не станет общим. Связан данный факт с тем, что компьютер общего доступа к Интернету становится еще и DHCP-сервером, раздающим другим компьютерам локальной сети адреса, что, в свою очередь, позволяет компьютерам сети автоматически получать адреса DNS-серверов. Это действительно удобно, если вы не собираетесь расширять сеть, а задача доступа в Интернет для компьютеров сети — последняя важная задача. Но мы решили устанавливать свои IP-адреса.

Что ж, придется "обмануть" разработчиков. Соглашаемся на замену IP-адреса подключения к нашей локальной сети. В результате в свойствах TCP/IP этого подключения (рис. 4.31) мы увидим адрес 192.168.0.1.

Без всяких сомнений меняем IP-адрес, на тот, что решили присвоить данному компьютеру. На рис. 4.16 это адрес 192.168.1.100.

Все. Нажимаем **ОК** и переходим к настройке рабочих станций. Здесь работы совсем не много. Открываем **Панель управления | Сеть**. Видим одно-единственное подключение к локальной сети. Если бы мы согласились на предложение разработчиков, то можно было бы воспользоваться мастером **Установить домашнюю сеть или сеть малого офиса**. Этот мастер автоматически определит наличие в сети подключения общего доступа, создаст шлюз **Подключение к Интернету** (рис. 4.32), и доступ в Интернет будет обеспечен. Но мы не согласились с простым вариантом настроек.

Мастер все равно может создать шлюз, но для того, чтобы он заработал, необходимо выполнить дополнительные настройки. Поэтому можно обойтись и без мастера.

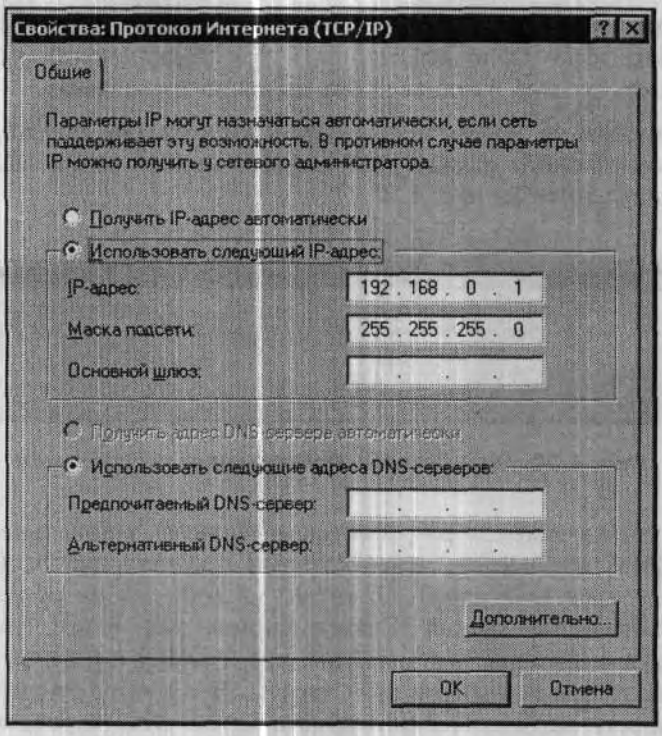


Рис. 4.31. Окно **Свойства: Протокол Интернета (TCP/IP)** (для сети квартиры или офиса)

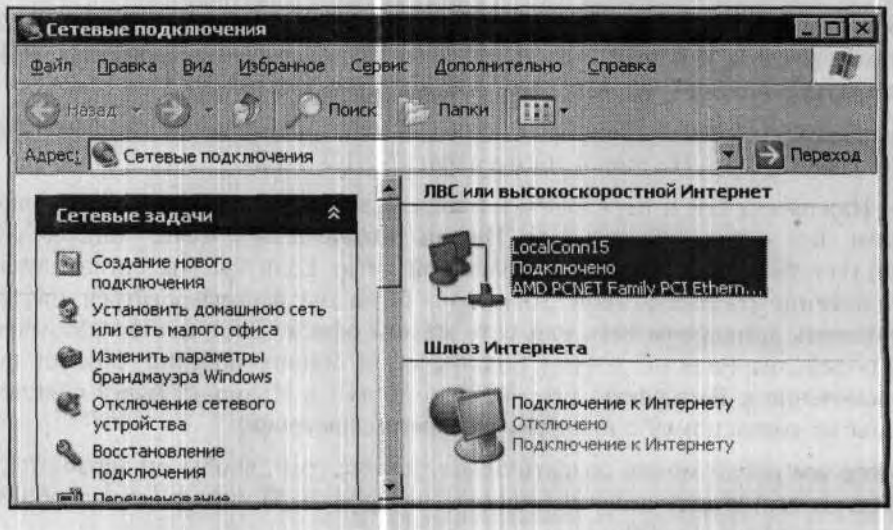


Рис. 4.32. Окно **Сетевые подключения**

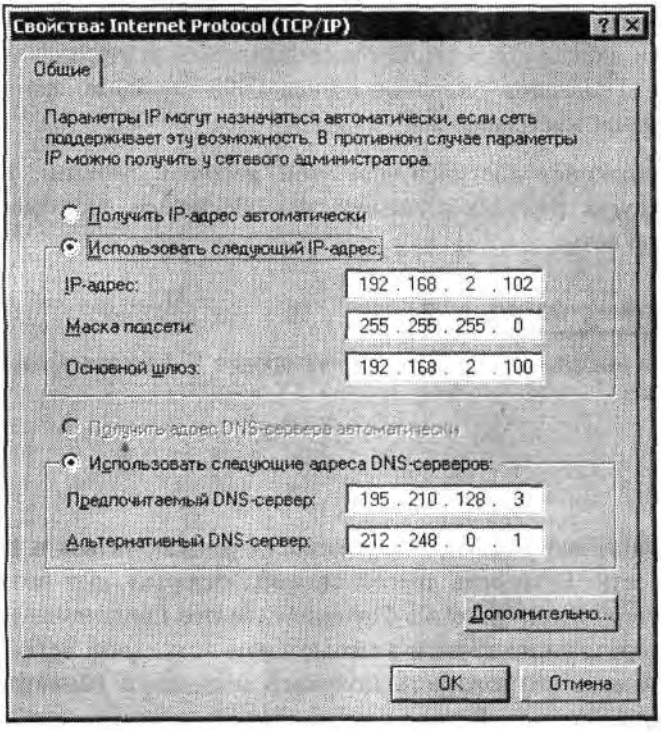


Рис. 4.33. Окно **Свойства: Internet Protocol (TCP/IP)** (на рабочей станции)

В свойствах протокола TCP/IP (рис. 4.33) подключения LocalConn15 (рис. 4.32) устанавливаем самостоятельно правильный адрес рабочей станции (если не установлен до настоящего времени), маску подсети (пока применяем только стандартное для локальной сети значение 255.255.255.0), а также адрес шлюза **Основной шлюз**, в качестве которого работает компьютер общего доступа к Интернету. Его адрес в нашем случае 192.168.1.100.

Но за обман надо расплачиваться. Необходимо самостоятельно указать адреса доступных DNS-серверов (минимум один). Когда доступ предоставлен одному компьютеру, имеющему доступ к локальной сети провайдера, можно использовать DNS-сервер локальной сети. Его адрес обычно предоставляется пользователю. Но в нашем случае этим адресом может воспользоваться только сам компьютер общего доступа. Невозможно сделать одинаково доступными два подключения — к локальной сети провайдера и VPN. Если же не указать DNS-сервер, то Интернет будет работать только по числовым IP-адресам. Вместо адреса известной поисковой системы **http://www.google.ru** придется указывать **http://216.239.59.104/** (так делали на заре Интернета).

Придется узнать доступный адрес DNS-сервера. Это совсем не сложно. Можно внести адреса DNS-серверов провайдеров, доступных в вашем городе. На рис. 3.33 указаны реальные адреса DNS-серверов, существующих во время проведения настроек.

Вот теперь Интернет доступен для этой рабочей станции. Повторив настройки на других рабочих станциях, мы обеспечим доступом в Интернет всю локальную сеть.

Примечание

Повторяя настройки, помните, что повторение IP-адресов в локальной сети не допустимо.

Модем

Очень возможно, что у вас нет возможности подключиться к Интернету через домовую сеть. Если есть другой способ, который дает возможность одному компьютеру иметь выход в Интернет, то это подключение всегда можно отдать в пользование другим компьютерам локальной сети. У некоторых пользователей есть возможность получить несколько вариантов доступа в Интернет одновременно. В этом случае следует помнить, что в одной логической сети не может быть более одного подключения общего доступа. Например, на моем компьютере есть модемное подключение, но я пользуюсь и общим подключением к Интернету в локальной сети. Я не могу в той же сети дать в общее пользование свое модемное подключение. Такая конфигурация сети работать не будет.

Но если других общих подключений нет, то можем предоставить в общее пользование и модем.

Создание подключения через обычный аналоговый модем описано в рекомендациях каждого поставщика услуг Интернета очень подробно. А учитывая наличие мастера **Создание нового подключения**, который встроен в системы Windows, — эта процедура не вызывает затруднений. Но для использования модемного подключения в качестве общего, некоторые параметры следует установить не совсем стандартно. Так, например, ввод имени пользователя и пароля лучше выполнять автоматически с помощью сценария. В свойствах созданного подключения на вкладке **Безопасность** (рис. 4.34) следует указать путь к сценарию. Сам сценарий — это текстовый файл с расширением scp.

В листинге 4.1 показан пример файла сценария.

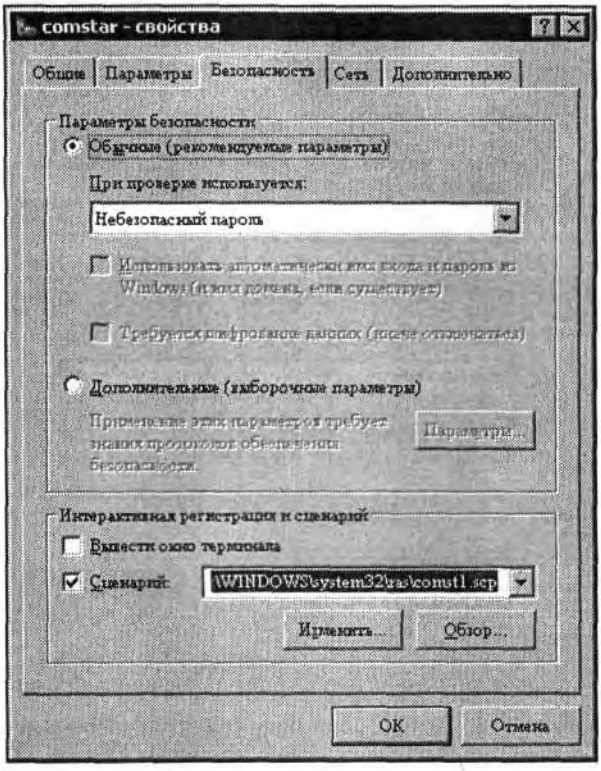


Рис. 4.34. Окно свойств подключения — вкладка **Безопасность**

Листинг 4.1. Файл сценария

```
proc main
 waitfor "login:"
 transmit "<имя_пользователя>"
 transmit "^M"
 waitfor "password:"
 transmit "<пароль>"
 transmit "^M"
endproc
```

В каталоге C:\WINDOWS\system32\ras\ можно найти заготовки файлов сценариев. Применение сценария исключит ситуации, когда имя пользователя или пароль случайно стираются и для установки соединения требуется вмешательство пользователя.

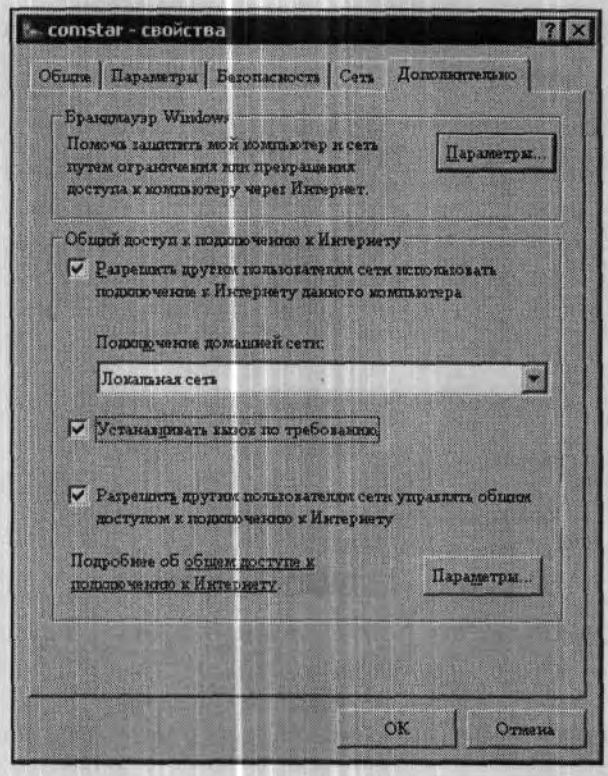


Рис. 4.35. Окно свойств подключения, вкладка **Дополнительно**

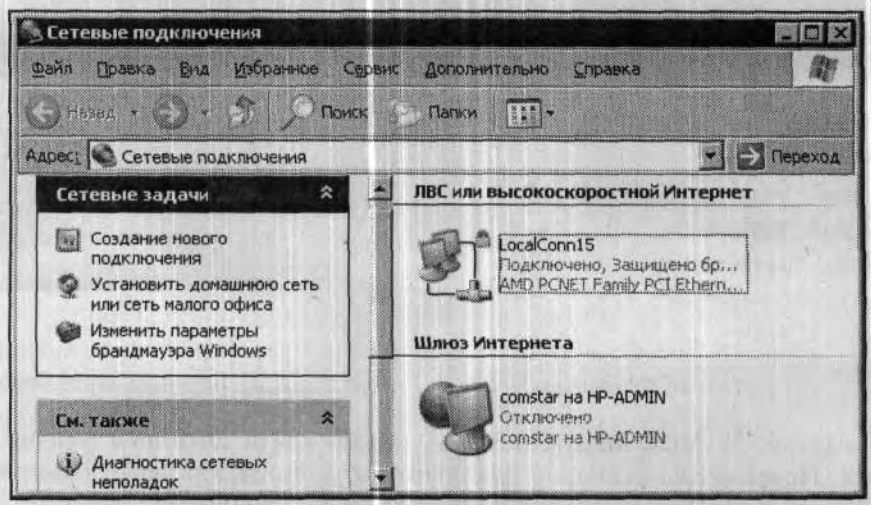


Рис. 4.36. Окно **Сетевые подключения**

На вкладке **Дополнительно** (рис. 4.35) необходимо установить флажок **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера**. После создания общего доступа к подключению Интернета локальному подключению будет присвоен адрес 192.168.0.1.

На рабочей станции, с которой хотим получить доступ к Интернету через общедоступное подключение, можно запустить мастер **Установить домашнюю сеть или сеть малого офиса** или настроить подключение самостоятельно. Если применены стандартные значения IP-адресов, предложенных операционной системой, то в окне **Сетевые подключения** (рис. 4.36) появится **Шлюз Интернета**.

Как и в случае с настройкой доступа через домовую сеть, мы можем отказаться от стандартных значений IP-адресов в свойствах TCP/IP-соединений, указав свои.

ADSL-модем

Обычное подключение в режиме моста (bridge) настраивается подобно обычному модемному подключению. Отличие заключается лишь в наличии некоторых непривычных параметров, которые указаны провайдером, и в том, что значок подключения выглядит иначе, находясь в области высокоскоростных подключений. Процедура такого подключения подробно описывается провайдерами, и служба поддержки всегда даст необходимые консультации. Далее созданное подключение можно опять использовать коллективно. Но есть ADSL-модемы, которые могут работать в качестве маршрутизаторов. Собственно подключение они устанавливают самостоятельно, а компьютеру пользователя остается использовать подключение к Интернету через локальную сеть. Относительно недорогой и удобный для такого применения модем — DSL-500T производства D-Link.

У различных провайдеров особенности подключения могут отличаться. В качестве примера рассмотрим популярное в Москве подключение по технологии Стрим. Думаю, что этот пример поможет разобраться и в других случаях.

На рис. 4.37 показан внешний вид подключенного модема. Для развязки сигналов модема и телефонной сети применяются сплитеры (Splitter). Сплитер представляет собой фильтр, который позволяет подключить модем напрямую в телефонную линию, а телефонный аппарат через фильтр, ограничивающий частотный диапазон сигналов областью низких (звуковых) частот. ADSL-модем использует высокие частоты.

На рис. 4.38 показана возможная схема подключения. Ethernet-порт модема включен в порт коммутатора, применяемого в сети.

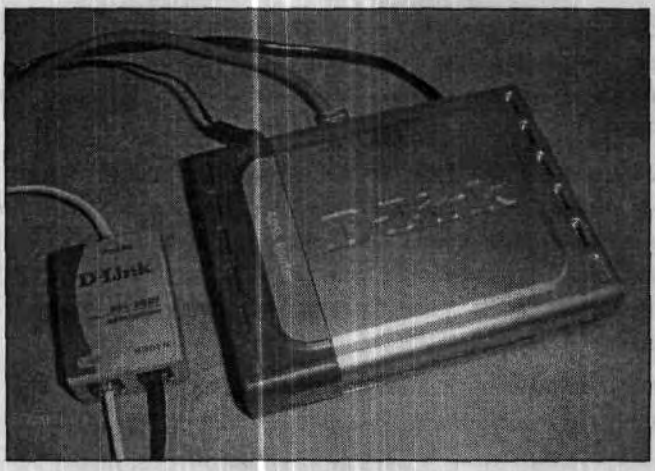


Рис. 4.37. Внешний вид DSL-500T и сплитера

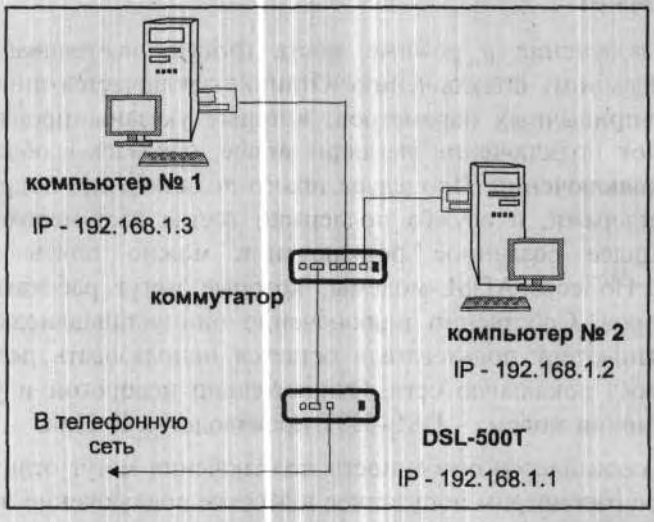


Рис. 4.38. Схема локальной сети с подключением к Интернету через DSL-500T

Управление DSL-500T и изменение его настроек возможно через HTTP-протокол. Это устройство содержит в себе операционную систему (подобную Linux), и под ее управлением работает сайт, через страницы которого и осуществляется все управление. Если во время настроек допущена ошибка, которая привела к потере связи с модемом, на его задней стенке есть кнопка **Reset**, позволяющая вернуть все настройки к заводскому варианту. Настройки можно сохранять в XML-файл. Если сохранять все удачные на-

стройки в файлы, то при необходимости всегда можно оперативно загрузить требуемый вариант. Это также избавит от повторения длинной цепочки настроек при необходимости их сброса при ошибке. Важно только вовремя сохранять настройки в файл.

При первом подключении к модему, а это можно сделать и до того, как вам предоставили ADSL-доступ, он имеет IP-адрес 192.168.1.1, имя пользователя admin, пароль admin. Об этом сказано в кратком руководстве, прилагаемом к модему. Для подключения к модему необходимо в адресной строке браузера набрать **http://192.168.1.1**. После авторизации, которая ничем не отличается от подобной процедуры на Web-страницах, вы попадете на главную страницу настроек (**Setup**). Общий вид этой страницы приведен на рис. 4.39.

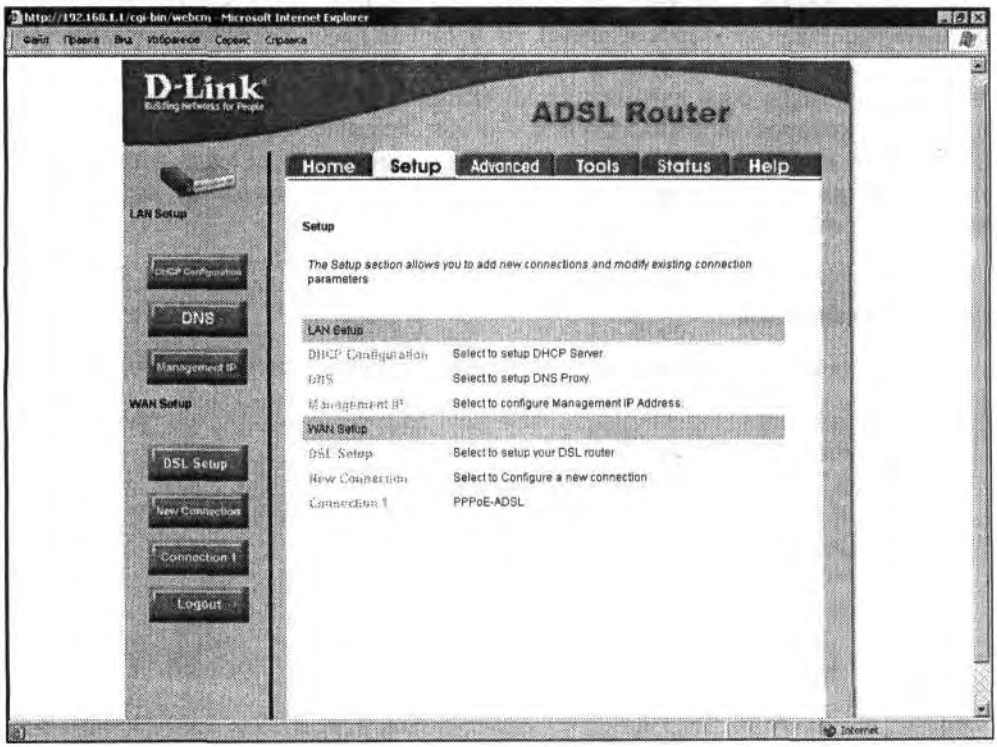


Рис. 4.39. Главная страница настроек DSL-500T

На этой странице есть две категории настроек. Первая (**Lan Setup**) позволяет настраивать параметры локальной сети:

- DHCP-сервер;

- варианты использования внешних DNS-серверов;
- IP-адрес самого модема.

Вторая категория (**WAN Setup**) позволяет настраивать параметры глобальной сети:

- параметры маршрутизатора;
- параметры нового подключения;
- параметры уже существующих подключений.

DSL-500T позволяет сохранять несколько вариантов подключений и активизировать одно из них.

На рис. 4.40 приведен вид страницы настройки DHCP-сервера — **DHCP Configuration**. Доступны два варианта этих настроек. DHCP-сервер можно просто отключить. Именно этот вариант показан на рисунке. Но можно настроить диапазон IP-адресов (**Start IP** и **End IP**) для назначения компьютерам сети. Также можно указать адрес DNS-сервера, который должны получить компьютеры сети автоматически (**Primary DNS**). Еще один параметр — время, на которое запоминаются выданные компьютерам параметры (**Lease Time**). При кратковременном отключении компьютера от сети и повторном подключении до истечения указанного периода он получит тот же IP-адрес, что был до отключения.

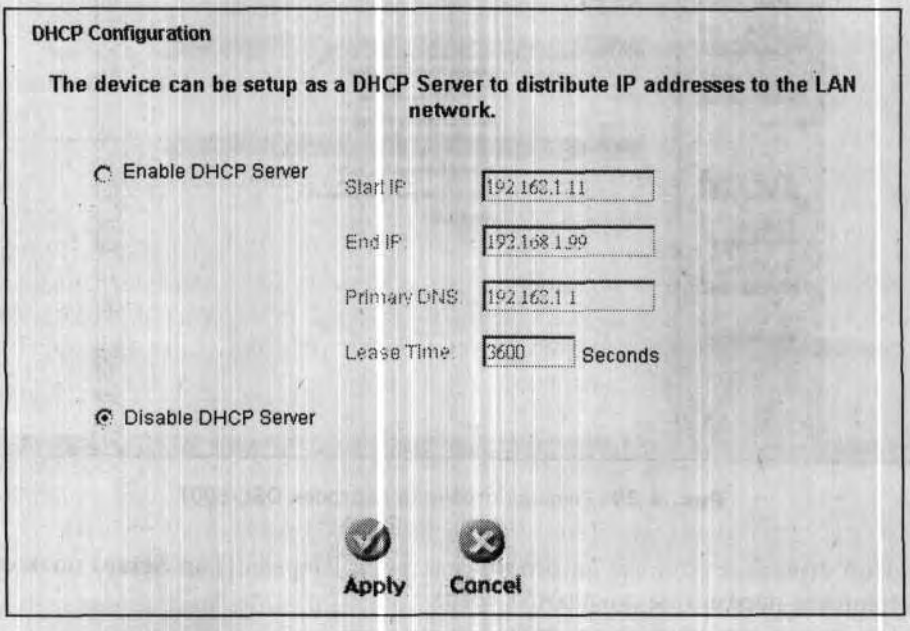


Рис. 4.40. Страница (фрагмент) **DHCP Configuration**

На рис. 4.41 показана страница конфигурации DNS. Здесь можно указать адреса DNS-серверов, полученные от провайдера. В поле **DNS Relay Selection** можно выбрать **Use User Discovered DNS Server Only** (Использовать только определенные пользователем серверы).

В этом случае модем всегда может выполнять для компьютеров локальной сети роль DNS-сервера, перенаправляя запросы рабочих станций на указанные адреса.

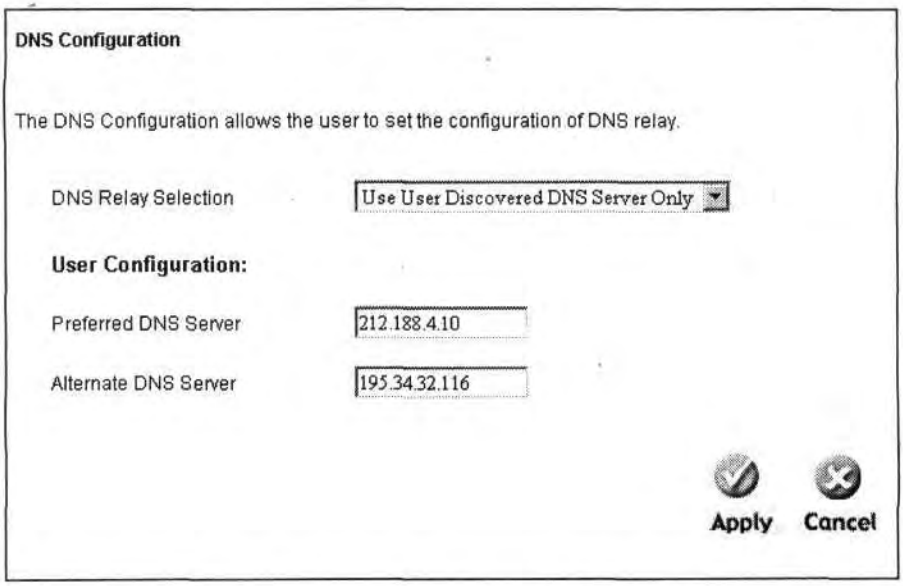


Рис. 4.41. Страница (фрагмент) **DNS Configuration**

На странице **Management IP** (рис. 4.42) в случае неизменности IP-адреса маршрутизатора модема можно ничего не менять. Если вы настраиваете не Стрим, а другую услугу ADSL-доступа, возможно, понадобится указать адрес шлюза по умолчанию — **Default Gateway**. Для услуги Стрим этот параметр получается модемом автоматически.

Переходим к **WAN Setup**.

На странице **DSL Setup** выбирают режим работы модема. Если провайдер не порекомендовал что-либо обязательное, то можно, как на рис. 4.43, выбрать **MMODE**, что соответствует автоматическому выбору режима работы.

Теперь можно создать новое подключение или редактировать имеющееся, нажав кнопку **Connection 1** (см. рис. 4.39). При этом откроется страница **PPPoE Connection Setup** (рис. 4.44).

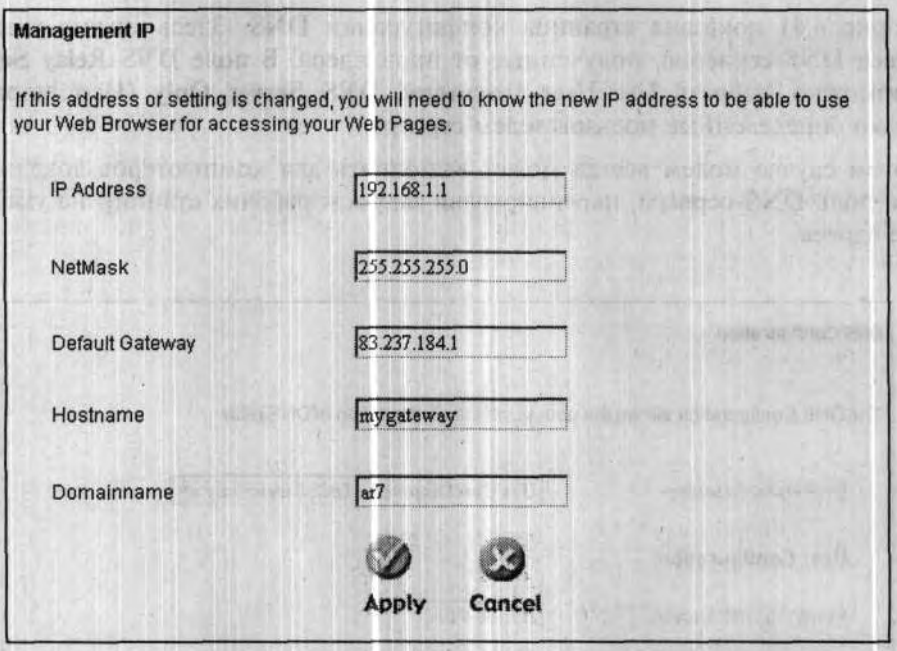


Рис. 4.42. Страница (фрагмент) **Management IP**

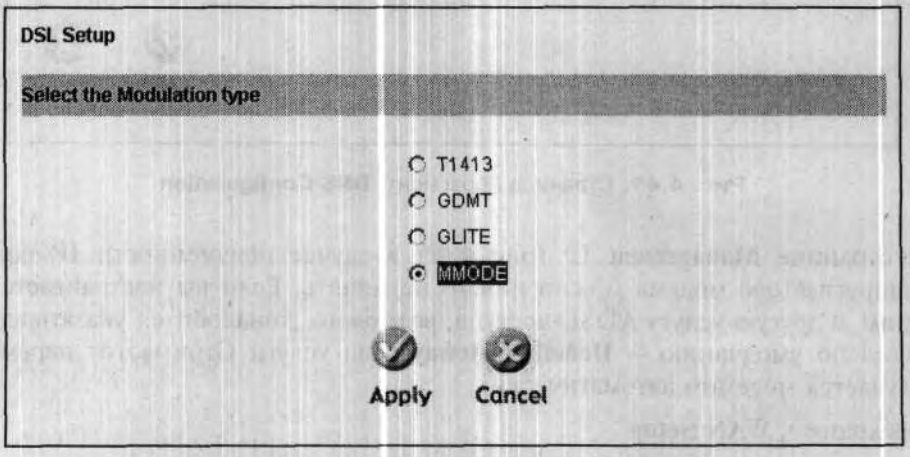


Рис. 4.43. Страница (фрагмент) **DSL Setup**

Имя подключения **Name** можно указать любое, тип (**Type**) подключения в нашем случае **PPPoE**. Это метод установки соединения типа "точка-точка" (PPP) по сети Ethernet через сетевой адаптер (PPP over Ethernet). Ставим два флажка в строке **Options — NAT** и **Firewall**. Это позволит компьютерам сети

выходить в Интернет под одним IP-адресом, который будет выделен провайдером, а также защитить сеть от непрошенного проникновения извне. **Username** и **Password** не должны вызвать затруднений. В группе **PVC Setting** в полях **VPI** и **VCI** укажите то, что предложил провайдер, в поле **QoS** значение **UBR**. Осталось установить флажки **Set Route** и **On Demand**, что позволит включить маршрутизатор модема и производить подключение по требованию сетевой рабочей станции. В остальных полях можно ничего не менять, если иное не предложено провайдером.

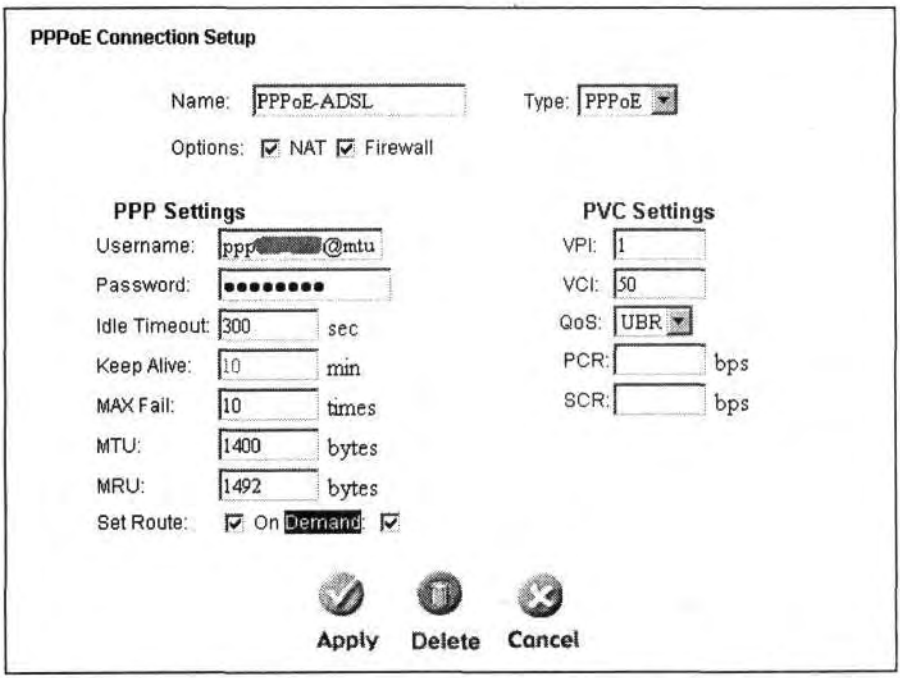


Рис. 4.44. Страница (фрагмент) **PPPoE Connection Setup**

При каждом изменении настроек перед переходом на другую страницу необходимо нажимать кнопку **Apply** (Применить), а перед завершением всех настроек нужно перейти на вкладку **Tools**, нажать кнопку **System Commands** и на открывшейся странице выбрать **Save All** (Сохранить все). Перед закрытием страниц настройки следует выйти из системы модема, нажав кнопку **Logout**.

Теперь, при наличии предоставленного вам доступа к услуге Стрим, можно всей сетью работать в Интернете. Только не забудьте настроить у рабочей станции TCP/IP-протокол в соответствии с настройками модема.

Доступ к рабочей станции из Интернета

В последнее время все более распространяются безлимитные тарифы на доступ в Интернет, что позволяет никогда не отключать домашний компьютер от Интернета. А это, в свою очередь, позволяет получить доступ к домашнему или офисному компьютеру из Интернета.

Это возможно, если ваша локальная сеть имеет хотя бы один настоящий IP-адрес. Данный адрес предоставлен провайдером и соответствует выделенным для использования в Интернете адресам. Совсем хорошо, если этот адрес постоянный. Но ограниченность адресного пространства заставляет провайдеров выдавать временные адреса. За счет этого множество пользователей, подключающихся к Интернету время от времени и в несовпадающие моменты, могут использовать меньшее, чем количество пользователей, число адресов. Появляется необходимость в определении текущего IP-адреса рабочей станции в Интернете, чтобы получить возможность контакта с ней. Это возможно несколькими способами, например, зарегистрировавшись на сайте **https://www.dyndns.org/account/**, вы можете получить бесплатную возможность использовать два очень интересных сервиса — Dynamic DNS (динамический DNS) и WebHop. Скачав специальную программу-клиент и установив ее на рабочую станцию, к которой требуется доступ из Интернета, вы дадите возможность сервису Dynamic DNS постоянно знать текущий IP-адрес рабочей станции в Интернете. Символьный адрес, присвоенный вашей рабочей станции, позволяет командой `ping` по этому адресу определить текущий числовой адрес, если это необходимо. Но большинство программ удаленного доступа или администрирования позволяют использовать именно символьные адреса. Это и удаленный доступ к рабочему столу, и программы удаленного администрирования RADMIN (**http://www.famatech.com/ru/radmin/**) или VNC (**http://www.realvnc.com/**).

Таким образом, вы можете иметь как доступ к Интернету из своей локальной сети, так и доступ к ЛЮБОЙ рабочей станции вашей локальной сети из Интернета. Многие сервисы позволяют выбирать произвольно порт, по которому будет проходить обмен информацией. Широко известно, например, что HTTP-протокол по умолчанию использует порт 80, но не редко применяют и порт 8080. Вообще же можно использовать любой свободный порт. Проблема лишь в том, что тот, кто соединяется с вашим компьютером, должен знать номер этого порта. Стандартизация портов для сервисов и приложений избавляет пользователей от их запоминания. Но если вы сами должны получить доступ к своему компьютеру, то можете даже Web-сайту на вашей рабочей станции назначить порт 9083, например. Если вам известен этот номер порта, а сервис Dynamic DNS предоставил вам символьный адрес вида `<ваше имя>.dinip.net`, то, набрав в адресной строке браузера

адрес `http://<ваше имя>.dinip.net :9083`, вы попадете на сайт вашего компьютера. Таким же образом можно создавать почтовые серверы, FTP-серверы, словом, любые мыслимые сервисы, к которым вы хотите получить доступ. Имея всего один реальный IP-адрес, да еще не постоянный, вы можете иметь практически неограниченное число сервисов на каждой рабочей станции локальной сети, доступных из Интернета.

Остается лишь решить задачу распределения потоков информации, пришедшей из Интернета, в соответствии с номерами портов и протоколами. Имея маршрутизатор для подключения локальной сети к Интернету, можно использовать его и для обратной задачи — доступа из Интернета к рабочим станциям. Настраивая DSL-500T (см. рис. 4.44), мы установили флажки **Set Route** и **NAT**. Вторая возможность уже использована для выхода в Интернет. Все локальные адреса преобразуются в один-единственный адрес, дающий доступ в Интернет. Теперь воспользуемся маршрутизацией из Интернета в локальную сеть.

На вкладке **Advanced** есть страница **Port Forwarding** (Перенаправление портов) (рис. 4.45). Это для нашей сети просто находка!

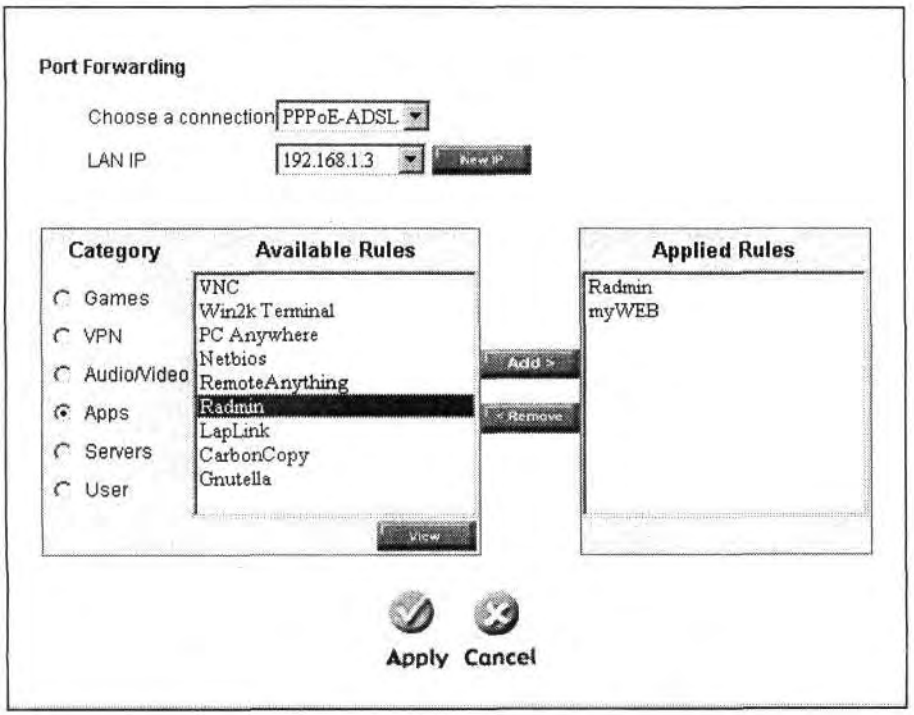


Рис. 4.45. Страница (фрагмент) **Port Forwarding**

Здесь поле **LAN IP** — это адрес рабочей станции, на которую мы хотим попасть из Интернета. Вот причина, по которой мы упорно отказывались от применения DHCP-сервера в нашей сети. Имея постоянные адреса внутри сети, мы можем без проблем получить к ним доступ из Интернета. Конечно, можно задать диапазон адресов, которые будут выдаваться рабочим станциям, а отдельным машинам назначить статические адреса. Но это имеет смысл в сети, где больше трех рабочих станций. А у нас пока их не больше.

Для того чтобы узнать, на какие IP-адреса можно перенаправлять информацию из Интернета, надо открыть страницу **LAN Clients** (рис. 4.46). На ней вы увидите диапазон "правильных", по мнению маршрутизатора, адресов **Valid IP Range**. Это те адреса, что выделяются DHCP-сервером.

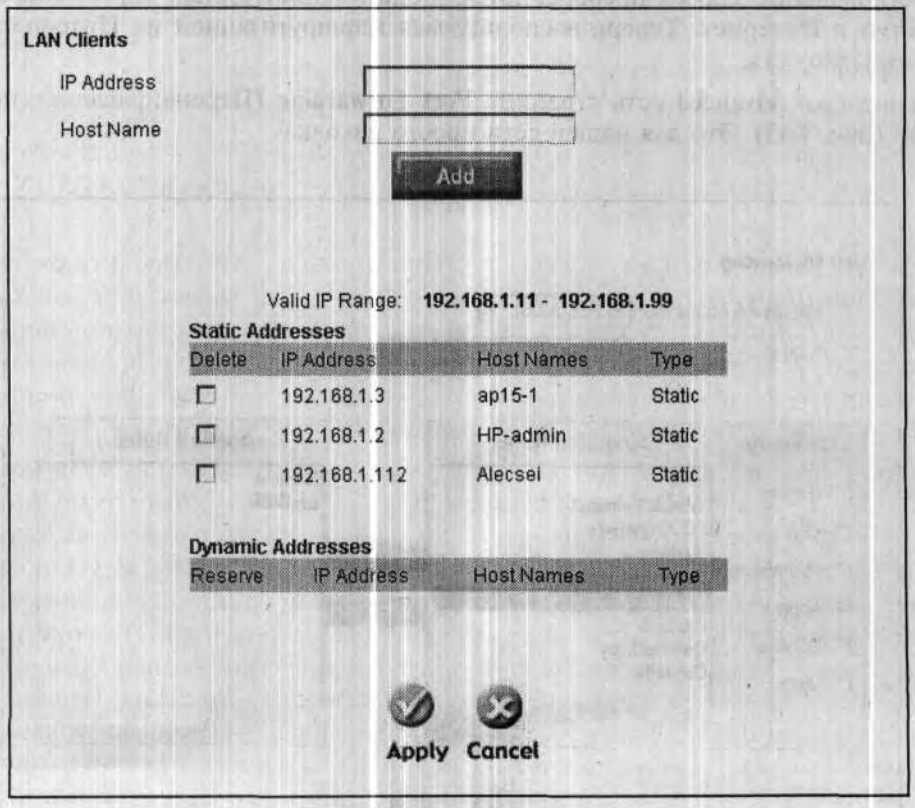


Рис. 4.46. Страница (фрагмент) **LAN Clients**

А под ними статические адреса **Static Addresses** рабочих станций локальной сети. Эти статические адреса и можно применять для перенаправления портов.

На странице **Port Forwarding** (см. рис. 4.47) есть две таблицы — **Available Rules** (Доступные правила) и **Applied Rules** (Примененные правила).

В таблице **Available Rules** доступные правила условно распределены по категориям, среди которых есть категория **User**, где можно создавать нестандартные правила. Но в уже созданных правилах есть даже вариант для программы RADMIN для стандартного порта, применяемого в этой программе. Но никто не мешает создать такое правило для каждой рабочей станции сети, определив для них уникальные номера портов. Правила (Rules) представляют из себя описание перенаправления IP-пакетов на указанный IP-адрес. Выделив правило и нажав кнопку **View** (Просмотр), можно увидеть его содержание. В нем четыре составляющие:

- **Protocol** — протокол, для которого создано правило;
- **Port Start** — начало диапазона портов перенаправления;
- **Port End** — конец диапазона портов перенаправления;
- **Port Map** — порт, на который направляются пакеты.

Протокол чаще всего TCP, а значения портов могут быть одинаковы для всех трех составляющих. Например, для стандартного режима RADMIN все порты имеют значение 4899.

Если для каждого IP-адреса рабочей станции вашей сети назначить соответствующий порт, которому сопоставить определенный сервис или приложение, то вы сможете обеспечить двухсторонней связью все рабочие станции. Известно, например, что порты в диапазоне 25800—25900 не используются стандартными приложениями. Вы можете совершенно свободно распоряжаться этими портами, назначая их своим рабочим станциям.

На рис. 4.46 мы видим три IP-адреса. 192.168.1.2 — это мой компьютер, 192.168.1.3 — компьютер моей дочери, 192.168.1.112 — компьютер моего сына. Мы хотим получить удаленный доступ ко всем компьютерам для администрирования из Интернета, а на компьютере моей дочери установлен экспериментальный Web-сервер, который следует сделать доступным для всех желающих. Кроме того, все компьютеры подключены к Интернету через Стрим. По услуге сервиса Dynamic DNS получаем символьный адрес `okobox.homeip.net` и `okobox.webhop.net` с помощью WebHop. Первая услуга позволяет привязать изменяющийся IP-адрес к адресу символьному. Вторая услуга перенаправляет попытки подключения к адресу `okobox.webhop.net` на адрес `okobox.homeip.net :9080`. Стрим не позволяет из Интернета использовать стандартные порты для Web-сервисов. Поэтому выбираем порт 9080, а для всех, кому это надо, даем адрес `okobox.webhop.net`, для которого не требуется запоминать номер порта. При необходимости можно создать еще один сайт с другим портом и периодически переключать на Dynamic DNS перенаправление на один или другой

порт. Для администрирования выбираем программу RADMIN, а порты 25802, 25803, 25812.

В маршрутизаторе модема создаем сервисы пользователя с характеристиками, описанными в табл. 4.1.

Таблица 4.1. *Сервисы пользователя*

Сервис	LAN IP	Protocol	Port Start	Port End	Port Map
MyWEB	192.168.1.3	TCP	9080	9080	9080
Radmin1	192.168.1.2	TCP	25802	25802	25802
Radmin2	192.168.1.3	TCP	25803	25803	25803
Radmin3	192.168.1.112	TCP	25812	25812	25812

Наименование сервисов, конечно, условно. Если мы захотим использовать порт 25812 для Web-сервиса на компьютере 192.168.1.112, то ничто не может этому помешать. Перенастраивать ничего не придется. Только в маршрутизаторе наименование сервиса лучше изменить, чтобы не запутаться самим позднее.

Все сервисы, которые сделаны доступными из Интернета, доступны и внутри локальной сети, но по внутренним IP-адресам.

Если применяем dial-up

Вариант доступа к сети, который был описан ранее, годится при постоянном подключении к Интернету. А если такой возможности нет, и доступ в Интернет обеспечивается через коммутируемую линию? Возможен ли доступ к нашей сети из Интернета?

Да. И в этом случае доступ возможен, но придется мириться с некоторыми неудобствами. Во время подключения к Интернету занята ваша телефонная линия. Поэтому следует определить время, когда ее можно занимать для работы с сетью. Само подключение может выполняться автоматически. Соответственно, связь с вашей сетью из Интернета должна проходить по расписанию. Учитывая невысокую скорость модемного соединения, рассчитывать на передачу больших объемов информации не приходится.

Автоматическое подключение к Интернету можно выполнить, применив команду:

```
rasdial <имя_подключения>
```

Все данные о пользователе и пароле находятся в файле сценария и будут использованы при подключении.

Для отключения от Интернета выполняем команду:

```
rasdial <имя_подключения> /disconnect
```

Эти команды могут быть заранее записаны в командные файлы и запускаться планировщиком Windows.

Возможна и организация входящего вызова по телефонной линии. Но это уже не через Интернет.

Общий принтер

Практика работы на персональных компьютерах показала, что переход на исключительно электронный документооборот невозможен. Всегда требуются бумажные документы, как бы мы не стремились от них отказаться. Для изготовления бумажного документа требуется принтер. Рано или поздно каждый пользователь сети сталкивается с необходимостью подготовки твердой копии электронного документа.

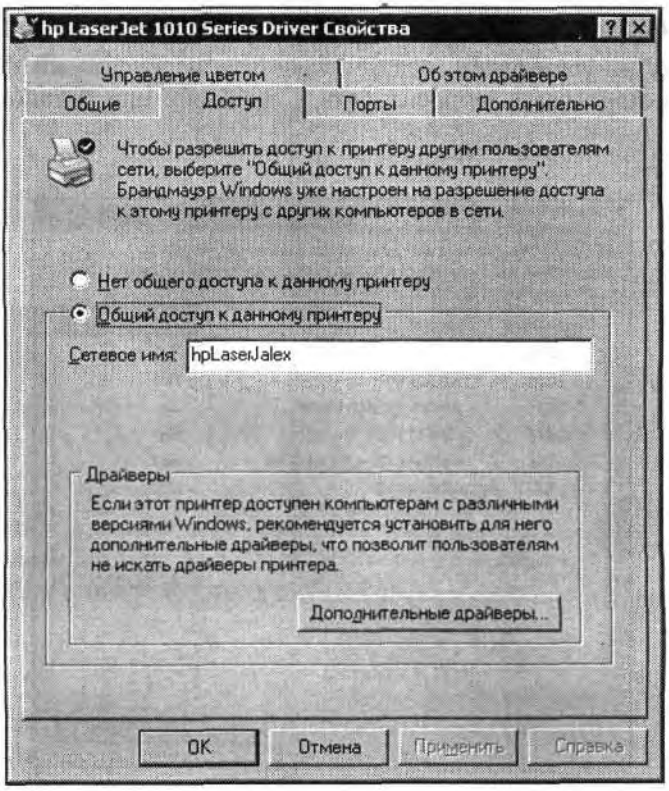


Рис. 4.47. Окно свойств локального принтера

Оснащать каждое рабочее место в сети принтером — нерационально, а заставлять пользователей сети ходить к компьютеру, на котором установлен принтер, отвлекая пользователя этого компьютера, тоже не хорошо. Необходимо каждому пользователю сети дать возможность использовать единственный принтер, имеющийся в сети.

И это совсем не сложно. Как файлы и папки, так и принтеры могут быть общедоступными ресурсами. С той разницей, что для сетевой работы с принтером необходимо иметь на своей рабочей станции соответствующий драйвер принтера. Многие современные принтеры не требуют установки драйвера на рабочей станции, с которой требуется получить доступ к общему принтеру. Драйвер в операционных системах Windows может быть установлен автоматически. Для того чтобы это было возможно, на компьютере, где установлен принтер, должен быть обеспечен общий доступ к нему (рис. 4.47) и установлены драйверы для всех операционных систем, которые могут быть на компьютерах пользователей.

Для того чтобы узнать, какие драйверы уже установлены, и добавить дополнительные, достаточно в окне свойств локального принтера нажать кнопку **Дополнительные драйверы**. При этом откроется одноименное окно (рис. 4.48).

Если драйвер не установлен, следует отметить необходимый флажок и нажать **OK**. Система сама запросит путь к драйверу или установочный диск принтера.

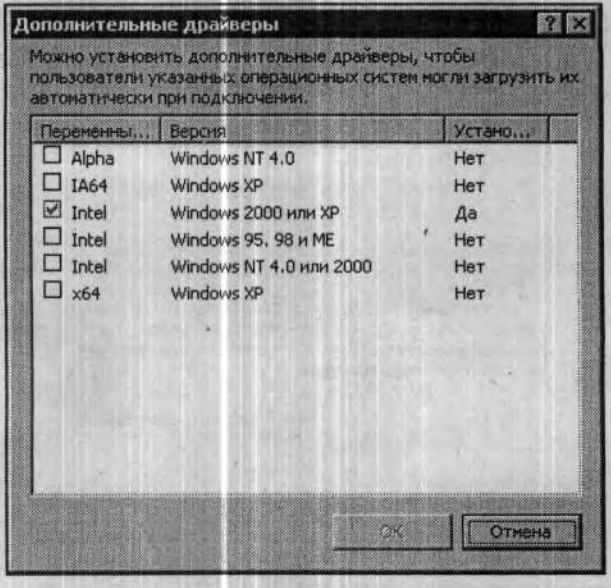


Рис. 4.48. Окно **Дополнительные драйверы**

На компьютерах сети теперь требуется только найти принтер в сетевом окружении (рис. 4.49) и выбрать в контекстном меню пункт **Подключить**.

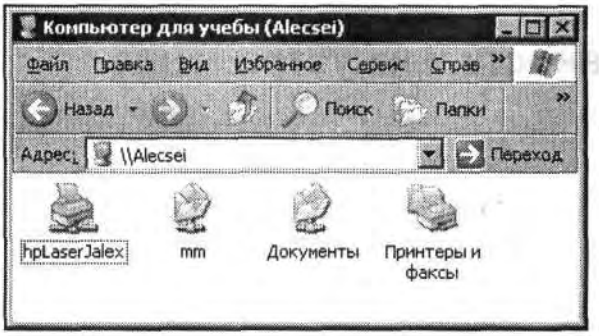


Рис. 4.49. Принтер hpLaserJalex в сетевом окружении

После этого будет выведено на экран окно предупреждения системы безопасности **Подключение к принтеру** (рис. 4.50).

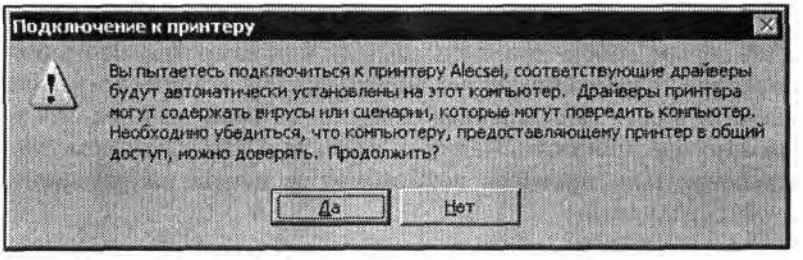


Рис. 4.50. Окно **Подключение к принтеру**

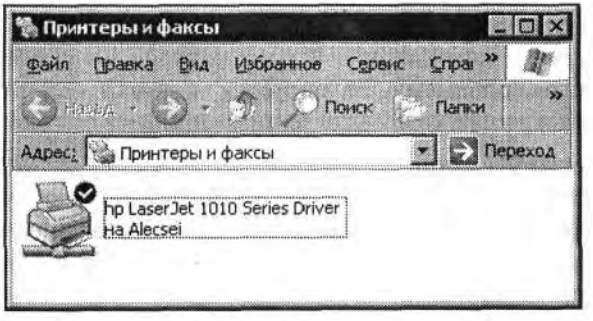


Рис. 4.51. Окно **Принтеры и факсы** с установленным принтером

После вашего согласия с продолжением операции драйвер принтера будет скопирован на ваш компьютер и в папке **Принтеры и факсы** (рис. 4.51) появится новый принтер.

Неисправности и их устранение

Некоторые проблемы, связанные с подключением компьютеров к сети, были рассмотрены ранее в этой главе и в *главе 3*.

Можно рассмотреть общий случай поиска неисправности в небольшой сети.

Ттипичные случаи проявления неисправностей.

- Не могу войти в сеть.
- Не могу открыть сетевой каталог.
- Не могу скопировать файл из сети.
- Не могу сохранить файл в сети.
- Не могу выйти в Интернет.
- Не работает электронная почта.
- Не работает ICQ.

Чаще всего первое сообщение пользователя или самостоятельно обнаруженное проявление неисправности не может указать конкретно на место этой неисправности в сети. Представляя себе общий путь информации в каждом случае, можно предположить наличие дефекта в том или ином месте. А затем, последовательно проверяя возможные варианты, определить действительную неисправность.

Все перечисленные проявления неисправности могут быть вызваны одной-единственной причиной — поломкой, возникшей в различные моменты работы с компьютером.

Поэтому, если опыт и интуиция не подсказали сразу место дефекта, лучше начать с перезагрузки компьютера. В ходе загрузки вы увидите момент входа в сеть, возможные сообщения об ошибках, а также исключите временные проблемы, которые могут возникать в операционной системе.

Если загрузка системы прошла нормально, то тестируем работоспособность компьютера в сети с помощью команды `ping`. Если к любому компьютеру сети есть доступ этой командой, а время отклика не превышает 10 мс, то сеть работает нормально. Если время отклика нестабильно и достигает иногда значений, близких к одной секунде, то следует проверить надежность всех контактов по пути сигнала. Если все соединения исправны, возможна проблема с сетевым адаптером. Каким? Надо определять. Попробуйте повторить тест работы в сети с компьютера, связь с которым неудовлетвори-

тельная. Если `ping` по всем сетевым адресам с этого компьютера дает неутешительные результаты, то, скорее всего, причина именно в его сетевой карте или в кабеле, которым этот компьютер связан с сетью. Определить это можно, временно поменяв сетевой адаптер на заведомо исправный. Если работа восстановилась, то попробуйте еще раз поставить на место старый адаптер. Бывает, что нарушается контакт в разъеме самой сетевой карты. Если дефект возвратился, меняем сетевой адаптер. Если не возвратился, считаем на этот раз дефект устраненным, но обращаем внимание на работу этого компьютера в течение некоторого времени. Если замена сетевой карты не приводит к положительному результату, ищем дефект в линии связи. Пробуем переключить кабель в другой порт коммутатора, выключить коммутатор на короткое время и включить снова. Ничего не помогло? Меняем кабель.

Если все тесты сети проходят нормально, выполняем действия, которые вызвали проблему.

Не удается выполнить действия с файлами в сети? Проверяем права на каталоги, с которыми выполняются операции. Может быть, пользователь компьютера, где находятся файлы, невольно изменил разрешения на них для сетевых пользователей. Не работает электронная почта или ICQ? А работает ли Интернет? Если да, то проверяем настройки проблемных сервисов на рабочих станциях, если нет, то выясняем причины. Если не удается найти причины в вашей сети, то возможно это сбой у провайдера. Повторите попытку через несколько минут.

Таким образом, анализируя ситуацию, проверяя наличие проблемы от момента загрузки, вы можете достаточно быстро локализовать проблему.



Глава 5

Защита информации в вашей сети

Работая в сети, имеющей доступ в Интернет, следует подумать о защите данных. Дело не в том, что у вас могут быть секретные данные (но и это может иметь место), а в том, что ваши пароли и имена пользователей могут быть доступны "доброжелателям", после чего вы будете "обрадованы" проблемами в системе или завалены спамом по электронной почте, адреса которой будут позаимствованы с ваших компьютеров. Да и вообще, неприятно, когда дверь в квартиру открыта и каждый проходящий мимо видит вас.

Наиболее простыми средствами защиты можно считать те, что встроены в операционную систему.

Брандмауэр

В Windows XP и Windows Server 2003 встроен брандмауэр. Это программное средство, которое не пропускает из сети пакеты, которые не были запрошены пользователем или программой. То, что будут пропущены пакеты, запрошенные программой, говорит, что есть риск открыть доступ к своему компьютеру или сети, пропустив однажды программу-шпион, которая будет сама определять необходимость получения или отправки данных компьютером в сеть.

Как защититься от таких программ, мы поговорим позднее, а пока о самом брандмауэре.

Панель управления | Брандмауэр Windows — это адрес устройства в вашей системе.

Вкладка **Общие** окна **Брандмауэр Windows** (рис. 5.1) позволяет включить или выключить брандмауэр, или запретить/разрешить исключения. Если выключить брандмауэр, то говорить в этом разделе будет не о чем. Поэтому будем считать, что во всех случаях, кроме оговоренных специально, брандмауэр

включен. Но многие приложения и сервисы требуют, чтобы какой-то доступ без вашего предварительного запроса существовал постоянно. Если вы наглухо запретите все запросы к компьютеру из сети, то даже команда `ping` перестанет давать результаты, несмотря на присутствие компьютера в сети.

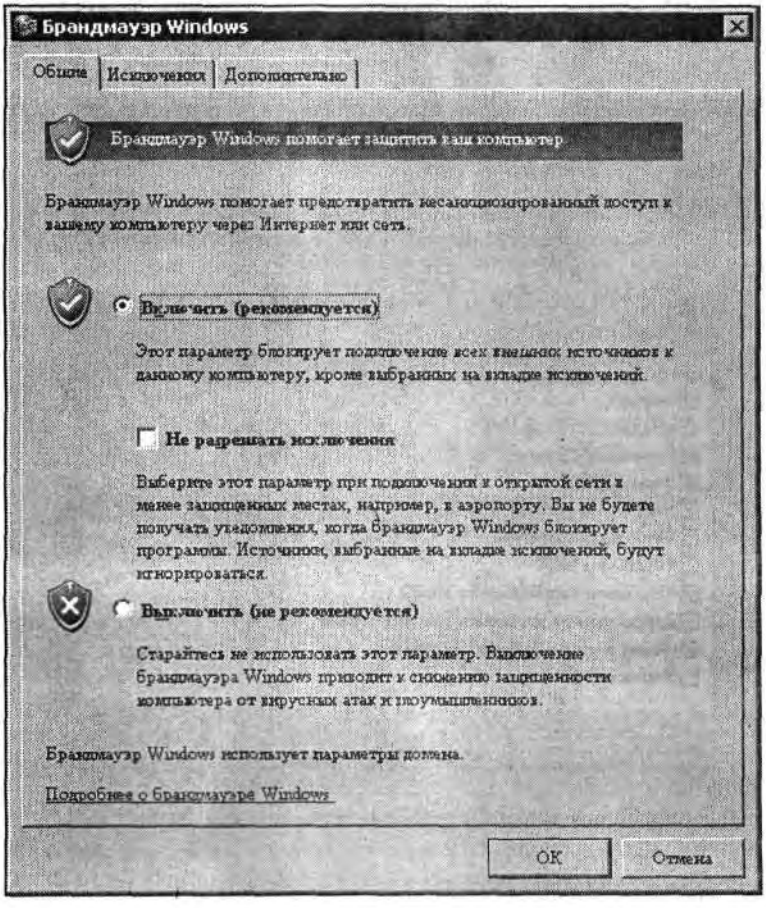


Рис. 5.1. Окно **Брандмауэр Windows**, вкладка **Общие**

Работа брандмауэра построена таким образом, что управлять можно как защитой в целом, так и защитой отдельных сетевых адаптеров. Это позволяет сделать совершенно свободным доступ через адаптеры, подключенные к доверенным участкам сети и запретить доступ через адаптеры сегментов сети, откуда можно ожидать непрошенных гостей.

На вкладке **Исключения** (рис. 5.2) можно указать программы или порты, для которых вы бы хотели разрешить беспрепятственный доступ из сети. Если

для программы не разрешен доступ из Интернета или сети и установлен флажок **Отображать уведомление, когда брандмауэр блокирует программу**, вы будете видеть попытку программы разрешить доступ к ней. В некоторых случаях это оправдано (ICQ, например), а иногда это лишнее. Часто авторы и распространители бесплатных программ включают в них элементы, которые не требуются для нормальной работы программы, но позволяют получить сведения о потенциальном покупателе, например.

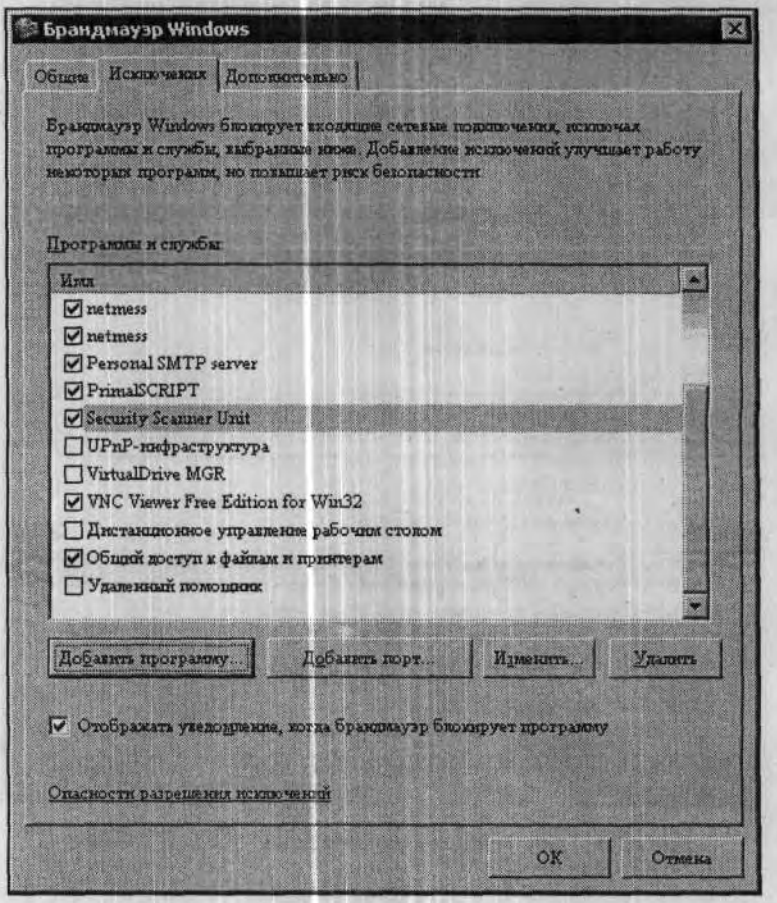


Рис. 5.2. Окно **Брандмауэр Windows**, вкладка **Исключения**

Из тех программ, которые видны на рис. 5.2, пробная версия PrimalSCRIPT, например, показывает рекламную информацию во время подключения к Интернету. Об этом, правда, разработчики предупреждают заранее, но в отдельных случаях о подобном факте не сообщают.

В вашей власти — заблокировать программу или разрешить ей общение с кем-либо или с чем-либо через сеть или Интернет.

Если вы придерживаетесь политики тотального ограничения свободы для установленных программ, то вам придется самостоятельно разрешать доступ по некоторым портам, нажав на кнопку **Добавить порт**.

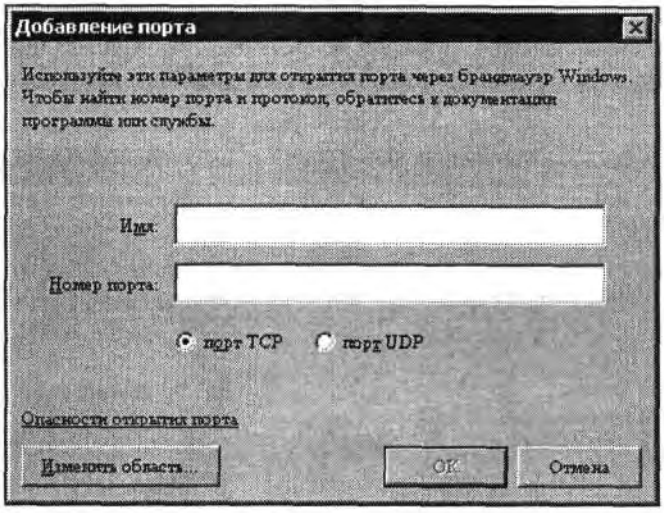


Рис. 5.3. Окно **Добавление порта**

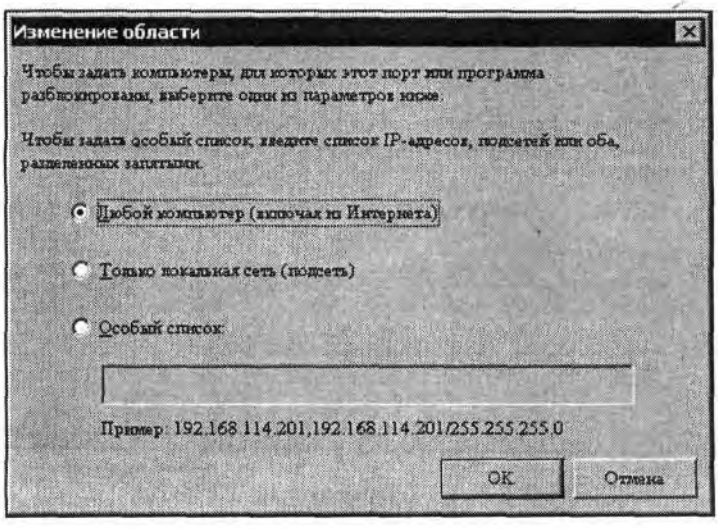


Рис. 5.4. Окно **Изменение области**

При этом откроется окно (рис. 5.3), где есть возможность выбрать протокол, по которому должен проходить обмен информацией, задать имя и указать номер порта. Например, создавая Web-сервер на компьютере внутри сети, вам придется разрешить к нему доступ по TCP-протоколу, через 80-й (или другой) порт. Нажав кнопку **Изменить область**, вы попадете в окно **Изменение области** (рис. 5.4).

В этом окне есть возможность разрешить доступ с любого компьютера или только из локальной сети. Можно и указать совершенно конкретные IP-адреса или подсети, с которых разрешено иметь доступ к вашему компьютеру.



Рис. 5.5. Окно **Брандмауэр Windows**, вкладка **Дополнительно**

На вкладке **Дополнительно** (рис. 5.5) можно установить параметры по умолчанию, если вы запутались и намудрили, для этого достаточно нажать кнопку **По умолчанию**. Этой кнопкой, надеюсь, придется пользоваться не часто. Есть здесь средство, которое запрещает работу команды `ping` из сети или Интернета, когда делаются попытки найти ваш компьютер или сеть и сканировать на предмет уязвимостей. Это кнопка **Параметры** в разделе **Протокол ICMP**.

При нажатии этой кнопки откроется окно **Параметры ICMP** (рис. 5.6).

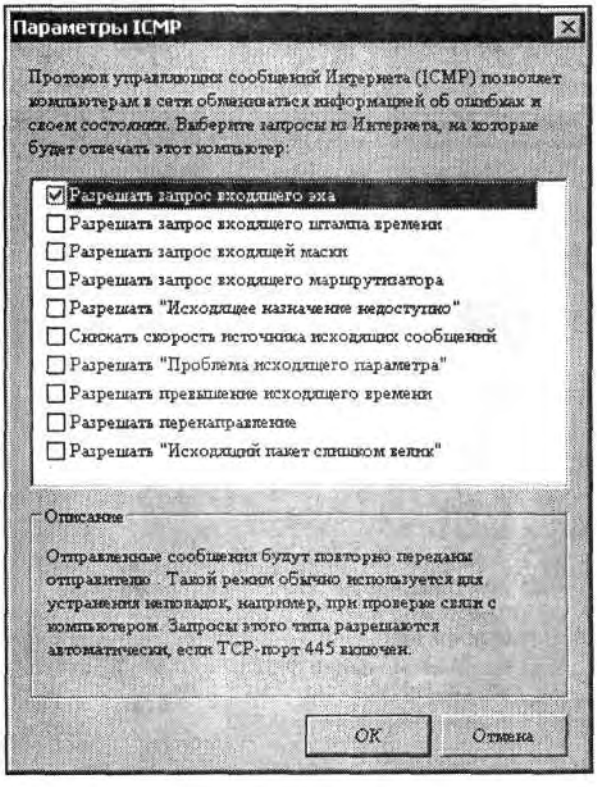


Рис. 5.6. Окно **Параметры ICMP**

Каждый параметр имеет описание, которое появляется в нижней части окна. Первый из параметров — **Разрешать запрос входящего эха** как раз и отвечает за возможность "пингования" компьютера. Возможно, что, усложняя задачи, решаемые вашим компьютером, вам потребуется включить какие-либо из этих параметров. Например, если вы решите использовать вирту-

альную сеть для связи с другими компьютерами или сетями через Интернет, параметр **Разрешать запрос входящего эха** потребуется включить. Иначе ваши компьютеры не смогут найти друг друга для образования виртуальной сети.

В верхней части окна **Параметры сетевого подключения** перечислены все сетевые подключения, которые есть на вашем компьютере. Если не установлен флажок против имени подключения, то на него не распространяется действие общих установок брандмауэра. Если флажок установлен, а настройки брандмауэра очень строги, то можно, нажав кнопку **Параметры** (рис. 5.7), установить разрешения для этого подключения. На другие подключения эти параметры распространяться не будут.

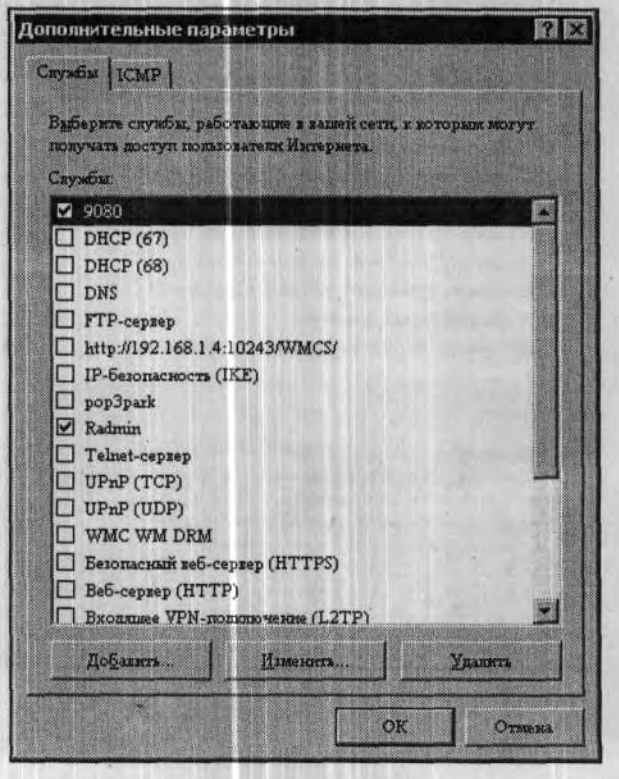


Рис. 5.7. Окно **Дополнительные параметры**

Таким образом, есть возможность довольно тонкой настройки брандмауэра, что при работе с несколькими сетевыми подключениями очень полезно.

Маршрутизация

Современные сети без маршрутизаторов представить сложно. В одних случаях маршрутизаторы аппаратные, в других — это программные устройства. Даже обычный общий доступ к Интернету, настроенный через использование общего подключения, обеспечен программным маршрутизатором.

Но раз настройка общего доступа в Интернет — это настройка маршрутизатора, то нельзя ли использовать эту настройку не для общего доступа в Интернет, а для маршрутизации между локальными сетями? Можно. Специалисты в области маршрутизации могут сказать, что это можно и просто вручную с помощью команды `route add` сделать. Но это для специалистов просто. Для вас тоже станет не очень сложно, когда вы рассмотрите таблицы маршрутизации на уже работающем маршрутизаторе.

Итак, предположим, что для более надежной защиты информации вы решили создать вторую сеть, которая будет брать данные из основной сети, но к ней самой добраться не очень просто. (Такой вариант сети может пожелать руководство офиса.) Возьмем за основу проекта уже созданную сеть из двух компьютеров с доступом в Интернет (см. рис. 4.38). Добавим еще один компьютер, принадлежащий другой сети, а для его физического подключения к сети применим еще один коммутатор.

Получится схема сети, показанная на рис. 5.8. Новому компьютеру (компьютер № 3) присвоим IP-адрес 192.168.6.6 с маской подсети 255.255.255.0. На компьютер № 1 добавим второй сетевой адаптер. Подключение, связанное с этим адаптером, сделаем общедоступным, но после завершения работы мастера установки домашней сети или сети малого офиса изменим IP-адрес на 192.168.6.5. При этом, как мы уже знаем, не будет включен DHCP-сервер, и все IP-адреса мы сможем назначать самостоятельно. На компьютере № 3 остается указать IP-адрес 192.168.6.5 в качестве шлюза.

Все! Теперь, с компьютера № 3 мы можем, выполнив команду `ping` на адрес 192.168.1.2, убедиться, что с ним есть связь. Связь будет и с любым другим компьютером сети 192.168.1.0. Более того, по IP-адресу будут доступны и узлы Интернета. Чтобы они стали доступны по символьным адресам, потребуется для компьютера № 3 указать еще IP-адрес (или адреса) доступного DNS-сервера. Если этот компьютер под управлением ОС Windows 98, то придется перезагружать его при каждом добавлении или изменении IP-адресов.

Попробуйте теперь "пинговать" компьютер № 3 с компьютеров сети 192.168.1.0, кроме компьютера № 1 (он маршрутизатор). Результат будет отрицательным. Некоторое неудобство в работе с сетью с компьютера № 3 создает то, что в сетевом окружении компьютеры соседней сети не видны. Для оперативного доступа к ним следует через средство поиска компьютеров найти их по IP-

адресу, после чего создать для каждого ярлык на рабочем столе или в отведенной для этого папке. Поиск по имени, к сожалению, не приведет к положительному результату. Но поставленная задача решена. Компьютеры из нашей скрытой сети смогут даже использовать принтеры из основной сети, если к ним обеспечен общий доступ.

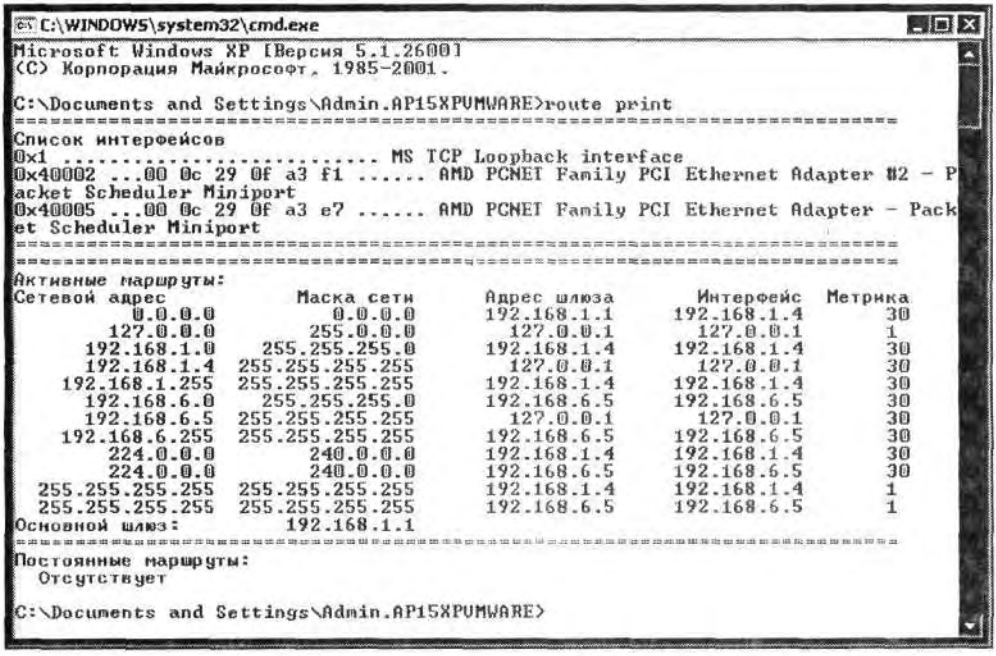


Рис. 5.8. Маршрутизация в локальной сети

Теперь вы можете изучить таблицу маршрутизации компьютера № 1 (рис. 5.9). Windows XP позволяет создавать маршруты вручную. Если в сети возникла необходимость создать маршрутизатор, можно сравнить имеющуюся в системе таблицу маршрутизации с той, что получилась у нас, и дополнить ее недостающими маршрутами, создав для удобства работы пакетный файл, содержащий необходимые команды добавления маршрутов.

Для всех этих операций следует применять команду `route` с соответствующими параметрами. Для просмотра имеющейся таблицы применяется команда `route print`. На экран будет выведена таблица, подобная изображенной на рис. 5.9. Недостающие маршруты (с учетом, конечно, тех IP-

адресов, с которыми придется работать), можно добавлять командой `route add`. Причем если команда будет с параметром `-p`, то маршруты будут записаны в реестр и сохранятся после перезагрузки. Без этого параметра маршруты будут действовать только в течение текущего сеанса.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Admin.AP15XPVMWARE>route print
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x40002 ...00 0c 29 0f a3 f1 ...... AMD PCNET Family PCI Ethernet Adapter #2 - P
acket Scheduler Miniport
0x40005 ...00 0c 29 0f a3 e7 ...... AMD PCNET Family PCI Ethernet Adapter - Pack
et Scheduler Miniport
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети       Адрес шлюза     Интерфейс  Метрика
          0.0.0.0          0.0.0.0     192.168.1.1    192.168.1.4      30
        127.0.0.0        255.0.0.0       127.0.0.1      127.0.0.1       1
      192.168.1.0    255.255.255.0     192.168.1.4    192.168.1.4      30
      192.168.1.4  255.255.255.255       127.0.0.1      127.0.0.1      30
    192.168.1.255  255.255.255.255     192.168.1.4    192.168.1.4      30
      192.168.6.0    255.255.255.0     192.168.6.5    192.168.6.5      30
      192.168.6.5  255.255.255.255       127.0.0.1      127.0.0.1      30
    192.168.6.255  255.255.255.255     192.168.6.5    192.168.6.5      30
        224.0.0.0        240.0.0.0     192.168.1.4    192.168.1.4      30
        224.0.0.0        240.0.0.0     192.168.6.5    192.168.6.5      30
  255.255.255.255  255.255.255.255     192.168.1.4    192.168.1.4      1
  255.255.255.255  255.255.255.255     192.168.6.5    192.168.6.5      1
Основной шлюз:        192.168.1.1
===========================================================================
Постоянные маршруты:
  Отсутствует

C:\Documents and Settings\Admin.AP15XPVMWARE>
```

Рис. 5.9. Таблица маршрутизации компьютера № 1

Синтаксис команды `route` такой:

```
Route add [-p] <сетевой_адрес> mask <маска_сети> <адрес_шлюза> metric
<m> if <ni>
```

Здесь `m` — метрика, или число "прыжков", необходимое для достижения адреса, `ni` — номер интерфейса. Если не известно точное значение метрики, то можно указать, как при автоматическом создании таблицы, число 30. Номер интерфейса можно увидеть в верхней части таблицы маршрутизации, выведенной командой `route print`. В нашем примере это 0x1 и 0x40002, где x — латинская.

Поместив последовательно в пакетном файле команды добавления маршрутов, вы можете тут же проверить правильность добавления командой `route print`.

Для удаления маршрутов вместо `route add` следует писать команду `route delete` с указанием тех же адресов, масок, шлюзов и номеров адаптеров. Для изменения без удаления можно применить команду `route change`, опять же со всеми данными.

Для настройки самих подключений в том же пакетном файле перед командами добавления маршрутов можно поместить команду `netsh`.

Эта команда позволяет:

- сбросить настройки подключения:

  ```
  netsh int ip reset "C:\Documents and Set-
  tings\Administrator\Desktop\adsl\resetip.txt"
  ```

  при сбросе настроек указывается путь и файл, в который должны быть записаны сведения о сбросе;

- указать новые настройки:

  ```
  netsh int ip set address "<имя_подключения>" static <IP-адрес>
  <маска_сети> <адрес_шлюза> <метрика_шлюза>
  ```

- указать DNS-серверы:

  ```
  netsh int ip set dns "<имя_подключения>" static <IP-адрес_DNS-
  сервера>
  ```

- добавить IP-адреса для соединения, если их несколько:

  ```
  netsh int ip add address name="<имя_подключения>" gateway=<IP-
  адрес_шлюза> gwmetric=<метрика_шлюза>
  ```

Эти команды позволят создавать временные маршрутизаторы и настройки подключений с помощью командных файлов. Кто-то может спросить, а зачем? Ведь сети создаются не на пять минут, и обычно не приходится менять настройки сети оперативно. С одной стороны это так, но все большее распространение получают мобильные компьютеры. Они часто стали заменять рабочую станцию на работе и дома, а также в других сетях, если пользователю в них приходится работать. При этом, подключаясь к сети, приходится изменять настройки компьютера, что меня, например, очень раздражало. Создав несколько командных файлов, содержащих настройки компьютера для различных сетей, можно в течение нескольких секунд перенастраивать свою машину в зависимости от места ее включения. В отдельных случаях и настройка рабочей станции может требовать оперативного изменения сетевых настроек для усиления защиты информации. При этом пакетные файлы с командами настройки можно хранить на "флэшке" или в зашифрованном виде на самой рабочей станции.

Шифрование

В одноранговых сетях доступ к зашифрованным файлам и папкам возможен только с самой рабочей станции и только для той учетной записи, от имени которой проводилось шифрование. Сама процедура шифрования чрезвычайно проста. Создав каталог, в котором предполагается хранить файлы в зашифрованном виде, просто поместите в него требуемые файлы. Для самого каталога перед этим следует указать свойство **Шифровать содержимое для защиты данных** (рис. 5.11). Это свойство доступно в окне, которое можно вызвать, нажав кнопку **Другие** в окне свойств каталога (рис. 5.10). После того как у каталога установлено данное свойство, все файлы, помещаемые в него, будут зашифрованы. В свойствах каждого файла при нажатии кнопки **Подробно** можно указать дополнительные учетные записи, для которых файлы могут быть доступны (рис. 5.12).

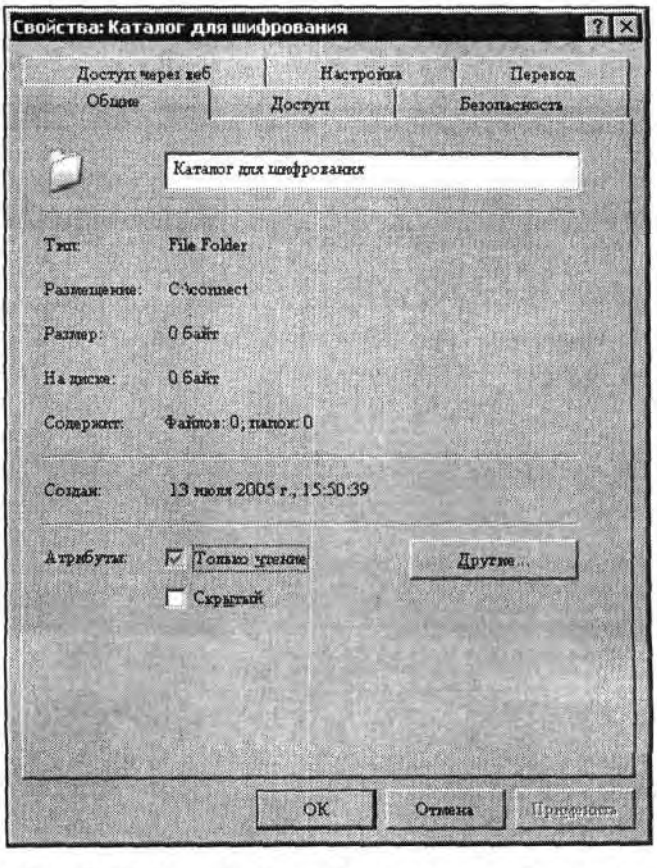


Рис. 5.10. Окно **Свойства: Каталог для шифрования**

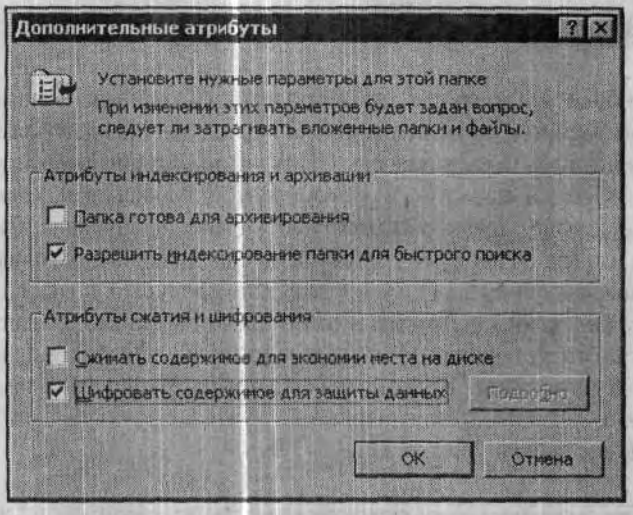


Рис. 5.11. Окно **Дополнительные атрибуты**

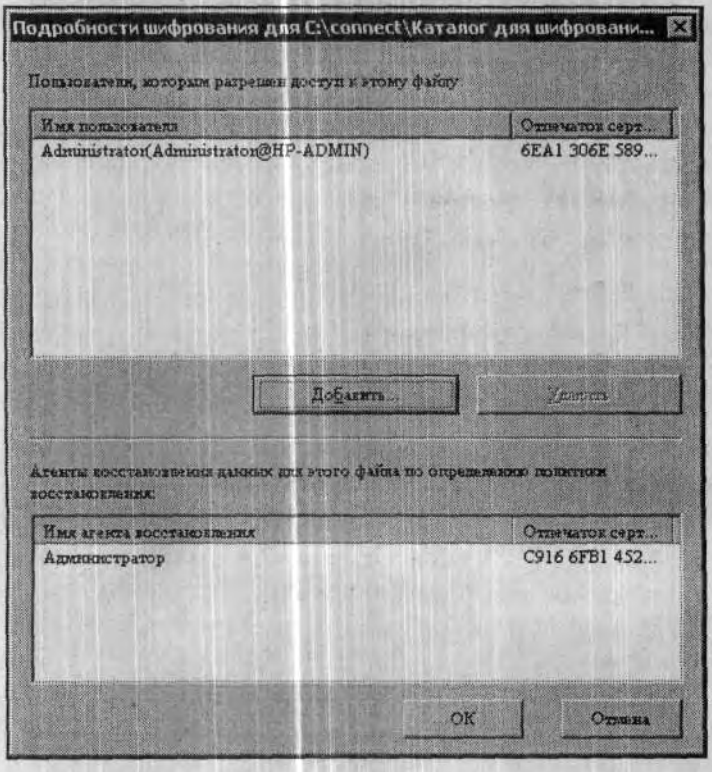


Рис. 5.12. Окно **Подробности шифрования для <имя_каталога>**

Антивирусная защита

Этот вопрос в любой сети стоит всегда очень остро. Во-первых, компьютеры сети необходимо защищать, во-вторых, большая часть имеющихся на рынке антивирусных средств не бесплатны. Иногда можно совершенно официально бесплатно использовать полноценно работающую антивирусную программу, но ограниченное время. Самый простой способ обеспечить нормальную защиту сети — приобрести антивирусный пакет. Иногда пользователи домашних ПК (и не только домашних) принципиально не желают покупать антивирусные пакеты, считая, что такие программы для индивидуальных пользователей должны быть бесплатными. Как ни странно, такого же мнения и некоторые разработчики антивирусных пакетов. Я, например, совершенно бесплатно и легально использую ТРИ программы, которые помогают защищать мои компьютеры и сети.

Anvir Virus Destroyer (AnVir Task Manager)

По адресу **http://anvir.com/index_ru.htm** можно найти очень компактную (всего 153 Кбайт), работающую под всеми операционными системами семейства Windows программу, позволяющую уничтожать многие известные вирусы. Неизвестные вирусы программой могут быть обнаружены до начала их разрушительной деятельности в момент их проникновения в ваш компьютер и/или внесения изменений в реестр с целью самозапуска при очередной загрузке компьютера. При изменении записей в реестре программа предупреждает пользователя об этом событии. Остается средствами самой программы просмотреть измененные записи, запретить запуск вредоносной программы, удалить файл вируса. Во время эпидемии вируса MSBLAST программа исправно обнаруживала его проникновение в компьютер, и ни разу заражение не произошло.

Если предприняты меры предосторожности при работе с электронной почтой, когда вы сами не открываете подозрительные файлы и удаляете их, то вирусам остается надеяться лишь на автоматический запуск, который и исключается этой программой.

Кроме того, программа позволяет управлять процессами, идущими на компьютере. В любой момент любой процесс можно остановить, например, для освобождения памяти.

Программа имеет русскую бесплатную версию. Интерфейс абсолютно понятен. Может работать как на рабочей станции, так и на сервере.

Avast!

На официальной странице программы в Интернете есть такие слова:

"Avast! 4 Home Edition — полнофункциональный антивирусный пакет, разработанный исключительно для домашних пользователей. Данный продукт распространяется бесплатно, позволяя тем самым избежать глобальных вирусных эпидемий. Кроме того, многие пользователи не могут или не желают платить за антивирусное программное обеспечение".

По адресу **http://www.avast.ru/Free_avast_home_edition.htm** можно получить программу и ее подробное описание.

После опробования программы, если она вас устроила, следует зарегистрироваться на сайте разработчика и получить лицензионный ключ. Если в течение 14 месяцев вам не разонравилась эта программа, то можно зарегистрироваться повторно и продолжать ее использовать, получая регулярные обновления и поддержку. Интересно, что регулярные обновления имеют объем до 30 Кбайт, а крупные обновления не превышают 300 Кбайт.

Серверная версия программы не бесплатна.

Microsoft AntiSpyware

Это бесплатная программа от Microsoft. Скачать ее можно по адресу: **http://www.microsoft.com/athome/security/spyware/software/default.mspx**. В настоящий момент выпускаются бета-версии программы, имеющие ограниченный срок работы. Но до окончания этого срока становится доступна очередная версия. Обновления автоматические. Программа находит и уничтожает так называемые Spyware. Spyware — это программы, многие из которых официально не считаются вирусами. Но они заставляют вас регулярно получать рекламную информацию, часто собирают статистику посещений Web-страниц с целью избирательного действия рекламы, которую вам показывают. На один из компьютеров эту программу поставили на всякий случай. В его работе не замечалось каких-либо проблем. Установив и запустив программу, мы обнаружили девятнадцать(!) этих "не вирусов", после удаления которых компьютер стал работать существенно быстрее. Единственный недостаток, обнаруженный мной у этой программы, — она не имеет русского интерфейса.

Существуют и online-средства, позволяющие обнаружить и уничтожить вирусы на дисках вашего компьютера. Одно из них опять от Microsoft — **http://www.microsoft.com/security/malwareremove/default.mspx**.

Это средство обновляется ежемесячно и доступно с обновлениями операционной системы.

Реальные ситуации

На мой взгляд, описанного антивирусного комплекта вполне достаточно, чтобы бесплатно обеспечить антивирусную безопасность небольшой сети.

Но не только внешние опасности могут угрожать информации в сети. Некорректные действия администратора могут иметь более разрушительную силу, чем вирусы. И наоборот, если действия администратора продуманы и спланированы, то даже серьезные проблемы могут быть преодолены почти без осложнений для работы пользователей сети. В качестве подтверждения сказанному предлагаю описание реальных ситуаций, связанных с реорганизацией сети, работой ее администратора, а также имеющих прямое отношение к защите информации в сети.

Великое переселение

Теперь об этом вспоминают редко — к хорошему привыкают быстро. Наша сеть сейчас — это более сорока приличных компьютеров, два сервера, выполняющие важные вычислительные и коммуникационные задачи, внутренняя и внешняя электронная почта, Интернет для всех, кому он необходим, Web-сайт для служебного пользования, связь с сетями родственных организаций. И все это, включая поддержку половины активно работающих программ, исправно функционирует благодаря работе коллектива IT-отдела, не просто небольшого, а очень даже маленького. Ядро отдела, которое не поддавалось искушению сменить в трудные времена место работы, — два человека, включая меня, и было тем двигателем прогресса в нашей сети, который привел, в конце концов, к теперешнему ее состоянию.

А пару лет назад...

...я был приглашен в серьезную организацию для осуществления поддержки работоспособности сети, которая на тот момент состояла из пятнадцати компьютеров, десять из которых находились в компьютерном классе, куда в течение рабочего дня сходился народ из различных отделов, чтобы поработать на свободном в настоящий момент компьютере. Компьютеров катастрофически не хватало, NetWare-сервер с объемом оперативной памяти 64 Мбайт круглосуточно трудился, днем выдавая и получая от пользователей файлы, следя за правами доступа и обеспечивая сохранность разнообразной информации, доверенной ему пользователями и созданной им самим, а ночами общаясь с рабочей станцией, на которой запускалась программа обработки собранных за день данных.

Сервер, компьютеры, принтеры, пользователи, немногочисленный персонал IT-отдела, подобно стихийно сложившемуся экипажу, плыли через рабочий день в компьютерном классе, как в Ноевом ковчеге, собравшем в себе все, что необходимо, и всех, кто необходим, для работы сети. За бортом, однако,

был не безбрежный и пустынный океан, а огромный архипелаг, на островах которого проживали народы, уже знакомые с Windows 2000 Server и другими прелестями информатизации и компьютеризации. Тонкая ниточка dial-up-соединения связывала Ноев ковчег с внешним миром, откуда иногда поступала информация о том, что есть люди, которые имеют возможность работать с персональным компьютером, не выходя из своего кабинета, и более того, это считается нормальным.

Личный пример — лучший способ воздействия на массы. Я приобрел (само собой, не за свои) не слишком дорогой, но приличный компьютер со сканером, источником бесперебойного питания и 17-дюймовым монитором, который оказался самым крупным (читай — крутым) в организации. На этот компьютер была установлена Windows 98 — штатная система нашего программного комплекса, а в качестве второй системы пиратская версия Windows 2000 Server для проведения экспериментов. В первые дни работы нового компьютера, стоило мне отойти от него на расстояние более полутора метров, кто-нибудь из населения Ноева ковчега стремился притулиться к нему и понажимать кнопки клавиатуры в своих бескорыстных, сугубо производственных целях, и очень удивлялся, когда я вежливо просил пересесть к другой машине. Мотивировал я свою просьбу очень просто: "Этот компьютер работает неправильно, вашу работу придется переделывать". Через несколько дней я уже мог, оставив не надолго рабочее место, быть уверенным, что никто его не займет.

Компьютерный класс оказался очень удобным полигоном для сетевых экспериментов. Расположенные в одном помещении сервер и рабочие станции позволяли оперативно проверять различные варианты сетевых настроек. Тогда были опробованы практически все возможности нового сервера. Стало понятно, что переход на него действительно необходим.

Но само по себе сознание необходимости перемен не приведет к переменам. Требовалось убедить руководство организации в необходимости этих перемен и связанных с ними затрат. На тот момент высшее звено организации практически не использовало компьютеры в служебных целях и официально высказывалось мнение, что компьютеры — это роскошь — "считали столько лет вручную, и пусть считают". А тут не просто новые компьютеры, а реорганизация сети. Требовался новый сервер, перекладка старых и прокладка новых кабельных линий. Общее число компьютеров, необходимость приобретения которых уже определилась на тот момент, было около двадцати. Для небогатой организации, где руководство не очень хорошо представляет себе выгоды компьютеризации, планы несбыточные. Переселение из Ноева ковчега в комфортабельный лайнер новой сети появлялось в мечтах, снах и не слишком предметных разговорах внутри отдела.

Несмотря на неопределенность в сроках, постепенно составлялся план преобразований в сети. Было предчувствие скорых и неожиданных перемен,

подготовка к которым и проводилась все свободное время, появившееся за счет автоматизации некоторых ежедневных и весьма продолжительных операций.

Совершенно неожиданно для руководства приходит информация от фирмы-разработчика основного программного комплекса, применяемого в нашей организации, о прекращении в ближайшее время поддержки версии под NetWare и необходимости перейти на Windows 2000 Server(!). Мы этого момента ждали и были к нему готовы. После приобретения нового компьютера и установки на него необходимого программного обеспечения переход уже несколько подросшей сети на новый сервер занял один день. Накануне, конечно, на всех рабочих станциях была осуществлена предварительная подготовка второго варианта сетевого подключения.

Оставалась еще одна задача. Очень хотелось обезопасить сервер от любопытных пользователей, которые постоянно ходили около него и иногда пытались поработать за ним.

На этот раз мечта осуществилась по причине структурных преобразований в организации, которые заставили наш отдел поменять этаж. Уже было приобретено некоторое число компьютеров, что позволило сократить численность экипажа Ноева ковчега и количество машин в компьютерном классе.

Теперь перед нами была задача — не прерывая работу сети, подготовить и осуществить перенос отдела в новое помещение, где серверам отводилась отдельная изолированная площадь.

Заранее были проложены новые кабели, подготовлено активное сетевое оборудование, организовано временное подключение сервера к новому коммутатору, расположенному на новом этаже. По очереди рабочие станции переключались на новые линии или старые линии переключались на новые коммутаторы. Наконец, наступил момент, когда оставалось переселить только один сервер. Эта операция была осуществлена в течение одного обеденного часа.

Все дальнейшие преобразования в сети проводились планомерно и почти без стрессовых ситуаций. Пришлось доказать необходимость установки кондиционера в отделе для обеспечения нормального самочувствия серверов. А однажды потребовалось изменить адрес нашей сети, т. е. поменять адреса всех рабочих станций, сетевых принтеров, маршрутизаторов и серверов.

Вот как это было

Итак, в нашей сети произошло знаменательное событие — сеть перешла на Windows 2000 Server. Если учесть, что до этого момента сервер был не Windows, к тому же совсем не новый, возможности, появившиеся в сети с появлением 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 возможностей новой системы делали работу увлекательной. Был один неприятный момент, который ограничивал свободу выбора, — это Интернет через dial-up. Организация IP-адресов в сети не позволяла применить простые методы создания общего доступа к глобальной сети через новый сервер. Известное же своими возможностями и относительной сложностью настроек NAT (Network Address Translation, преобразование сетевых адресов) требовало выделения определенного пула адресов провайдером, что на тот момент было нереальным для нас. Тем не менее, я прошел практически весь путь настройки общего доступа к Интернету через NAT и dial-up. Но не стал возвращать настройки сервера в исходное состояние, поскольку их текущий статус не мешал нормальному функционированию сервера, 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 с нашей сетью сеть достаточно крупного удаленного офиса. 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 ничего 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? Ответов нет. Звоню знакомому специалисту по сетям. Через час он у меня в серверной, сидим вместе, меняем и возвращаем старый адрес. Никаких идей. Вспоминаем про второй сетевой адаптер, имеющийся на 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 "логи" системы, 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 пиратами версиях. Сама операционная система никак не реагирует на неполадку, никаких сообщений о конфликтующих службах или программах нет. Принимается решение привлечь дополнительные 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 своих 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.

Выбор режима работы сервера

Надеюсь, что приведенная история содержит много полезной фактической и эмоциональной информации для получения представления о мерах, необходимых для организации или реорганизации сети. Если сервера в вашей сети еще нет, ничего не меняется, следует лишь решить вопрос о его назначении. Несмотря на то, что для кабельной системы и прочего сетевого железа обычно не важно, какие задачи выполняет сервер, для вас незнание более или менее конкретно будущих задач сервера может привести к сложно решаемым ситуациям. Постарайтесь как можно более внимательно познакомиться с описанием операционной системы, которая будет установлена на сервер. Приведу пример ситуации, в которой оказались администраторы сети, не познакомившиеся заранее с новой операционной системой в достаточной степени.

В этой сети, как когда-то и в нашей, работал NetWare-сервер. Возникла необходимость замены сервера с переходом на Windows 2000 Server. Администраторы сети не придали серьезного значения предварительному изучению возможностей операционной системы. Более того, установка на новый сервер операционной системы, а также ее предварительная настройка была доверена некой небольшой организации, у которой приобретался сам компьютер. В результате в определенный момент сервер заработал, были подключены пользователи, а администратор наслаждался возможностями терминального доступа к серверу со своей рабочей станции. Но однажды он позвонил мне и взволнованно поведал, что пропала возможность терминального доступа.

Несколько вопросов с моей стороны прояснили ситуацию. Закончился срок лицензии для работы сервера приложений. Именно в режиме сервера приложений был сконфигурирован новый сервер. При этом никто не задумался о приобретении неограниченных лицензий для работы с таким сервером. Еще несколько вопросов привели к осознанию того, что сам режим сервера приложений был не нужен. Следовало переконфигурировать сервер в режим

файлового сервера. При этом два терминальных подключения для администраторов будут работать без ограничения времени. Сама операция изменения роли сервера не сложна. Необходимо лишь выбрать необходимый режим работы в настройках сервера и следовать указаниям на экране. Одно из таких указаний требует вставить диск с дистрибутивом операционной системы в дисковод.

Одна из рекомендаций компании Microsoft в отношении установки своих продуктов, говорит о том, что лучше дистрибутив переписать на жесткий диск, а с него производить установку. На дисках сервера обычно места достаточно, чтобы разместить там дистрибутивы, но в данном случае не оказалось человека, заинтересованного в выполнении этой рекомендации. Не оказалось заинтересованного человека и для того, чтобы проверить наличие дистрибутивов при получении компьютера.

Дальнейшие события не представляют интереса с точки зрения практики организации работы сети. И так уже понятно, что без четкого плана работа администратора сети может стать не только малоэффективной, отнимающей нерационально много времени, но с большой вероятностью приведет к очень серьезным проблемам.



ЧАСТЬ III

Переход на выделенный сервер

ЧАСТЬ III

ПЕРЕХОД НА ВЫДЕЛЕННЫЙ СЕРВЕР

Как бы хорошо не работала ваша одноранговая сеть, придет момент, когда вы устанете ходить от компьютера к компьютеру, меняя настройки, подыскивая рабочие станции, которые можно использовать для общего доступа к необходимой информации. А если потребуется свой Web-сервер, на какой рабочей станции его можно поместить? На собственном компьютере вы не сможете поместить все сервисы, которые предполагается сделать общедоступными. Если считать, что на каждом компьютере должны быть общедоступные ресурсы, то на каждом компьютере необходимо заводить учетные записи для всех пользователей сети! Когда в сети только три рабочие станции, это не сложно, но когда их число будет расти, а территория, занимаемая сетью, тоже будет расширяться, администрировать сеть будет все сложнее и сложнее. Значительные трудности возникнут в отношении сохранения режима доступа к информации. Если на каждом компьютере есть учетная запись администратора и это ваша учетная запись, то при необходимости сменить пароль администратора понадобится оперативно обойти все рабочие станции. Словом, расширяющаяся сеть не может оставаться одноранговой. Необходима некоторая централизация, как в управлении сетью, так и с размещением общедоступных ресурсов.



Глава 6

Планируем сеть и свою работу в ней

Собираясь делать кардинальные преобразования в сети, а переход от одноранговой сети к иерархической — это действительно кардинальное преобразование, — необходимо все спланировать с учетом дальнейшего развития сети. Если сеть работает давно, и в ней сложились определенные традиции, как технологические, так и политические (в смысле политики администрирования), изменение ее структуры, связанное с переходом на работу с выделенным сервером, может быть процессом достаточно болезненным. Судя по информации с форумов в Интернете, есть администраторы, работающие с одноранговыми сетями, в которых более двадцати компьютеров. Они не пытаются перейти на централизованное управление сетью, вероятно, в связи с теми традициями, которые сложились в сети, и боязнью нарушить порядок, который сложился в работе этой сети. Но я не завидую таким администраторам. Только их привычка и знание своей сети, сложившееся постепенно в процессе ее расширения, позволяют им поддерживать свою сеть в нормально работающем состоянии. Если число рабочих станций в сети предполагается более пяти, то имеет смысл сразу создавать сеть с выделенным сервером. Если же случилось так, что ваша сеть выросла, центрального сервера в ней нет, но явно видна необходимость преобразований, следует спланировать преобразования так, чтобы переход сделать наименее болезненным.

Перед составлением плана преобразований желательно проанализировать сложившуюся структуру сети, характер задач, выполняемых пользователями, принадлежность пользователей к административным или тематическим группам, наличие программ, которыми пользуются группы пользователей, общее число пользователей и рабочих мест, потребности во внедрении серверных версий программ, режим использования принтеров и потребность в печатных работах у групп пользователей. Число параметров, по которым следует анализировать работу сети, может быть довольно большим. Здесь и административные взаимоотношения между пользователями, требования и пожелания руководства, если оно есть, а может быть и некомпетентность

руководства в вопросе развития информационных технологий. Это тоже надо учитывать, чтобы не вызвать сопротивление руководства.

Предложив когда-то своему руководителю внедрить почтовый сервер, дать возможность каждому пользователю сети иметь свой почтовый адрес, я получил очень вежливый отказ. Не было резкого противодействия, было только непонимание преимуществ, которые получат пользователи сети, и непонимание выгод, которые может принести это преобразование. Оставалось просто установить бесплатный почтовый сервер, зарегистрировать на нем руководителя, а в удобный момент настроить на его компьютере почтовый клиент. (Системный администратор, к счастью, имеет практически неограниченный доступ к рабочим станциям пользователей независимо от их ранга.) Один раз руководителю была показана процедура получения почты, которую пока пересылал ему я сам. Через пару недель пересылку почты я прекратил. Еще через пару дней руководитель задал вопрос: «Почему перестала приходить почта?». Ну вот процесс и пошел...

Пользователи должны осознать и почувствовать необходимость и полезность преобразований. Тогда вы получите поддержку как моральную, так и материальную.

Вариантов воздействия на сознание пользователей может быть много. В одной из сетей, где не только централизованного управления не было, но даже необходимый для этого протокол TCP/IP не применялся, процесс осознания начался с настройки общего доступа к дорогостоящим принтерам, дефицит которых ощущался очень явно. Руководство, увидев экономию, созданную некоторой реорганизацией в сети, а после этого благосклонно выслушав возможные перспективы развития сети, приняло решение о выделении средств на приобретение сервера.

Найдя в результате анализа "тонкие" места в работе сети, а может быть и в применяемых информационных технологиях, надо начинать с малого, но полезного преобразования.

Примерим организацию одноранговой сети к возможностям сервера Windows Server 2003.

Группы пользователей

В одноранговой сети, содержащей большое число компьютеров (более десяти), нередко пользователи (если точнее, то их учетные записи) разбиты по рабочим группам. В каждую рабочую группу входят определенные рабочие станции. В сетевом окружении компьютера, принадлежащего к рабочей группе, видны компьютеры как своей, так и других рабочих групп, но каждая рабочая группа, как контейнер, содержит лишь свои компьютеры. Но деление на рабочие группы довольно условно. Трудно реально использовать

это деление при управлении сетью и организации ее работы. На рабочих станциях под управлением Windows 2000 или Windows XP можно упорядочить учетные записи локальных пользователей по группам учетных записей. Каждой группе можно назначать определенные права на рабочей станции, которые получат и учетные записи, помещенные в ту группу.

Сервер под управлением Windows Server 2003, при условии установки службы каталогов (Active Directory), позволяет создавать учетные записи, действие которых будет распространяться на всю сеть, на все рабочие станции. Роль локальных учетных записей на рабочих станциях в этом случае сводится в основном к возможности загрузки без подключения к сети.

Достаточно на сервере иметь учетную запись, чтобы задать ей все необходимые права в сети. Там же на сервере можно создать группы учетных записей, для которых тоже можно установить соответствующие права. Кроме групп, которым могут назначаться права в сети, можно создавать так называемые организационные единицы (Organization Unit, OU). Иначе эти организационные единицы называют подразделениями или контейнерами, что соответствует практически рабочим группам одноранговой сети. В OU можно помещать учетные записи пользователей, их группы и даже сетевые устройства, принтеры, например. OU внутри себя могут содержать другие подразделения с практически неограниченной возможностью вложения одно в другое.

На рис. 6.1 приведено окно, содержащее дерево подразделений с учетными записями пользователей и контейнерами, содержащими другие объекты сети. Выделен контейнер с учетными записями компьютеров, перечень которых виден в правой части окна. Для OU нельзя назначать права, но можно все учетные записи пользователей, находящиеся в подразделении, помещать в какую-либо группу, присваивая этим учетным записям соответствующие группе права. В группы можно помещать не только учетные записи пользователей, но и учетные записи компьютеров, наделяя компьютеры дополнительными правами или, наоборот, ограничивая их права в сети.

Ко всем объектам, входящим в Active Directory, возможен доступ из командной строки. Для обращения к объектам в командах применяют специальное обозначение, после которого через знак равенства указывается имя объекта.

- CN = Контейнеры, пользователи, контакты, группы и другие объекты которые обычно не имеют дочерних объектов. (От common name — общее имя.)
- OU = Организационные модули, которые содержат такие объекты, как пользователи, контакты, группы и др.
- DC = Доменные контейнеры, которые создаются отделением полного внутреннего доменного имени. (От domain component — компонент домена.)

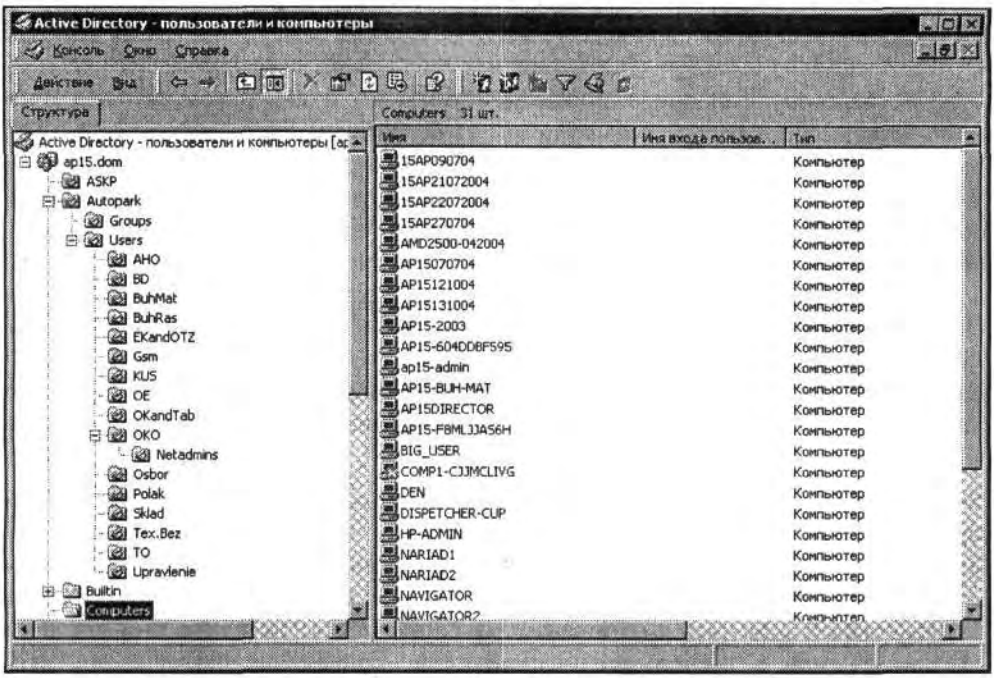


Рис. 6.1. Окно **Active Directory - пользователи и компьютеры**

На рис. 6.1 можно найти подразделение **OKO**. Для обращения к этому подразделению в командах будет применяться такая запись:

```
//OU=oko,OU=users,OU=autopark,DC=ap15,DC=dom"
```

Эта запись обозначает, что подразделение **OKO** вложено в подразделение **users**, вложенное в подразделение **autopark**, которое, в свою очередь, принадлежит домену **ap15** в домене верхнего уровня **dom**.

Такие логичные построения позволяют довольно легко ориентироваться при подготовке команд управления Active Directory, написании сценариев, которые оказывают серьезную помощь администратору доменной сети при чтении результатов выполнения команд и сценариев.

Рассматривая учетные записи, мы встретились с понятием *домен*. Это основная логическая единица службы каталогов. Обычно в небольших сетях не возникает такой необходимости, но доменов в сети может быть несколько. Более того, домены могут объединяться корневым доменом, корневые домены могут объединяться в лес доменов. Но нас будет интересовать лишь один домен, а все более крупные структуры могут присутствовать в сетях довольно большого размера и здесь приведены только для указания на возможности построения сетей на базе ОС Windows Server 2003.

Операционные системы в сети

В качестве серверной операционной системы мы будем рассматривать Windows Server 2003. Многие возможности этой системы были доступны и в ОС Windows 2000 Server, но не все. В качестве ОС для рабочих станций в сети с Windows Server 2003 могут применяться Windows 98, Windows 2000 и Windows XP Professional. Но, в отличие от других, Windows XP Professional поддерживает все возможности серверной ОС. Иногда могут применяться Windows 2000 и Windows 98, но при возможности их лучше постепенно заменять новой операционной системой. Во всяком случае на рабочей станции администратора должна быть только Windows XP Professional. Применение этой ОС на рабочих станциях позволит в полной мере использовать групповые политики. Это определенные правила безопасности, которые можно назначать объектам службы каталогов.

Если учесть, что в одной физической среде могут существовать разные логические сети, то в той же сети могут работать любые операционные системы, в том числе Linux и даже DOS. Но использовать в полной мере возможности сервера Windows Server 2003 они не смогут. Эти операционные системы могут работать в одноранговых сетях. Это значит, что они составят отдельную сеть в общей физической сети. Применяя протокол TCP/IP, можно будет организовать обмен информацией между этими сетями с помощью Web-сервера или FTP-сервера. Простые реализации данных серверов возможны даже для DOS.

В каких случаях есть смысл оставлять в сети рабочие станции со старыми операционными системами? В основном из соображений экономии. Если есть процесс, управление которым осуществляется рабочей станцией с DOS, и вас абсолютно устраивает это, то нет смысла устанавливать дорогую рабочую станцию с дорогой операционной системой, искать или писать программы, которые смогут выполнять старые задачи, но в новой ОС. Но если ранее эти рабочие станции не работали в сети, то, возможно, не удастся простым путем подключить их к ней. Проблемы могут быть в недостатке памяти. Если же задачи выполнялись рабочей станцией с ОС Linux, то она вполне может продолжать работу в новой сети.

Сервер терминалов

Среди достоинств Windows Server 2003 наличие встроенной возможности работы через терминальный доступ. Собственно сервер терминалов, позволяющий работать большому числу рабочих станций с ним, требует дополнительного лицензирования. Но можно использовать удаленный доступ к рабочему столу, который позволяет работать одновременно двум подключе-

ниям. Для этого Windows Server 2003 не надо конфигурировать как сервер терминалов. Основное назначение удаленного доступа к рабочему столу — это администрирование сервера. Но, при необходимости, вы можете предоставить возможность работы в удаленном режиме и кому-либо из пользователей сети.

Удаленный доступ к рабочему столу Windows Server 2003 отличается от аналогичной программы в Windows XP. Если в Windows XP подключение к рабочему столу приводит к скрытию рабочего стола текущего сеанса, либо блокировке сеанса, если рабочая станция зарегистрирована в домене, то в серверной ОС текущий сеанс остается в работоспособном состоянии. Кроме того, в Windows XP невозможно более одного удаленного подключения к рабочему столу.

Интересно, что компания ЭF1 (**http://www.ef1.ru/ef/about.htm**) разработала программные средства, позволяющие превратить Windows XP Professional в сервер терминалов. Число подключений к серверу при наличии у него достаточных ресурсов может достигать двадцати одного. Причем подключение к нему возможно с рабочих станций под управлением Linux.

С рабочих станций Linux, кроме того, можно подключаться к серверу терминалов с помощью специально разработанного для этой ОС приложения rdesktop, свободно распространяемого с дистрибутивами Linux. Одно из описаний реальной настройки подключения рабочих станций Linux к серверу терминалов с загрузкой по сети можно найти по адресу **http://www.markelov.net/articles.php?lng=ru&pg=48**.

В дистрибутиве Linux Fedora Core 3 есть встроенный терминальный клиент — Terminal Server Client на основе rdesktop. На рис. 6.2 показан момент подключения к Windows Server 2003 и управления этим компьютером через терминальный доступ.

Применение в сети компьютеров с не-Windows операционными системами вполне допустимо, если они позволяют решить стоящие перед ними задачи.

Использование сервера терминалов делает возможным применение парка устаревающих машин в сети, но при условии, что сам сервер установлен на мощной машине. Для средней сети сервер должен иметь частоту процессора не менее 3 ГГц и 1 Гбайт оперативной памяти. Но в совсем небольшой сети сервер терминалов может работать и на любом современном компьютере. Например, в домашней сети, содержащей три-четыре компьютера, один из которых современный, а остальные, мягко говоря, не новые, вполне возможно предоставить всем домашним пользователям ресурсы современного компьютера, если это необходимо. Причем, как уже стало ясно из вышесказанного, сервер терминалов Windows Server 2003 доступен не только пользователям Windows, но и приверженцам Linux, что послужит смягчению конфликтов, продолжающихся между двумя лагерями пользователей этих ОС с

момента появления Linux. Причем в маленькой сети совсем не обязательно получать лицензии на доступ к серверу терминалов, поскольку можно использовать два разрешенных сеанса для администраторов.

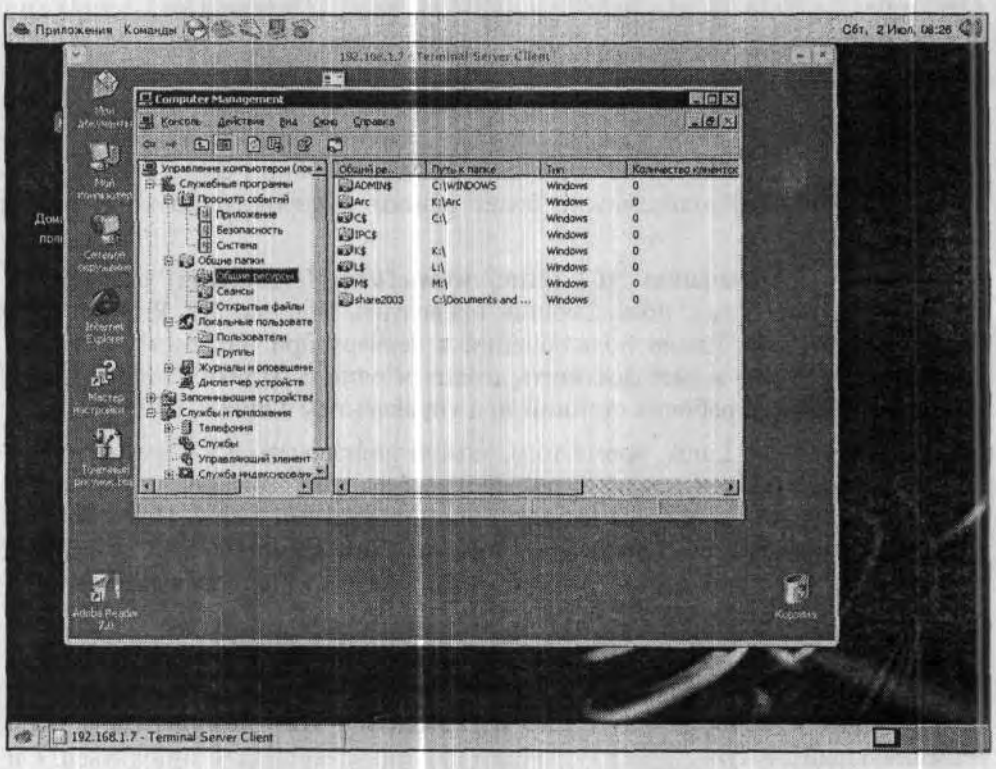


Рис. 6.2. Встроенный **Terminal Server Client** в ОС Linux (Fedora Core 3)

Для управления удаленной системой могут использоваться и программы удаленного администрирования типа VNC или Radmin, но они позволяют лишь подключиться к рабочему столу текущего локального сеанса, что не позволит использовать эту возможность вдвоем.

На сайте компании WTware (Windows Terminal ware) по адресу **http://www.wtware.ru** можно найти программное обеспечение для настоящих терминалов — бездисковых рабочих станций, которые могут подключаться к серверу терминалов, загружаясь по сети. Описание установки и настройки приведено на сайте разработчиков. Правда, это программное обеспечение не бесплатно.

Где поставим сервер

Если принято решение установить сервер, следует решить вопрос: «Где он будет установлен?». Ответ на этот вопрос зависит от того, какой режим работы предполагается у этого сервера, а также от того, насколько необходимо обеспечение бесперебойной работы и защиты данных.

Если это офисная сеть, то придется подумать об отдельном помещении или выделении некоторого пространства в офисе. Второй вариант может быть применен и в домашней сети.

Если требуется повышенная надежность работы сервера, то придется устанавливать источники бесперебойного питания, что тоже потребует места. В офисе можно воспользоваться рекомендациями из *главы 3*, где описан вариант размещения сервера в специальной стойке. Но в малом офисе и в квартире придется определяться самостоятельно. Важно исключить случайное повреждение сервера, его соединений с сетью, дополнительными устройствами. Один из важных факторов, имеющих большое значение при выборе места для сервера, — это шум, который он будет издавать во время работы. Особенно, если предполагается круглосуточная работа сервера. Если вы создали на этом сервере Web-сайт, то не рассчитываете, видимо, что посетители должны подчиняться вашему ритму жизни. Но шум сервера может элементарно мешать спать вам или членам вашей семьи. Даже когда этот шум днем кажется незначительным.

Выбор места для сервера не простое, ответственное дело. Можно рассмотреть варианты, которые применяются в известных домашних сетях.

- В квартире есть комната, в которой никто не спит ночью. Если в этой комнате есть компьютер, то и сервер вполне может в ней прижиться. Он может находиться рядом с компьютерным столом, например.
- В квартирах часто есть антресоли, которые содержат множество совершенно ненужных вещей. Если попытаться навести там порядок, то сервер мог бы поместиться и на антресоли. При этом естественным образом решается вопрос безопасности сервера от случайных повреждений.
- Существуют и разнообразные темные комнаты — кладовки. Если навести порядок, сервер может стоять именно там. Один мой знакомый вообще в такой комнате организовал свое рабочее место, разместив там и сервер, и рабочий компьютер и все необходимое оборудование.
- В моей домашней сети три компьютеризированных рабочих места и сервер. Пользователи этой сети не обращают внимания на шум этого оборудования. Хотя вполне возможно, что со временем, когда в семье появятся новые члены, которые менее дружелюбно настроены к шумя-

щим устройствам, придется решать проблему одним из описанных ранее путей.

- Не стоит помещать сервер на лоджиях и остекленных балконах. Помещение, в котором находится компьютер, должно быть отапливаемым.

Сети и подсети

Расширяя сеть и предполагая переход на работу с выделенным сервером, следует подумать не только о физической структуре сети, но и о логической структуре.

Рабочие группы, группы пользователей, организационные единицы — это структура определенной логической сети. Но, как мы уже говорили, в одной физической сети могут существовать логические сети, что может быть вызвано различными причинами. Для небольших сетей это обычно соображения безопасности.

Возможно сосуществование в одной физической сети двух логических сетей, одна из которых одноранговая, а другая управляется сервером. Но возможно, что одним сервером управляются две сети. Через два сетевых адаптера они могут подключаться к одному серверу. При этом каждая сеть может быть в отдельном домене, и общение между этими сетями возможно лишь при соответствующих административных настройках сервера. Проектируя новую или совершенствуя старую сеть, желательно рассмотреть необходимость организации таких сетей.

Отдельные компьютеры могут иметь более одного IP-адреса даже для одного сетевого адаптера. Это позволяет им работать в двух сетях сразу. Особенно полезна такая возможность при построении сетей, связанных с другими сетями. Например, требуется обеспечить безопасную связь с удаленной сетью через модем по выделенной линии. В точке соединения сетей установлен маршрутизатор, обеспечивающий возможность общения удаленной сети с нашей. Но для обеспечения информационной безопасности необходимо ограничить число компьютеров в нашей сети, к которым будут иметь доступ пользователи удаленной сети. Для этого маршрутизатор настраивается не на адреса нашей сети, а на адреса некоторой третьей сети, а отдельным компьютерам нашей сети присваиваются дополнительные IP-адреса из этого диапазона. Поскольку в локальных сетях адреса узлов должны соответствовать диапазону и маске, которые предназначены именно для этой сети, то компьютеры, не имеющие соответствующих адресов, не смогут войти в нее. На рис. 6.3 показана схема взаимодействия двух сетей по описанной технологии. На рисунке не показано, как организована модемная связь, поскольку вариант связи между сетями может быть любым, в том числе по VPN через Интернет, а модемная связь применяется реально в известных мне сетях.

Возможно, что сеть не имеет связей с другими внешними сетями (рис. 6.3), но по каким-либо причинам есть необходимость логически разделить участки сети. Один вариант разделения мы рассмотрели в *главе 5*, говоря о маршрутизации.



Рис. 6.3. Схема взаимодействия двух сетей

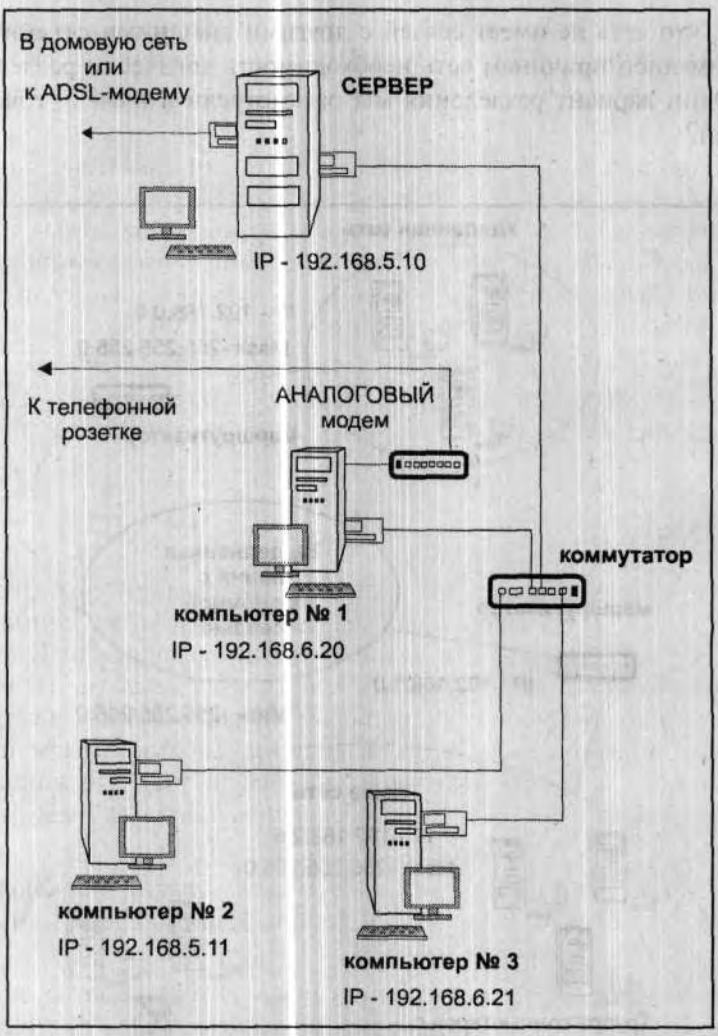


Рис. 6.4. Схема сети с двумя общими подключениями к Интернету

Есть ситуации, когда сеть делится не из соображений информационной безопасности, а в связи с необходимостью работать с ресурсами, доступ к которым невозможно организовать в одной логической сети. Так, в одной небольшой сети применяются два варианта доступа в Интернет. Была поставлена задача использовать оба варианта доступа в качестве общих, но для разных групп пользователей. Но если вы попытаетесь при наличии одного общедоступного подключения создать еще одно, операционная система не позволит этого сделать. В одной сети не должно быть двух общих подключений к Интернету. Но это ограничение можно обойти, если сеть разделить

на две подсети. Опять присвоим этим подсетям адреса из разных диапазонов. При этом логически сети будут разные, и операционная система не запретит использовать второе общее подключение при условии, что использоваться они будут каждое своей группой компьютеров.

Посмотрите на рис. 6.4. Компьютеры № 1 и № 3 принадлежат одной подсети, а компьютеры СЕРВЕР и № 2 — другой. Через СЕРВЕР и компьютер № 1 организовано общее подключение к Интернету, но по различным технологиям. Взаимодействие между компьютерами, принадлежащими разным подсетям, по обычной сетевой технологии невозможно. Но если в подсетях работают FTP или Web-серверы, то к ним доступ возможен.

Таким образом, мы можем создавать сети, отвечающие практически любым разумным требованиям, если будем использовать не только стандартную организацию малой сети, но и деление ее на логические сети и подсети.

Принтеры

Практически во всех локальных сетях используются принтеры. Создавая или расширяя (модернизируя) сеть, необходимо принимать во внимание появление новых принтеров и оптимизацию работы со старыми. Если принтер применяется только для работы конкретного пользователя, то вопросов с его подключением не возникает при любых преобразованиях в сети. В то же время общие принтеры должны быть доступны пользователям при любых преобразованиях. Если сеть делится на логические подсети, а принтер применяется только один, необходимо обеспечить доступ к нему из каждой подсети.

Есть два способа включения принтеров в сеть. Можно подключить его к рабочей станции и дать к нему общий доступ. Как это сделать, мы рассматривали в *разд. "Общий принтер" главы 4.*

Второй способ — это установить принт-сервер. Это устройство, которое может быть приобретено отдельно или уже встроено в новый принтер. Многие современные принтеры высокой производительности могут поставляться с встроенным принт-сервером.

Преимущество принт-сервера состоит в том, что для него не требуется отдельный компьютер, к которому необходимо подключить принтеры. Он просто включается в вашу сеть, как любой компьютер, и доступ к нему обеспечивается по TCP/IP-протоколу. То есть принтер в вашей сети имеет собственный IP-адрес, который вы можете задать для него через средства управления принтером. Реализация средств управления может быть различной, но очень часто применяется Web-интерфейс (рис. 6.5). Подключаясь к принтеру, как к обычной странице в Интернете, используя его IP-адрес, вы можете выполнять значительное число настроек со своего рабочего места,

не подходя к принтеру. Интересно, что IP-адрес принтера может не принадлежать диапазону адресов вашей сети, но вы сможете к нему подключаться, если есть физическая возможность такого подключения. В частности, если есть возможность дать принтеру "настоящий" IP-адрес в Интернете, то печатать на него сможет любой пользователь Интернета. Но этот случай, я думаю, не очень вас интересует, зачем всем пользователям Интернета раздавать ваши запасы тонера и бумаги? В локальной сети IP-адрес принтера должен принадлежать диапазону адресов сети.

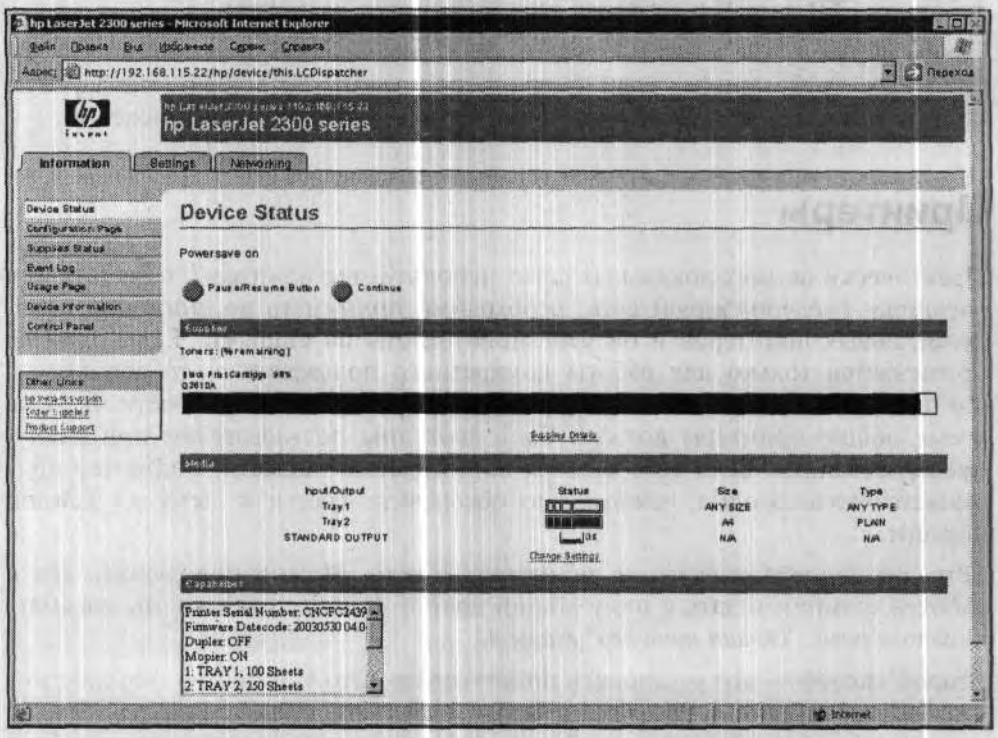


Рис. 6.5. Web-интерфейс управления сетевым принтером

Если у сервера есть два или более сетевых интерфейсов, то не имеет значения, в какой из подсетей находится принтер. Достаточно, чтобы этот принтер был доступен с сервера и был установлен его драйвер. Принтер будет виден в папке **Принтеры и факсы** сервера. Как и для принтера, непосредственно подключенного к серверу, к сетевому принтеру можно установить общий доступ. При этом сервер будет выполнять функции, подобные функциям маршрутизатора, но только для адреса и порта сетевого принтера с принт-сервером.

В качестве иллюстрации такого подключения к принтеру приведем реально работающую схему сети (рис. 6.6).

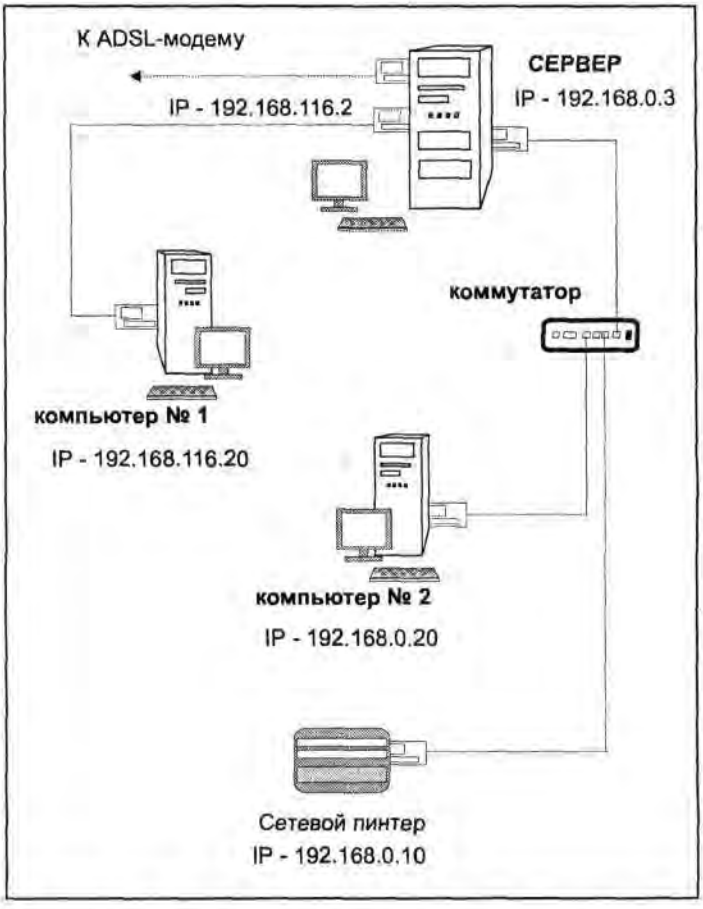


Рис. 6.6. Подключение к сетевому принтеру

Имея такое разнообразие вариантов подключения принтеров, следует заранее продумывать, как будет использоваться принтер в сети, чтобы число точек подключения к сети позволяло включать сетевые принтеры, если в этом есть необходимость. Точки подключения сетевых принтеров не отличаются от точек подключения обычных рабочих станций. То есть при расчете сети предусматривается дополнительное рабочее место, и при необходимости вместо принтера может быть подключена обычная рабочая станция.

Дополнительное оборудование

В обычной сети дополнительное оборудование — это коммутаторы и маршрутизаторы. О том, как подключать и размещать эти устройства, мы уже говорили в *главе 3*. В отдельных случаях сеть может содержать и другие устройства, например, предназначенные для выполнения задач по сбору какой-либо информации. Строго говоря, эти устройства не являются необходимыми в сети — они выполняют задачи пользователей и, скорее, могут быть отнесены к технологическому оборудованию. Тем не менее, они постоянно работают в сети и без сети бесполезны. Чаще всего такое оборудование нестандартно, производится по специальным заказам и не существует общепринятой практики работы с ним. Администратору сети в этих случаях необходимо обеспечить безопасное для сети функционирование этих устройств.

В число таких нестандартных устройств могут входить оптические преобразователи, которые позволяют без применения оптоволокна осуществить оптическую связь с удаленными устройствами или участками сети, радиоконтроллеры для сбора телематической информации, устройства видеонаблюдения, устройства передачи информации через электросеть и др. Если такие разработки проводятся вами или в вашей организации, то необходимо обеспечить контроль безопасности этих устройств для вашей сети. Не следует подключать данные устройства непосредственно в сеть через имеющиеся точки подключения, если нет абсолютной уверенности в безопасности такого подключения. Лучше применить недорогой коммутатор на четыре-восемь портов. В случае электрического пробоя в нестандартном устройстве или наводки высокого напряжения во время грозы этот коммутатор станет защитой для всей сети. Замена основного коммутатора вашей сети может быть значительно более дорогим делом, учитывая, что при выходе его из строя сеть окажется неработоспособной до замены коммутатора или его ремонта. Наиболее безопасно подключение таких устройств через рабочую станцию, если они имеют интерфейс для связи с ней. Если устройство поставляется по договору с его изготовителем или разработчиком, то лучше включить рабочую станцию в договор поставки с оговоренным гарантийным сроком эксплуатации не только самого оборудования, но и рабочей станции.

Не соглашайтесь подключать нестандартное оборудование, пока вы сами не ознакомились с его документацией, степенью его безопасности для вашей сети. В любом случае ответственность за исправную работу сети лежит на ее администраторе.

Информацию об устройствах защиты сети от перенапряжений можно получить по адресу в Интернете **http://www.apc.ru/products/surge/protecnet.html**. Эти устройства рекомендуется применять и для защиты сети от атмосфер-

ного электричества на входе и выходе воздушных кабельных линий, соединяющих участки сети в разных зданиях. Фильтр для сетей EtherNet 100Base-T / 10Base-T / TokenRing(RJ45), информацию о котором можно найти по указанному адресу, защищает сетевые карты и имеет порог срабатывания защиты всего 8 В.

Организация работы администратора

Планируя сеть, необходимо планировать и свою работу в изменяющейся сети. Модернизация сети, поиск неисправностей в ней требует от администратора значительного числа операций, производимых на сервере и в сети. Эти операции могут выполняться как самим администратором, так и его помощником, что может привести к серьезным проблемам, если действия администратора не фиксируются с целью возможности просмотреть историю изменений в системе и в сети.

"У семи нянек дитя без глазу". Эта старинная поговорка определяет и основное правило администрирования компьютерной сети. Управлять сетью должен один администратор. В состав пользователей Windows 2000 Server заранее включены несколько групп, наделенных определенными правами, и только один пользователь, Администратор имеет неограниченные права управления сервером и сетью. Администратор вправе добавить любое число пользователей с правами администратора, но этого делать не следует. Последствия коллективного администрирования могут быть весьма плачевными, поскольку даже при высокой квалификации многочисленных администраторов их действия могут быть не согласованы и могут противоречить 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 быть свой администратор. Администратор домена координирует свои действия с нижестоящими администраторами. До тех пор, пока у вас один домен и одна небольшая сеть, вы должны быть единственным администратором вашей сети. В зависимости от задач, которые решаются в вашей сети, работы по ее обслуживанию могут быть более или менее периодическими. 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 проводимых изменениях. Например, замена сетевой карты на клиентском компьютере иногда приводит к нарушению работы базы данных MS Access. Если у вас в хронологическом порядке регистрируются изменения, произве-

денные в сети, то причина сбоя в работе 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. Не следует полагаться на электронные записи в файле дневника. Проблемы могут быть настолько серьезными, что у вас не будет доступа к электронным записям. Бумажный журнал всегда доступен. Конечно, можно обойтись и без бумажного носителя, но в этом случае файлы дневника должны копироваться при каждом их изменении на разные компьютеры, чтобы наверняка быть доступными при самых серьезных проблемах в сети.

Дневник администратора

Форма дневника может быть произвольной. Но необходимо предусмотреть 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 если заниматься этим придется новому администратору. А смена руководства сети, как и смена любого другого руководства, вполне возможна.

Опишем вариант дневника, который может применяться в небольшой сети.

Состав дневника

Дневник может содержать следующие разделы:

- работы по обслуживанию сервера — программное обеспечение и аппаратная модификация, изменения разрешений (табл. 6.1);
- работы по обслуживанию применяемого программного комплекса (табл. 6.2);
- работы по обслуживанию сети — кабельная система и оборудование (табл. 6.3);
- пользователи — закрепление пользователей за компьютерами (табл. 6.4);
- компьютеры сети — краткая характеристика и сведения о модификации (табл. 6.5);
- схема сети (рис. 6.6).

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

Таблица 6.1. *Работы по обслуживанию сервера*

Дата	Время	Проблемы	Сделано	Результат
19.06.2003	12:53	Неиспользуемые учетные записи	Удалены пользователи User1, User2, User3	+
19.06.2003	16:00–16:30	Сбой при настройке нового программного обеспечения	Перезагрузка	+
20.06.2003	21:00	Права пользователей	Установлены права на DIR для User25 и User 15	+
21.06.2003	22:15–23:50	Внеплановое отключение в связи с перебоями электроснабжения	Сервер запущен	+
21.06.2003	23:00	Модификация	Замена CDROM (тип)	+

Второй раздел содержит записи об установке и модификации прикладного программного обеспечения.

Таблица 6.2. *Работы по обслуживанию программного комплекса*

Дата	Время	Проблемы	Сделано	Результат
15.06.2003	09:15	Замена программных модулей	Заменены M1 и M2 на версии от 10.06.2003	+
19.06.2003	15:00	Не работает M1 в режиме A	Настройка	– (сбой сервера)
19.06.2003	16:35	Не работает M1 в режиме A	Настройка	+

Третий радел содержит записи об обслуживании сети.

Таблица 6.3. *Работы по обслуживанию сети*

Дата	Время	Проблемы	Сделано	Результат
12.06.2003	10:15	Не обеспечивается 100 Мбит для User13	Замена устаревшего (к3) кабеля на (к5) 25 м	+
19.06.2003	15:00	Добавление рабочей станции Komp18	Подключение	+

В четвертом разделе — сведения о пользователях и компьютерах.

Таблица 6.4. *Пользователи и компьютеры*

Дата	Компьютер	Пользователь
01.03.2003	DEN (в отделе N)	Иванов Иван Иванович (User17)
01.03.2003	GSM (в отделе L)	Петров Петр Петрович (User14)

Пятый раздел удобно поместить на отдельных листах (карточках) в качестве приложения к дневнику.

Таблица 6.5. *Компьютеры сети*

Дата	Компьютер	Система
Подключен 01.03.2003	Komputer System	Win98SE
Сведения: Идентификация — Komp1, Сетевая карта — (тип), Office 2000, IE6, IP статический 192.168.0.109		
Модификации		
15.05.2003	Обновление Office	
20.06.2003	Замена сетевой карты (тип 1 на тип 2)	

Шестой раздел — схема сети (рис. 6.7) с изображением структуры сети, здесь отмечены некоторые особенности, например, категория кабеля на участке.

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 приведенной, могут быть добавлены какие-либо разделы, если это необходимо.

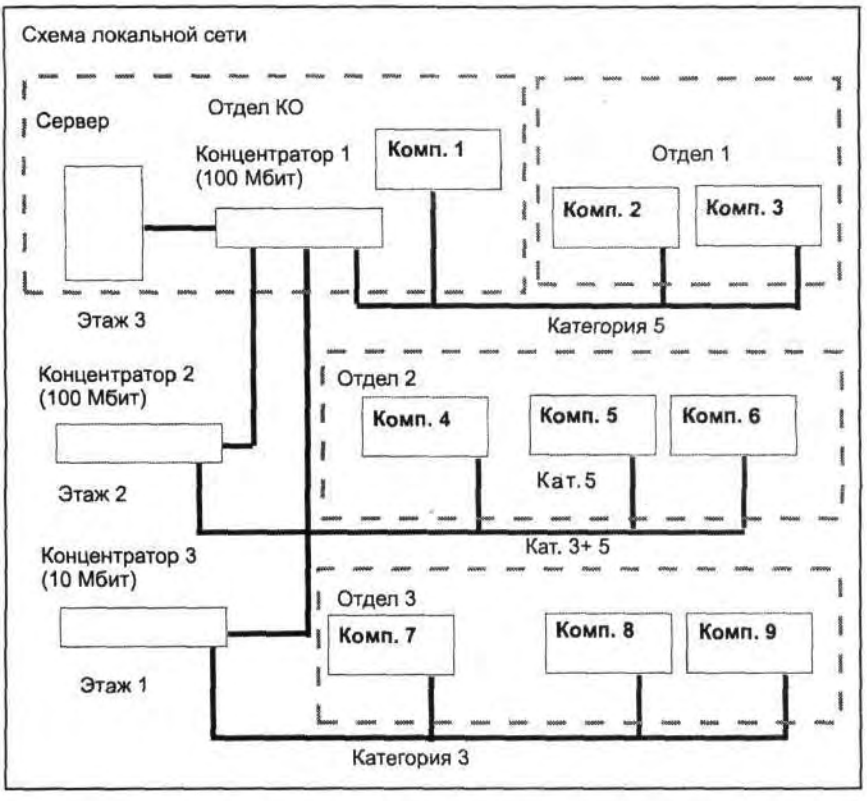


Рис. 6.7. Схема локальной сети

Возможно, что заполнение дневника вам покажется обременительной задачей. Может быть у вас хорошая память, и вы отлично помните все, что делали в сети за всю ее историю. Но мне, например, совсем не хочется, чтобы во время моего отпуска помощник, оставшийся за меня, вызывал меня через день по телефону с просьбой проконсультировать о возможных причинах возникшей проблемы, а то и просить подключиться к серверу через Интернет, чтобы исправить неблагоприятную ситуацию. Просмотрев записи в журналах, он может в большинстве случаев решить проблему самостоятельно.

Инструменты администратора

Разговор пойдет не о слесарных и электромонтажных инструментах, наличие которых часто тоже необходимо, а о программах и утилитах, помогающих вам следить за здоровьем сети.

Перечень инструментов администратора может расширяться по мере развития вашей сети практически неограниченно. Многое уже есть в самой операционной системе, другие инструменты разработаны различными программистами. Какие конкретно средства будете применять вы — это ваше дело, рассмотрим лишь средства, которые, на мой взгляд, могут быть полезны большинству администраторов. Некоторые из приведенных здесь средств будут подробнее описаны в следующих главах, а другие уже упоминались в книге ранее, но не описаны подробно.

Команда *Ping*

Запускается из командной строки, присутствует во всех операционных системах, поддерживающих работу в сети. Особенности команды и список параметров могут отличаться от системы к системе, но основные функции неизменны. Далее приведен результат применения команды, который можно увидеть на экране компьютера в окне командной строки.

```
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 = 0мс, наибольшее =  0мс, среднее =  0мс
```

Команда позволяет определить следующие параметры сети:

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

Запуская команду с различными параметрами, можно анализировать и другие характеристики сети. О параметрах команды вы узнаете из ее справки, запустив команду `ping` без адреса и параметров. Если при проверке с помощью `ping` новой кабельной линии 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. Замена обычного хаба коммутатором, который поддерживает скорость передачи данных 100 Мбайт/с, иногда приводит к ухудшению связи между компьютерами. Причин может быть несколько, но, перестроив

порты коммутатора на пониженную скорость, вы восстановите нормальную связь. Контроль качества связи можно осуществлять также командой Ping.

Команда *Ipconfig*

Тоже запускается из командной строки. Она позволяет определить сетевые настройки компьютера, на котором она запущена. Далее приведен 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 о IP-адресах. При неполадках, которые могут быть вызваны неправильными настройками рабочей станции, вы можете проверить эти настройки, пользуясь описанной командой.

Утилита SuperScan

Большую помощь может оказать бесплатная утилита SuperScan (рис. 6.8), которую можно найти по адресу: **http://www.webattack.com/get/superscan.shtml**.

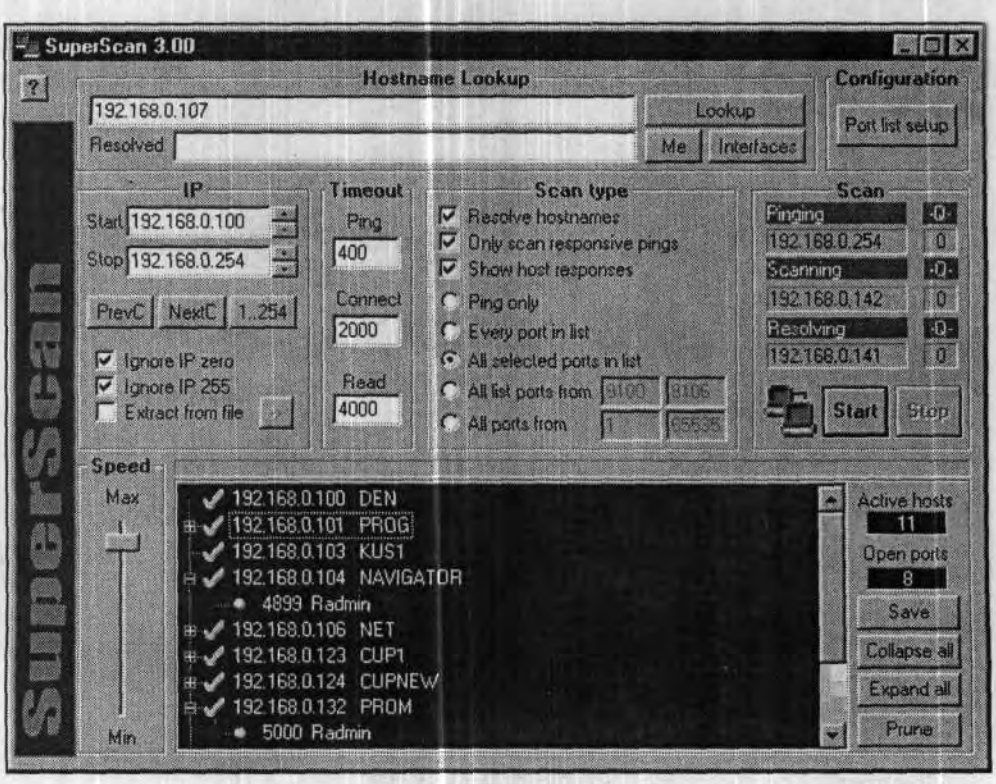


Рис. 6.8. SuperScan 3.0

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. Вы получите полную информацию о доступности компьютеров в сети, запустив эту программу.

Удобна эта утилита и при сборе статистики о работе компьютеров в сети. Результат работы программы может быть сохранен в файл. Запуская SuperScan в определенные часы и сохраняя результат сканирования, вы получите достоверные сведения о работе компьютеров в это время.

Можно применять и массу других утилит различных разработчиков, но главное, о чем вам придется заботиться, — это работа сервера. Операционная система Windows Server 2003 имеет в своем составе множество инструментов, предназначенных специально для администратора.

Управление компьютером

Прежде всего, это средство управления компьютером, на котором установлена Windows 2000 Server или Windows Server 2003. Откройте **Администрирование | Управление компьютером**. Вы увидите окно, показанное на рис. 6.9.

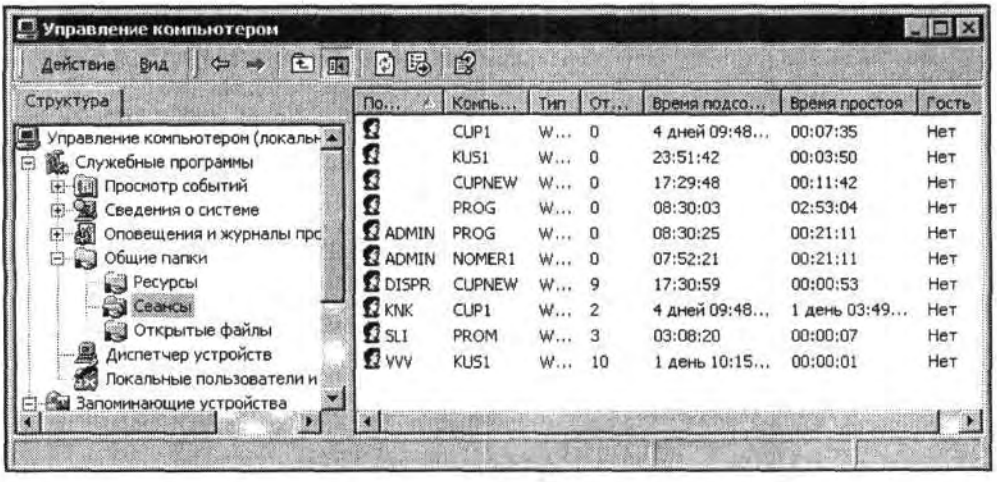


Рис. 6.9. Окно **Управление компьютером**

Войдя в раздел **Общие папки**, вы сможете контролировать работу пользователей, связанную с подключением к серверу. В подразделе **Сеансы** приводятся активные сеансы пользователей с указанием компьютера и имени пользователя, а также времени подключения и состояния сеанса. В случае обнаружения каких-либо нарушений пользователем установленных для вашей сети правил

вы можете отключить сеанс пользователя. В подразделе **Открытые файлы** вы увидите список открытых пользователем файлов. Иногда возникает необходимость освободить какой-либо файл, занятый пользователем, вы можете закрыть файл, нажав правую кнопку мыши. Само собой разумеется, что эту процедуру следует выполнять только в случае явной необходимости, поскольку она может привести к потере данных пользователя.

В подразделе **Ресурсы** можно запретить общий доступ к ресурсам, открытым для доступа ранее. Такая необходимость возникает при обнаружении несанкционированного доступа к файлам.

Количество других средств администрирования может колебаться в зависимости от установленных компонентов и достигать нескольких десятков. Рассмотрим наиболее важные из них.

Просмотр событий

Открыв **Администрирование | Просмотр событий**, вы увидите окно (рис. 6.10), предоставляющее доступ к журналам событий.

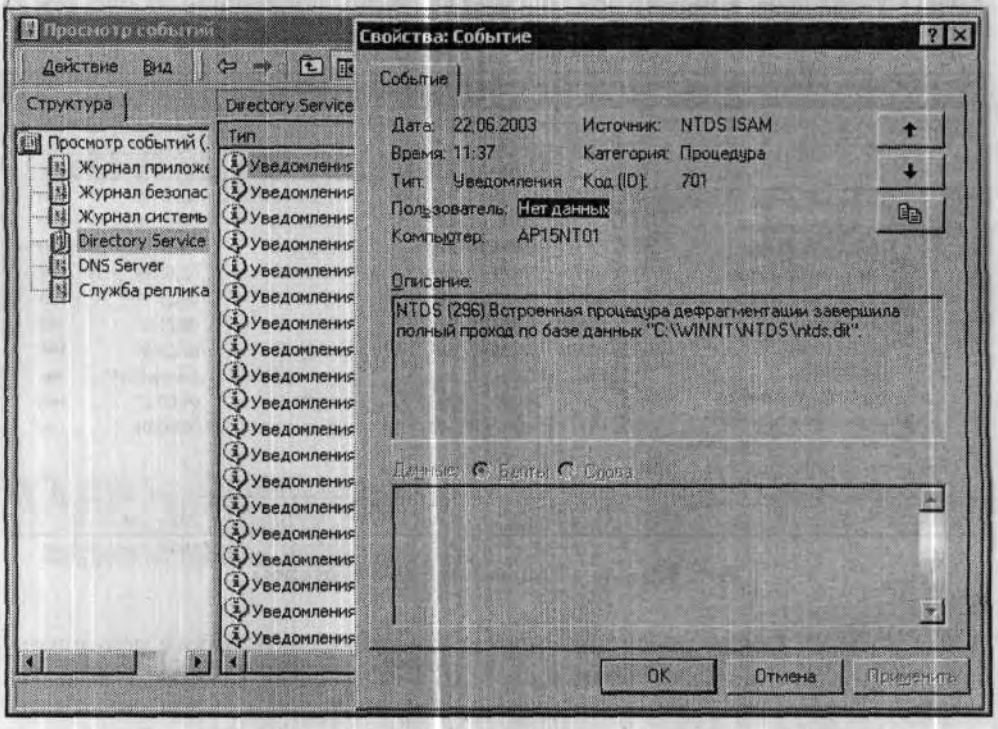


Рис. 6.10. Окно **Просмотр событий** с открытым окном события

Двойным щелчком мыши на интересующем событии вы можете открыть окно со сведениями о нем и прочитать сообщение сервера. В большинстве случаев это просто отчет сервера о выполняемых процедурах, но могут встречаться предупреждения и сообщения об ошибках. Многие предупреждения и ошибки вызваны временной нештатной ситуацией, но если ошибка повторяется регулярно, то стоит разобраться внимательней и, по возможности, устранить причину ее появления.

Active Directory — пользователи и компьютеры

На консоли **Active Directory - пользователи и компьютеры** (рис. 6.11), которую мы подробно рассмотрим в следующей главе, есть возможность управления учетными записями пользователей, групп и компьютеров.

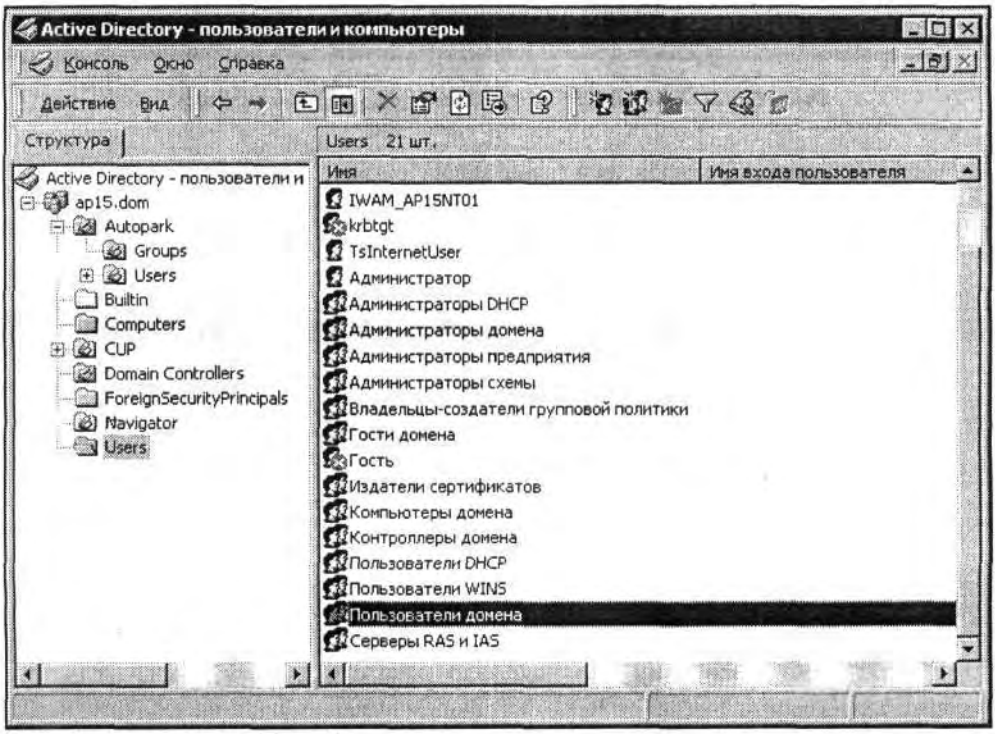


Рис. 6.11. Окно **Active Directory - пользователи и компьютеры**

DHCP и WINS

Очень важные для администратора консоли — **DHCP** и **WINS**. На рис. 6.12 показано окно **DHCP** с арендованными у сервера IP-адресами.

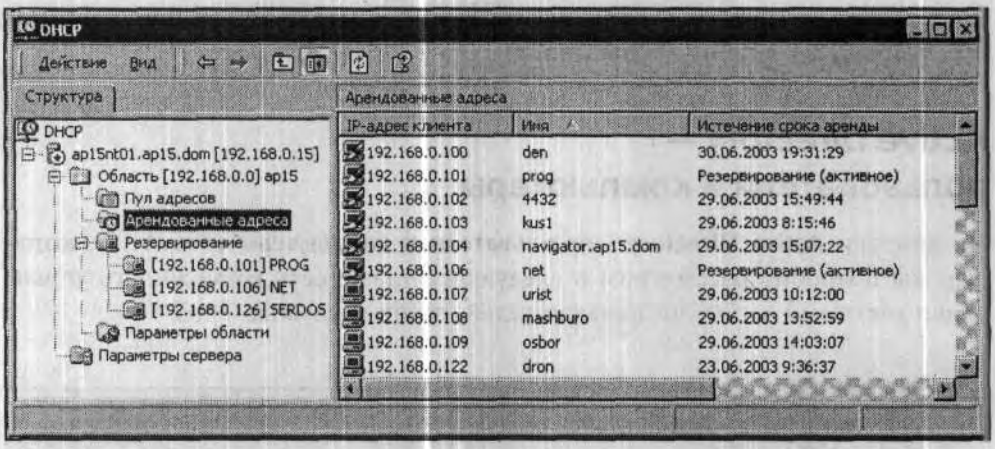


Рис. 6.12. Окно **DHCP** со списком арендованных адресов

Вы можете контролировать активные регистрации, удалять, при необходимости, старые "захороненные" регистрации, устанавливать диапазоны выдаваемых и не выдаваемых в аренду адресов (рис. 6.13).

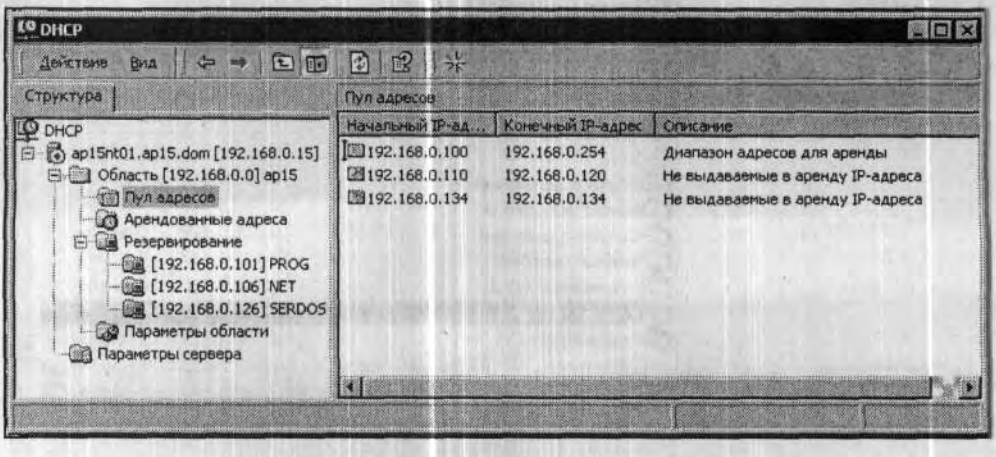


Рис. 6.13. Окно **DHCP** с диапазонами адресов

Для ускорения выдачи адресов сервером по умолчанию отключена проверка существования узла с ранее арендованным адресом. Для сервера основным параметром идентификации компьютеров является физический адрес сетевого адаптера. Это значит, что при смене имени компьютера и неизменной сетевой карте сервер не сможет выдать новый адрес, пока не удалена старая регистрация. Для некоторых компьютеров необходимо всегда сохранять один и тот же IP-адрес. В этом случае адрес резервируется для данного компьютера. Для других серверов, работающих в сети, следует устанавливать адреса, не входящие в область адресов, выдаваемых сервером DHCP. Если среди арендованных адресов вы встретите адрес с пометкой **BAD_ADDRESS** (плохой адрес), то необходимо найти и устранить неполадку, отключив от сети рабочую станцию, вызвавшую проблему.

Вообще говоря, DHCP-серверов в сети может быть несколько, что повышает надежность службы в больших сетях. В таком случае каждый сервер должен выдавать определенный для него диапазон адресов. Все остальные адреса для этого сервера должны попасть в диапазон исключения — не входить в область выдаваемых сервером адресов. Для установки диапазона исключения следует выделить папку **Пул адресов**, а затем нажать на кнопку **Действие** и выбрать пункт меню **Диапазон исключения**. В появившемся окне ввести адреса начала и конца диапазона исключения. Аналогично можно установить и все другие диапазоны адресов, включая резервированные адреса. Справочная система, доступная прямо из окна консоли, поможет решить сложные на первых порах проблемы.

Для разрешения имен в сети применяется несколько механизмов. Один из них — консоль **WINS** (рис. 6.14).

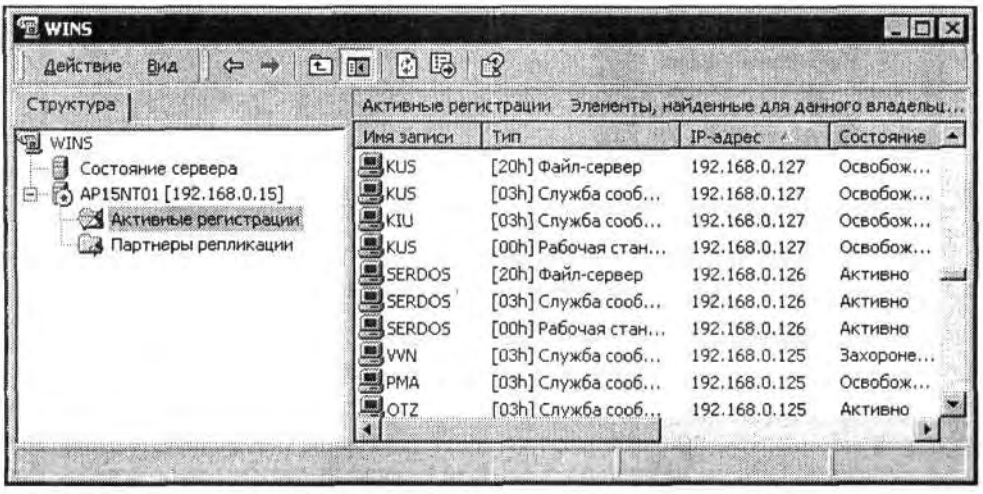


Рис. 6.14. Окно **WINS** со списком активных регистраций

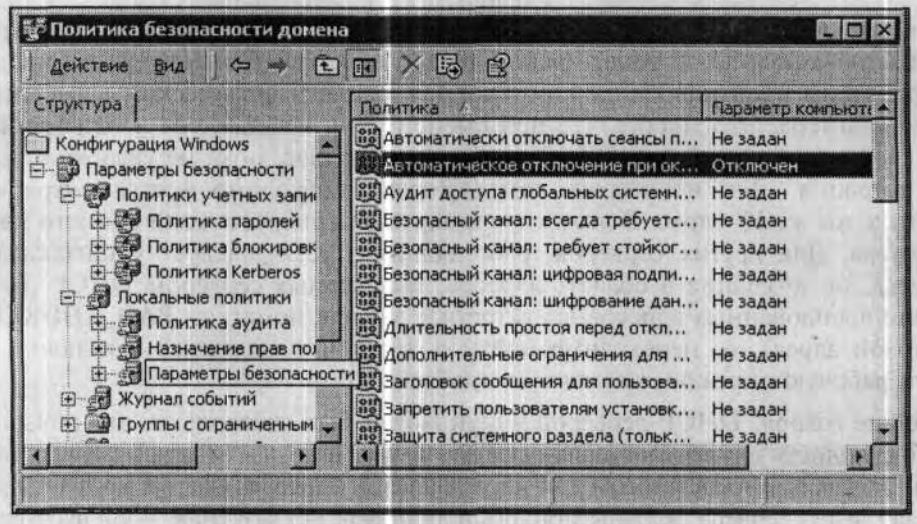


Рис. 6.15. Окно **Политика безопасности домена** (параметры безопасности)

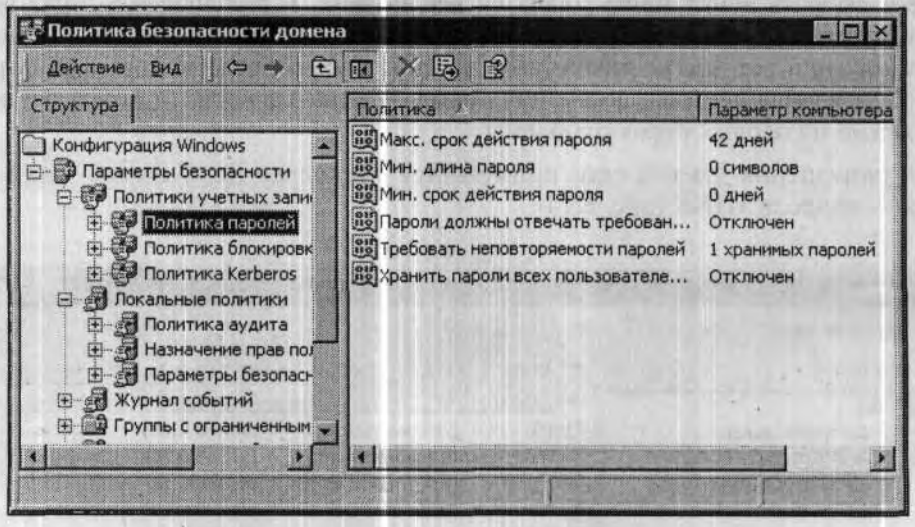


Рис. 6.16. Окно **Политика безопасности домена** (политика паролей)

Для просмотра сведений об активных регистрациях необходимо, нажав кнопку **Действие**, выбрать один из пунктов: **Найти по владельцу** или **Найти по имени**. На экране появятся регистрации, которые соответствуют выбранному условию. В роли владельца в данном случае выступает ваш сервер. Для некоторых компьютеров может потребоваться статическое сопоставление

имени и IP-адреса. Это можно сделать, нажав кнопку **Действие** и выбрав пункт **Создать статическое сопоставление**.

Вполне возможно, что установленные по умолчанию политики безопасности домена и политики паролей вам потребуется скорректировать. Для этого существует консоль **Политика безопасности домена** (рис. 6.15 и 6.16).

Вы можете просмотреть возможные варианты настроек, открывая каждую политику двойным щелчком мыши и устанавливая, при необходимости, требуемые параметры.

Другие средства

Есть и более прозаичные средства администрирования, такие как известные всем BAT-файлы, а также планировщик заданий, входящий в операционную систему. Они позволят без вашего участия, по расписанию, выполнять многие процедуры, связанные с обслуживанием сервера, прикладных программ и баз данных, находящихся на сервере. Рассмотрим несколько задач, которые приходится решать в небольшой сети.

Предположим, что требуется регулярное сохранение на другом компьютере сети копии данных, расположенных на сервере. Для этого очень подходит команда XCOPY и планировщик заданий, встроенный в Windows. Приведем реальный пример такой процедуры (листинг 6.1).

Листинг 6.1. BAT-файл с командами XCOPY

```
@ echo off
xcopy /c /y /z /i /e /d C:\AutoPark \\Big_user\Archive\Autopark\AutoPark\
>C:\ASU15\ArchAutoPark.txt
if errorlevel 4 goto lowmemory
if errorlevel 2 goto abort

xcopy /c /y /z /i /e /d /exclude:C:\ASU15\exclude.txt C:\AutoParkSrv
\\Big_user\AutoParkSrv\ >C:\ASU15\ArchAutoParkSrv.txt
if errorlevel 4 goto lowmemory
if errorlevel 2 goto abort

goto exit

:lowmemory
echo Недостаточно памяти
echo или не верный путь.
goto exit
```

```
:abort
echo Нажата Ctrl + C
:exit
```

Полный список ключей команды можно найти в ее справке, здесь опишем только примененные.

- `c` — продолжение копирования независимо от наличия ошибок. Этот ключ необходим, когда задание выполняется автоматически и не должно останавливаться.
- `y` — подавление запроса на перезапись файла.
- `z` — копирование сетевых файлов с возобновлением. При потере соединения копирование продолжится, когда связь восстановится.
- `i` — если результат не существует, а копируется несколько файлов, считается, что указано имя каталога. Это избавит от появления вопросов программы, на которые кто-то должен дать ответ.
- `e` — копирование каталогов с подкаталогами.
- `d` — заменяются файлы только более старые, чем исходные. Это сократит время копирования.
- `EXCLUDE:<имя файла>` — исключение копирования файлов, имена или части имен которых записаны в текстовом файле, на который указывает ключ. Это необходимо для исключения из процедуры копирования файлов, которые всегда открыты.

Файлы копируются на компьютер `Big_user`. Система анализирует результат выполнения команды (`ERRORLEVEL` — вид ошибки) и выдает сообщение, которое необходимо в процессе отладки процедуры.

С помощью перенаправления вывода информации о выполнении копирования в файл (символом >) получаем отчет о завершенном копировании в виде текстового файла.

Для переноса команды в планировщик достаточно перетащить мышью значок BAT-файла в папку **Назначенные задания** (рис. 6.17), которая находится на панели управления. После перетаскивания потребуется лишь установить расписание для выполнения задания.

Теперь, в соответствии с расписанием, процедура копирования будет проходить без вашего вмешательства.

Если нужно предупредить пользователей о необходимости выйти из какой-либо программы, можно включить в другой командный файл строку, подобную следующей:

```
NET SEND <имя компьютера> "Закройте программу А на 10 минут! Возможна
потеря данных!"
```

В этой строке применена команда `NET SEND` для отправки сообщения компьютерам сети. Но в большинстве случаев этого не требуется, поскольку будут скопированы все файлы, редактирование которых завершено.

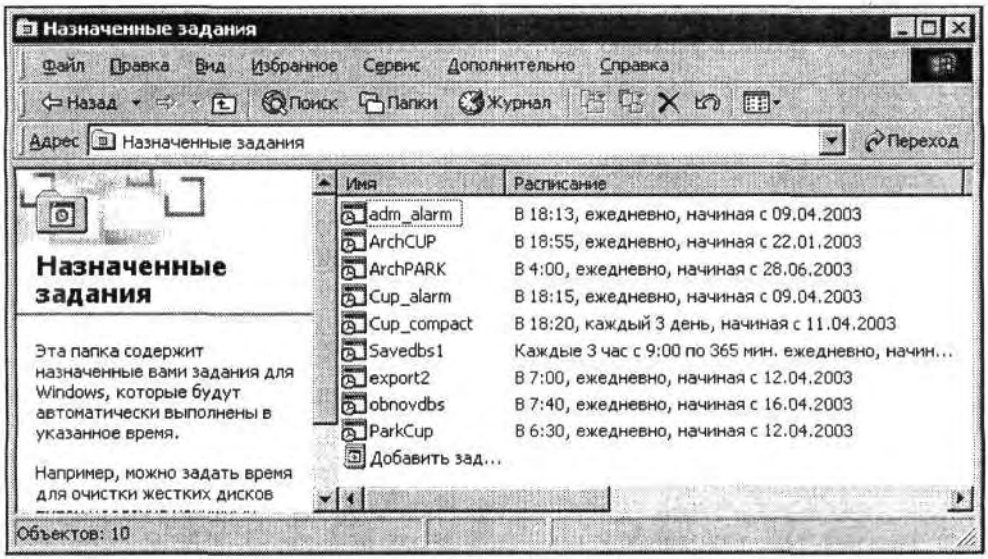


Рис. 6.17. Папка **Назначенные задания**

Замечание

Если объем копируемых данных велик, а компьютеры подключены через старые хабы, не поддерживающие маршрутизацию пакетов, то возможно временное замедление работы сети. Применение коммутаторов (Switch) избавит вас от этой неприятности.

Рассмотрим полнее возможности утилиты NET, входящей в комплект Windows 2000 Server и Windows Server 2003. Эта утилита запускается из командной строки и может с успехом заменить окно **Active Directory - пользователи и компьютеры**. Командная строка, например, выглядит так:

```
NET USER USERNAME PASSWORD / commands
```

В приведенной строке:

- `USERNAME` — управляемая учетная запись;
- `PASSWORD` — пароль;
- `Commands` — команды.

Среди команд утилиты, которые можно использовать, следующие:

- `/ADD` — добавить учетную запись;
- `/ACTIVE:[YES][NO]` — выполнить активацию учетной записи;
- `/DELETE` — удалить учетную запись;
- `/DOMAIN` — создать учетную запись в указанном домене;
- `/COMMENT:"[текст комментария]"` — описание учетной записи;
- `/USERCOMMENT:"[текст комментария]"` — описание пользователя;
- `/EXPIRES:[NEVER] [MM/DD/YY]` — установить дату окончания действия учетной записи. `NEVER` — никогда, или значение даты;
- `/FULLNAME:"[наименование]"` — полное наименование учетной записи;
- `/HOMEDIR:[путь]` — домашний каталог;
- `/PASSWORD:[YES] [NO]` — возможность смены пароля пользователем;
- `/PASSWORDREQ:[YES] [NO]` — необходимость запроса пароля у пользователя;
- `/TIMES:[дни],[часы]` — дни и часы указываются по-английски, например, `MONDAY-THURSDAY` (понедельник-четверг) или `ALL` (все), часы — в формате `XAM-YPM`, где `X` и `Y` — часы суток от 0 до 12, а `AM` и `PM` — обозначения первой или второй половины суток относительно полудня.

Есть и другие команды. Их можно найти в справке утилиты NET. Освоив режим командной строки, вы сможете создавать сценарии для проведения настроек сети.

Вообще, стоит внимательно ознакомиться с командами, запускаемыми из командной строки, среди них есть много очень полезных. Включив их в командные файлы, вы сможете автоматически синхронизировать часы на клиентских машинах с часами сервера, запускать и останавливать программы на сервере, автоматически обновлять программное обеспечение клиентов... Можно BAT-файл, содержащий команды синхронизации часов, обновления программного обеспечения, если оно присутствует в сети, и запуска самой программы, разместить в сетевом каталоге, а на рабочем столе пользователя поместить ярлык к этому файлу. При этом если с данного компьютера в сеть вошел пользователь, не имеющий прав на запуск файла, то программа не сможет запуститься, несмотря на то, что ее файлы находятся на локальной машине. Можно включать в число команд проверку существования файла, доступ к которому ограничен узким кругом пользователей, что позволит дополнительно защитить доступ к информации и программам, если это необходимо.

Radmin (Remote Administrator)

Существует множество средств для удаленного управления компьютерами сети. Среди них и бесплатная программа VNC (**www.realvnc.com**), но по моему опыту, лучшим средством оказалась эта небольшая программа. Адрес программы: **http://www.radmin.com**. Она позволит вам, не отходя от своего компьютера, подключаться к любому компьютеру сети для помощи пользователю или контроля правильности его работы, а также для дистанционной установки программного обеспечения и настройки клиентских машин. Ее применение требует наличия клиентской части на вашем компьютере и серверной — на удаленных. При этом вы видите экран удаленного компьютера в окне на своем рабочем столе или развернутым на весь экран. А ваши мышь и клавиатура подменяют мышь и клавиатуру на удаленном компьютере, если управление осуществляется в полноэкранном режиме или окно удаленного экрана активно. Но можно и просто наблюдать за происходящим. Программа поддерживает LAN, WAN, а также соединение dial-up — модемное соединение через Интернет или с использованием сервера удаленного доступа, т. к. она не требует высокоскоростного соединения. При подключении через модем вы можете получить приемлемую частоту обновления экрана (около 5—10 обновлений экрана в секунду). При работе внутри локальной сети экран обновляется в реальном времени (около 100—500 обновлений экрана в секунду). Иногда, используя Radmin в полноэкранном режиме, вы можете даже забыть, что работаете на удаленном компьютере! Программа постоянно совершенствуется, выпускаются новые версии, но принцип работы с ней и ее основные возможности не меняются. В большинстве случаев подходит версия 2.1, для работы с Windows XP Sp2 — версия 2.2, некоторые дополнительные возможности имеет версия 3.0. Версия 2.1 содержит все возможности, необходимые администратору сети. Radmin состоит из двух частей:

- серверной части, которая генерирует изображение экрана;
- клиентской части (программа просмотра), которая постоянно отображает экран удаленного компьютера на вашем экране.

Для старта Radmin вы должны запустить сервер, а также установить соединение с помощью клиентской части (программы просмотра).

Возможности программы

Radmin-сервер может работать как сервис под Widows XP/2000 и Windows 9*x*/ME, что позволяет вам выполнять команды `logon` и `logoff` дистанционно, поддерживает одновременно несколько сессий дистанционного управления и просмотра на одном рабочем месте. Полноэкранный режим позволяет вам видеть экран удаленного компьютера во весь экран своего дисплея, а масштабируемый режим — изменять размер экрана удаленного компьютера в своем окне.

Radmin позволяет вам работать на удаленном компьютере в реальном времени с потрясающей скоростью (сотни обновлений экрана в секунду), обмениваться файлами с удаленным компьютером и даже выключить компьютер дистанционно, без необходимости соединения, в режиме просмотра. Radmin-сервер предоставляет Telnet-доступ к удаленному компьютеру, если этот сервер работает под Windows 2000. Вы можете разрешить удаленное управление, просмотр, обмен файлами, а также Telnet-доступ определенным пользователям или группам пользователей. Если пользователь принадлежит к домену Windows 2000, то Radmin будет использовать текущие регистрационные (пользователь/пароль) данные для предоставления доступа к Radmin-серверу. Если система безопасности Windows 2000 выключена, то доступ контролируется паролем. Radmin определяет пользователя методом запрос-ответ, основанным на 128-битном шифровании, которое применяется для всех передаваемых данных. Начиная с версии программы 2.1, шифрование невозможно отключить. IP-фильтр предоставляет доступ к Radmin-серверу только определенным IP-адресам и подсетям. Максимальное разрешение экрана, поддерживаемое Radmin, до 2048×2048 при 32-битном цвете.

Radmin требует соединения между серверной и клиентской частями по протоколу TCP/IP.

Системные требования

Программа работает даже на P386 с 8 Мбайт RAM под управлением Windows 95. Может работать без дисплея, мыши или клавиатуры. Для всех операционных систем (Win9*x*/ME/NT/2000/XP/2003) необходим установленный протокол TCP/IP. Один из серверов нашей сети с операционной системой Windows 2000 именно так и работает. Он применяется как архивное хранилище файлов и работать на нем в локальном режиме нет необходимости, но когда требуется изменить какие-либо настройки этого сервера или перезагрузить его, то достаточно удаленного подключения.

Установка

Для работы с Radmin вам необходимы два компьютера, соединенные через сеть. Установите протокол TCP/IP и Radmin на оба компьютера. Перед инсталляцией для всех пользователей деинсталлируйте предыдущие версии Radmin, если таковые присутствуют.

Рекомендации для пользователей Windows NT 4.0

Для установки сервиса или драйвера вы должны иметь права администратора.

- Если вы хотите использовать Radmin-сервер с драйвером видеозахвата, вы должны деинсталлировать все другие программы удаленного доступа, применяющие технологию видеозахвата.

- Выполнение нескольких программ, использующих один драйвер видеозахвата, может привести к разрушению системы во время загрузки.

  Примерами таких приложений могут быть: NetMeeting 3.0+, SMS, Timbuktu. Если возникают проблемы при загрузке Radmin-драйвера, то необходимо нажать клавишу <1> пять раз в течение 1 с, пока идет загрузка, и Radmin-драйвер загружен не будет.

- Для Windows NT 4.0 требуется Service Pack 4 или более поздний.

Рекомендации для пользователей Windows 2000/XP

Для установки сервиса Remote Administrator вы должны иметь права администратора.

1. Распакуйте установочные файлы.
2. Запустите radmin21.exe.
3. Следуйте инструкциям программы установки.

После установки программы вы можете запустить из меню **Пуск** серверную или клиентскую часть программы или выполнить команду **Установ. службу** из меню **Настройка сервера**, в котором также можно настроить Radmin-сервер для автоматической загрузки при старте Windows, изменить пароль для сетевого доступа и выполнить другие настройки.

Установка соединения

1. Запустите Radmin-сервер на удаленном компьютере. При этом должен появиться значок Radmin-сервера на панели задач Windows.
2. Подведите мышь к значку, появится IP-адрес компьютера, двойной щелчок кнопки мыши по значку выводит на экран список текущих соединений. Значок может быть отключен в настройках Radmin-сервера.
3. На локальном компьютере запустите обозреватель Radmin viewer.
4. Выберите из меню обозревателя **Соединение | Соединение с**.
5. В поле **IP адрес или имя DNS** введите IP-адрес (например, 10.0.0.1) или DNS-имя (например, comp1.company.com) удаленного компьютера, на котором запущен Radmin-сервер.

Подключение модем-модем

Radmin не работает непосредственно с модемами. Для использования соединения модем-модем вы должны настроить удаленный доступ на клиенте и сервере. Протокол TCP/IP нужно установить на обоих компьютерах. На серверной стороне вы должны установить сервер удаленного доступа (это стандартный компонент для Windows 98 и компонент из MS Plus! для Win-

dows 95), если вы используете Windows 9x, или же RAS — сервер удаленного доступа в Windows 2000 и Windows XP. Кроме того, следует настроить сервер для работы с протоколом TCP/IP. На клиентской стороне вы также должны установить Контроллер удаленного доступа и настроить его на применение протокола TCP/IP. Далее нужно сделать звонок, используя соединение dial-up. После подключения вы можете найти IP-адрес удаленного сервера в свойствах подключения или в Мониторе подключения, находящемся на панели управления. Используйте этот IP-адрес для подключения Radmin-клиента к удаленному серверу. Как правило, при данном типе соединения он равен 192.168.55.1. Когда соединяемые компьютеры входят в локальные сети, могут быть присвоены и другие адреса из диапазона 192.168.X.X.

Конечно, скорость соединения очень зависит от качества связи. Но мне удается контролировать некоторые долго идущие процессы в сети из дома, находясь в сорока километрах от сервера.

Подключение через Интернет

Установить соединение через Интернет так же просто, как сетевое соединение. Единственная проблема заключается в том, что IP-адрес удаленного компьютера, на котором выполняется Radmin-сервер, не всегда известен до подключения. Он может назначаться провайдером (ISP) динамически или статически. В первом случае IP-адрес становится известен только после подключения к Интернету и необходимо каким-либо образом "передать" его на клиентскую сторону.

1. Установите Radmin на оба компьютера.
2. Запустите Radmin-сервер на удаленном компьютере.
3. Подключите удаленный компьютер к Интернету.
4. Любым способом получите информацию об IP-адресе компьютера, к которому вы хотите подключиться.
5. Подключите ваш компьютер к Интернету.
6. Запустите Radmin-клиент на локальном компьютере, выберите в меню **Соединение | Соединение с**, введите IP-адрес удаленного компьютера, который вам уже известен.

Соединение через прокси-сервер

Программа Radmin использует по умолчанию порт 4899 TCP. Вы можете открыть данный порт на вашем прокси-сервере. Другим решением этой проблемы является изменение номера порта (на обеих сторонах соединения) на уже открытый на вашем прокси-сервере. Если ваш прокси работает под управлением Windows, вы можете установить Radmin-сервер на этом же компьютере. Далее вы сможете подключаться, используя **Соедине-**

ние через. Сказанное ранее относится и к firewall/router (сетевой экран и маршрутизатор).

Иногда только firewall/router имеет "настоящий" IP-адрес. Сконфигурируйте маршрутизатор так, чтобы он перенаправлял соединения на сетевые интерфейсы компьютеров, находящихся в локальной сети (forwarding). После этого вы должны указывать IP-адрес маршрутизатора, для того чтобы подключиться к компьютеру во внутренней сети.

Если используется совместное интернет-соединение, входящее в Windows 98 SE, обозреватель Radmin viewer не найдет ваш сервер. Проблема в том, что порт должен быть открыт, чтобы обозреватель мог найти сервер. Далее приводится ссылка на программу, которая позволяет это делать **www.practicallynetworked.com/sharing/ics.htm**.

Пример настроек TCP/IP для сегмента локальной сети

Для задания IP-адреса одного сегмента локальной сети в установках TCP/IP сетевой карты на первом компьютере введите IP-адрес 10.0.0.1 (адреса этого типа часто применяют в одноранговых сетях) и сетевую маску 255.255.255.0.

На втором компьютере установите IP-адрес 10.0.0.2 и сетевую маску 255.255.255.0.

Попробуйте выполнить следующую команду `ping` со второго компьютера:

```
ping 10.0.0.1
```

Если компьютеры сети получают адреса автоматически, то, применяя программу SuperScan, которая была уже описана, вы без труда определите адрес нужного вам компьютера. Можно использовать и команду `ping`.

Telnet-доступ

Доступ через Telnet для Windows 95/98/ME не поддерживается из-за ограничений интерпретатора командной строки в этих версиях Windows (command.com).

В некоторых приложениях Win32 применяется прямой доступ к консоли. Такие приложения не работают через Telnet, потому что Telnet-режим использует стандартные потоки ввода/вывода для взаимодействия с приложениями. Вы просто не запустите такие приложения через Telnet, но можно выполнять их в режиме просмотра удаленного экрана.

Настройка RADMIN-сервера

Log-файл

Все действия могут быть записаны в Log-файл из окна **Настройки** программы Remote Administrator.

IP-фильтр

Эти настройки позволят вам предоставлять доступ к Radmin-серверу только с определенного IP-адреса или подсети. Установить IP-фильтр можно, используя **Настройки** в меню **Настройка Remote Administrator Server** (доступно из меню **Пуск**).

Например:

- подсеть — 192.168.1.xx;
- компьютер — 192.168.1.67.

Для доступа к целой подсети установите:

- фильтр IP — 192.168.1.0;
- маска — 255.255.255.0.

Если IP-адрес и маска подсети не соответствуют фильтру IP, вы получите сообщение **Client I/O error**.

Установка/изменение пароля для Radmin-сервера

Вы можете установить или изменить пароль для Radmin-сервера непосредственно из меню **Настройка Remote Administrator Server**. При открытии соединения для ввода пароля будет появляться отдельное окно. На рис. 6.18 показано это окно на фоне обозревателя Radmin.

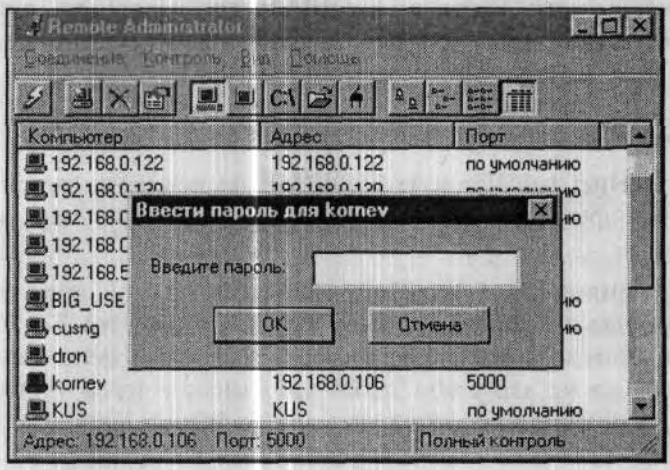


Рис. 6.18. Окно ввода пароля при открытии соединения на фоне окна обозревателя

Если вы пользуетесь Windows NT\2000, то можно включить поддержку системы безопасности NT в настройках Radmin-сервера. После чего следует

предоставить соответствующие права доступа (**Полный контроль**, **Обзор**, **Телнет**, **Перепись файлов**, **Выключение**) к Radmin-серверу.

Установки порта

Номер и адрес порта сервера могут быть изменены из меню **Настройка Remote Administrator Server**. Номер порта по умолчанию 4899.

Меню *Соединение*

Вы можете создать новое соединение, использовать уже установленное, а также выбрать вид соединения непосредственно из меню клиента Remote Administrator.

Окно обозревателя Radmin

Команды меню обозревателя Remote Administrator (см. рис. 6.12) **Соединение с** или **Создать** используются для создания соединения. **Соединение с** позволяет выбирать компьютер, через который производится подключение (поле **Соединение через**), а также устанавливать тип соединения и номер порта.

Меню режимов

С помощью этого меню можно выбрать режим контроля за удаленным компьютером. Вы можете использовать **Полный контроль**, **Обзор**, **Телнет**, **Перепись файлов**, **Выключение** и разные режимы соединения. Если режим **Обзор** позволяет только видеть экран удаленного компьютера, то использование режима **Полный контроль** позволяет вам управлять удаленным компьютером с помощью мыши и клавиатуры и т. д.

Работа с файлами

Этот режим включен в Radmin, начиная с версии 2.0. Вам необходимо выбрать пункт **Перепись файлов** из меню **Контроль** или нажать кнопку на панели инструментов. Интерфейс передачи файлов в Radmin похож на интерфейс обозревателя Windows (рис. 6.19), однако он работает с двумя окнами — локальным и удаленным. Вы можете выбрать вид просмотра файлов, используя кнопки на панели инструментов. Для копирования файлов можно применять технологию Drag and Drop, нажать кнопку **Копировать** на панели инструментов или щелкнуть правую кнопку мыши и выбрать команду **Копировать** в появившемся меню. Команда **Стоп** отменяет операцию.

Примечание

В этом режиме Radmin не поддерживает сетевые диски.

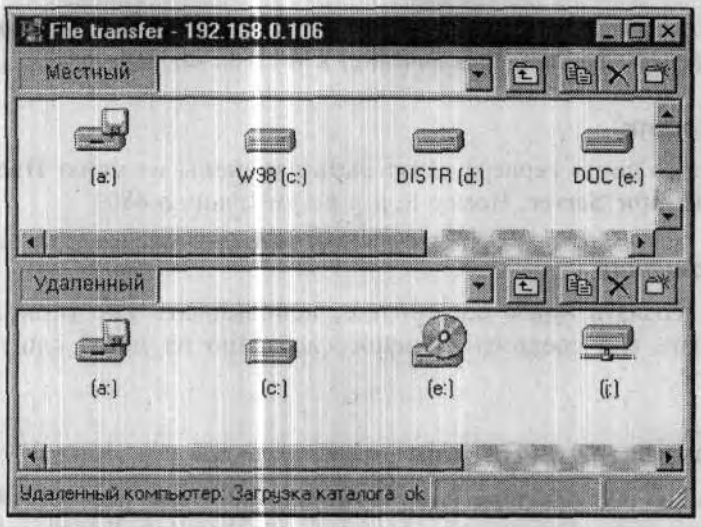


Рис. 6.19. Панели перемещения файлов

Переключение между нормальным и полноэкранным режимами

Переключение между нормальным, растянутым (в этом режиме экран удаленного компьютера вписывается в окно программы) и полноэкранным режимами производится нажатием клавиши <F12>. Если вы хотите передать клавишу <F12> удаленному компьютеру, используйте команду **Передать F12** из меню **RScreen window**. Иногда режим нормального просмотра не подходит (например, экран удаленного компьютера больше). Тогда можно сжать или растянуть окно **RScreen** на полный экран. Меню удаленного экрана вызывается комбинацией клавиш <Ctrl>+<F12>.

Полноэкранный текстовый режим

Radmin не регистрирует экранные изменения, если удаленный компьютер находится в полноэкранном текстовом режиме. В таком режиме GDI (Graphic Display Interface, графический интерфейс) не выполняет прорисовку экрана. Это связано с тем, что в Windows работа драйвера видеопорта не документирована, и разработчики программ не могут применить возможности этого драйвера. Обеспечить текстовый режим на удаленной машине можно в оконном режиме.

Послать <Ctrl>+<Alt>+<Del>

Если вы хотите послать команду <Ctrl>+<Alt>+<Del> на удаленный компьютер, то можно воспользоваться пунктом меню окна обозревателя **Послать <Ctrl>+<Alt>+<Del>**. Эта возможность у вас появится только при

подключении в режиме полного контроля и работе Radmin-сервера как системного сервиса под управлением Windows NT или Windows 2000. Эту команду на удаленный компьютер можно послать и с помощью комбинации "горячих" клавиш: <Ctrl>+<Alt>+<F12>.

Послать команду

Вы можете использовать этот пункт меню для отправки на удаленный компьютер "горячих" клавиш, таких как:

- <Ctrl>+<Esc> — для вызова главного меню;
- <F12> — для изменения размеров окна клиентской части программы Radmin, если она запущена на удаленном компьютере;
- <Ctrl>+<F12> — для вызова меню в окне клиентской части программы Radmin, если она запущена на удаленном компьютере;
- <Alt>+<F12> — аналог команды <F12>;
- <Ctrl>+<Alt>+<F12> — для вызова окна завершения работы на удаленном компьютере.

Команды для получения и установки буфера обмена

Эти команды меню **RScreen** позволяют изменять содержимое буфера обмена.

Для того чтобы скопировать буфер обмена:

1. Выделите текст в удаленном окне.
2. Выполните стандартную команду **Копировать** (можно просто нажать <Ctrl>+<C>).
3. Щелчком кнопки мыши выполните команду **Получить буфер**, она доступна в меню окна удаленного компьютера **RScreen**, которое вызывается нажатием клавиш <Ctrl>+<F12>.
4. Выполните стандартную команду **Вставить** (<Ctrl>+<V>), предварительно переключившись для работы в локальном окне.

Примечание

Radmin не позволяет работать с файлами через буфер обмена.

Перезагрузка

Radmin позволяет вам перезагрузить и выключить удаленный компьютер, завершить и возобновить сеанс пользователя на этом компьютере. Сделать это можно из меню окна удаленного компьютера **RScreen**.

Настройки окна удаленного компьютера (Rscreen)

Если процессор на удаленном компьютере сильно загружен — установите меньшее значение максимальной скорости обновлений в минуту в настройках **RScreen**. Если удаленный компьютер работает под Windows 95/98 (или под Windows NT, без установленного драйвера видеозахвата) Radmin-сервер может стать причиной большой загрузки процессора при установке максимальной скорости более 50 обновлений в минуту.

Отключение обоев на рабочем столе приводит к увеличению скорости взаимодействия между локальным и удаленным компьютерами. Кроме того, можно установить **Формат цвета** в режим **16 цветов** (доступно в меню свойств соединения). Если вы подключены через модем dial-up, то не сможете установить более 10 обновлений экрана в секунду, потому что сигнал не способен пройти туда и обратно более 10 раз в секунду (`ping > 100ms`).

Если применяется операционная система Windows 95/98 на удаленной стороне, скорость будет зависеть от разрешения экрана удаленного компьютера. Устанавливайте невысокие разрешения на удаленном компьютере. Кроме того, пользуйтесь пониженными цветовыми форматами 8bpp (256 цветов) или 16bpp (65 536 цветов). В некоторых системах быстрее формат 8bpp, в некоторых — 16bpp. Убедитесь, что скорость обновления не ограничена полем **Максимальная скорость обновлений в минуту** в настройках окна **Rscreen**.

Если вы пользуетесь на удаленной машине Windows NT без установленного драйвера видеозахвата, помните, что с этим драйвером Radmin работает примерно в 10 раз быстрее и намного меньше использует процессорного времени.

Статистика соединения

Используйте окно **Информация о соединении**, вызываемое из меню **Rscreen**, предоставляющего окно для получения информации о количестве прорисовок в секунду, байтов, переданных в секунду, и т. д.

Управление из командной строки (Command line)

Radmin-клиент может управляться из командной строки, которая позволяет создавать соединение с хостом без использования адресной книги.

Приведем формат такой командной строки:

```
radmin.exe /connect:xxxxx:nnnn other_options
```

Например:

```
radmin.exe /connect:server:1000 /fullscreen /encrypt
radmin.exe /connect:10.0.0.100:4000 /telnet
radmin.exe /connect:server /through:gate
```

Для выполнения настроек в командной строке используются следующие ключи.

- `/connect:xxxxx:nnnn` — указывает сервер и порт для подключения. Этот ключ обеспечивает соединение с сервером даже при отсутствии записи в адресной книге.
- `/through:xxxxx:nnnn` — указывает адрес и порт промежуточного сервера.

По умолчанию устанавливается режим соединения **Полный контроль** (видеть удаленный экран, управлять мышью и клавиатурой).

Для указания других режимов соединения используются следующие ключи:

- `/noinput` — режим просмотра (видишь только экран);
- `/shutdown` — режим удаленного выключения компьютера;
- `/file` — режим пересылки файлов;
- `/telnet` — режим телнет.

Следующие далее ключи работают только в режимах **Полный контроль** и **Просмотр**:

- `/fullscreen` — устанавливает полноэкранный режим просмотра;
- `/hicolor` — устанавливает формат 65 536 цветов для передачи по сети;
- `/locolor` — устанавливает формат 16 цветов для передачи по сети;
- `/updates:nn` — указывает максимальное количество прорисовок для просмотра;
- `/encrypt` — включает шифрование всех данных при работе.

Другие ключи:

- `/unregister` — удаляет все уже введенные ключи для Radmin;
- `/?` — показывает окно помощи.

Но, конечно, лучше всего, если вы все настройки будете производить, следуя указаниям программы установки или используя меню **Настройка Remote Administrator Server**. В этом случае вам не придется пользоваться настройками из командной строки.

Есть еще несколько команд для системных администраторов, позволяющих вручную инсталлировать и деинсталлировать Radmin-сервер, а также изменять его настройки (номер порта, пароль и т. д.). Рассмотрим одну из них:

```
r_server.exe
```

Программу r_server.exe можно выполнять со следующими ключами.

- `/setup` — запускает диалог (мастера), который вам поможет установить сервис и драйвер, а также указать пароль и номер порта для Radmin-сервера. Например:

```
r_server.exe /setup
```

- `[/port:xxxx] [/pass:xxxxx]` — если в командной строке нет никаких других ключей, кроме `/port` и `/pass`, программа r_server выполняется как Radmin-сервер. Далее приведены примеры возможных вариантов командной строки:
  - `r_server.exe`;
  - `r_server.exe /pass:mypass` — устанавливает пароль `mypass` для сервера Radmin;
  - `r_server.exe /port:5505` — устанавливает номер порта 5505 для сервера Radmin;
  - `r_server.exe /port:3333 /pass:qwerty` — устанавливает пароль `qwerty` и номер порта 3333 для сервера Radmin.
- `/save [/port:xxxx] [/pass:xxxxx]` — позволит вам изменить номер порта и/или пароль в реестре. Например, для сохранения пароля и номера порта в реестре следует ввести команду:

  ```
  r_server.exe /port:5505 /pass:qwerty /save
  ```

  Для записи в реестр номера порта по умолчанию и пустого пароля выполните команду:

  ```
  r_server.exe /save
  ```
- `/install` — позволяет установить программу.
- `/uninstall` — деинсталлирует программу.
- `/installservice` — устанавливает только сервис.
- `/uninstallservice` — деинсталлирует сервис.

  Важно

  Ошибочное выполнение данной команды сопровождается сообщением о том, что сервис не установлен.

- `/silence` — не показывать сообщения об ошибках (`error`) или успешно выполненных операциях (`ok`) при запуске с ключами: `/install`, `/uninstall` или `/save`.
- `/stop` — останавливает Radmin-сервер. Применение этого ключа останавливает сервис и завершает приложение. Для остановки сервиса под Windows NT требуется наличие соответствующих прав.
- `/?` — показывает окно помощи.

Остановка Radmin-сервера

Для остановки сервера вы можете использовать соответствующий ярлык в папке Remote Administrator или просто ввести в командную строку:

```
r_server.exe /stop
```

Адресная книга Radmin

Вся информация об удаленных подключениях содержится в адресной книге. Ваша адресная книга хранится в системном реестре (registry). Все операции с ней можно выполнять с помощью regedit.exe. Экспортируйте в файл все ключи, находящиеся в разделе реестра HKEY_CURRENT_USER\Software\RAdmin\v2.0\Clients.

Далее вы можете импортировать этот файл (собственно адресную книгу) в реестр на другом компьютере. Если вы хотите воспользоваться старой (из прошлой версии программы) адресной книгой, то выполните следующую команду, создающую адресную книгу Radmin2.x из Radmin1.11:

```
radmin.exe /copyphonebook
```

Несмотря на то, что Windows имеет некоторые встроенные средства для работы с удаленным рабочим столом, они не идут ни в какое сравнение с описанной программой. Более того, используя эту программу, вы можете работать с каталогами, доступ к которым по сети запрещен для пользователей. Никто, кроме вас, к этим каталогам не сможет подключиться из сети. Единственное средство, встроенное в Windows 2000 Server, которое может заменить Radmin при удаленной работе с самим сервером, — это сервер терминалов. Но с его помощью вы не получите доступ к компьютерам сети. Интересной может быть и возможность работы двух администраторов или пользователей с различных компьютеров с рабочим столом третьей машины одновременно. Но такая задача потребует дополнительной лицензии на программу, цена которой, впрочем, не так уж и высока — 750 рублей.

Вспомогательные средства

Существуют задачи, которые не всегда напрямую связаны с работой сети, но от решения которых может зависеть многое. Например, вышедший из строя привод CD-ROM лишит возможности оперативно установить программное обеспечение на компьютер, который вы собирались использовать для решения какой-либо важной задачи в сети. Существуют простые средства, позволяющие осуществить ваши планы, а заодно сэкономить на приобретении нового привода, если на данном компьютере он обычно не нужен.

Прямое кабельное соединение

Редко кто его использует в обычной практике работы с компьютером, но в отдельных случаях это почти единственное возможное решение возникшей проблемы. Для настройки соединения необходима небольшая предварительная подготовка. Лучше ее провести до возникновения проблемы, и быть готовым, когда это понадобится. Нужно изготовить или приобрести кабель,

который можно использовать для такого соединения. Подходит обычный кабель с двумя разъемами LPT. Разберите один из разъемов кабеля и перепаяйте жилы в соответствии с табл. 6.6.

Таблица 6.6. *Распайка кабеля для LPT-порта*

Разъем 1	Разъем 2	Разъем 1	Разъем 2
1	7	14	8
2	15	15	2
3	13	16	9
4	12	17	7
5	10	18	18
6	11	19	19
7	1	20	20
8	14	21	21
9	16	22	22
10	5	23	23
11	6	24	24
12	4	25	25
13	3		

После переделки вы получите *нуль-модемный кабель*, который можно применить для прямого кабельного соединения двух компьютеров.

Для настройки прямого кабельного соединения необходимо установить этот компонент в Windows 9*x*. Установка производится стандартным образом.

При запуске программы появится окно со списком портов, доступных для подключения (рис. 6.20), затем окно, позволяющее определить роль компьютера (рис. 6.21).

В последующих окнах потребуется ввести имя компьютера, с которым устанавливается связь. После выполнения соединения вы увидите в окне проводника папки, к которым открыт доступ (рис. 6.22), и сообщение об установлении связи. Программа очень проста в использовании, но имеет некоторые ограничения. Если связь настроена с одним из компьютеров, необходимо переустановить программу для настройки связи с другим.

Есть и другой вариант установки связи по кабелю. Достаточно иметь на обоих компьютерах программу Norton Commander версии 4 или выше.

Важно иметь одну и ту же версию. При установлении связи на экране ведомого компьютера появится сообщение с указанием некоторых параметров сеанса связи. При этом работать в окне файлового менеджера будет нельзя (рис. 6.23).



Рис. 6.20. Прямое соединение (выбор портов)

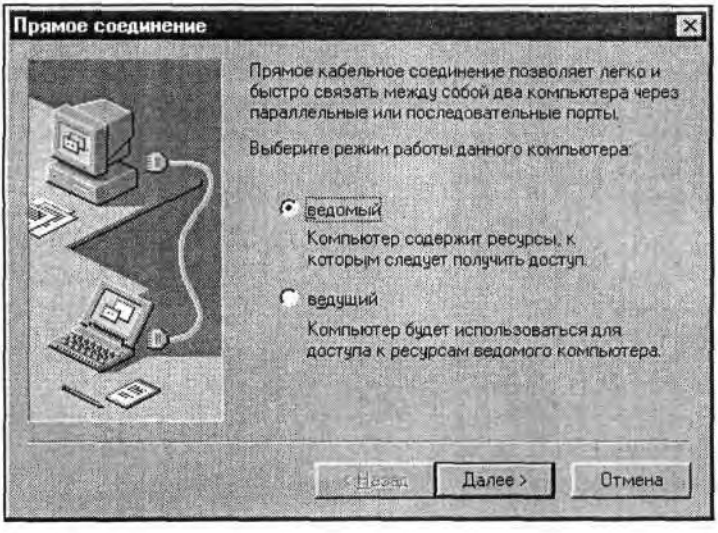


Рис. 6.21. Прямое соединение (определение роли компьютера)



Рис. 6.22. Прямое соединение (состояние)



Рис. 6.23. Norton Commander (ведомый компьютер)

На экране ведущего компьютера будет изображение всех файлов и дисков ведомого, включая сетевые и те, к которым доступ не открывался (рис. 6.24).



Рис. 6.24. Norton Commander (ведущий компьютер)

Соединение возможно с любым компьютером в любое время без предварительной установки программ.

Для соединения применяется тот же кабель. Само соединение устанавливается при выборе пункта **Связь** в меню любой из панелей Norton Commander. Первым должен быть установлен в режим связи ведущий компьютер.

Соединение может быть установлено как из Windows, так и из DOS.

Примечание

Во всех случаях прямого кабельного соединения длина кабеля не должна превышать 5 м.

Существуют и другие программные средства для организации связи через LPT- или COM-порты. Любое из этих средств может быть полезно при неисправностях, связанных с сетевым взаимодействием компьютеров, и необходимости в то же время установить связь между ними.

Конечно, приведенными примерами инструменты администратора не ограничиваются. В зависимости от встающих перед вами задач могут потребоваться и другие средства. Сохраняйте все найденные вами и заинтересовав-

шие вас вспомогательные программы. Некоторые инструменты могут применяться очень редко, но когда наступает соответствующий момент, без них приходится трудно. Следует обратить внимание и на набор Resource kit, находящийся на лицензионных дисках с операционными системами.

Правила администратора

Взяв на себя право быть хозяином сети, вы должны также принять и некоторые обязанности. Опишем некоторые из них в виде правил, которыми должен руководствоваться администратор сети.

- Никогда и никому не доверяйте пароль администратора. Лучше создайте еще одну учетную запись пользователя, наделенного необходимыми правами. Позже вы можете удалить эту запись. Однажды раскрытый пароль администратора через короткое время будет известен многим. Время от времени следует менять этот пароль.
- Регулярно проверяйте сервер, а при возможности и компьютеры пользователей на наличие вирусов. Ваша сеть может подвергаться вольным или невольным вирусным атакам. В Интернете можно найти достаточно много бесплатных антивирусных программ, но лучше приобрести программу, которую вы сможете регулярно обновлять и получать поддержку производителя. Никого не допускайте к настройкам сервера. В процессе развития и роста сети эти настройки будут становиться все сложнее, а нарушить их случайным нажатием клавиши можно очень легко. Восстанавливать нормальную работу сети, а заодно выслушивать недовольные голоса пользователей, придется вам.
- Регулярно ведите дневник.
- Не оставляйте незавершенными работы по настройке или обслуживанию сервера. Будьте внимательны и аккуратны, проводя эти работы.
- Внимательно относитесь к распределению прав пользователей сети. Слишком широкие права могут быть причиной нарушений работы сети, вызванных случайными или преднамеренными действиями пользователей.
- Внося изменения в настройки сервера, проанализируйте все возможные последствия и возможность отката для этих изменений.
- Не оставляйте сервер и важнейшие точки подключения кабельной системы без присмотра. Лучше, если сервер находится в отдельном помещении, доступ к которому есть только у вас.
- Никогда не работайте на сервере как на рабочей станции. Это может привести ко многим неприятностям.

- Следите за исправностью электропроводки и кабельной разводки, периодически осматривая участки сети, недостаточно защищенные от случайного воздействия.
- Регулярно проводите профилактическое обслуживание сервера.
- Внимательно относитесь к жалобам и просьбам пользователей. Иногда кажущаяся вам необоснованной жалоба может быть предвестником серьезного сбоя на сервере.
- Не используйте основной сервер для подключения к сети Интернет. Как бы не была надежна защита от внешнего проникновения, средства защиты всегда отстают от средств нападения.
- Не "варитесь в собственном соку", общайтесь с другими администраторами сетей. Коллективное знание поможет решить любые проблемы.



Глава 7

Устанавливаем сервер

Мы начинаем установку первого сервера сети. В дальнейшем понадобится второй сервер. Конфигурация сервера может очень сильно зависеть от его роли в сети. Назначение каждого из серверов желательно определить заранее, если предполагается установка именно двух серверов. Выбор конкретной конфигурации во многом зависит от вас и от требований, предъявляемых к вашей сети. Возможно, что последовательность настройки серверов, предложенная здесь, не подойдет вам. Но ничто не мешает ее изменить. Большинство серверных функций независимы друг от друга, и их совместимость на одном сервере определяется скорее здравым смыслом и поставленной задачей, чем физическими возможностями компьютера и ОС. В очень крупных сетях каждая функция может выполняться отдельным компьютером, а в нашем случае все функции сервера может выполнять и одна машина. Но есть некоторые ограничения, связанные с сетевой безопасностью, например, с балансировкой нагрузки между компьютерами, которые требуют применения второго сервера.

Одна из важнейших функций сервера сети, это обеспечение работы Active Directory — каталога сведений об объектах сети, в котором можно публиковать любые доступные ресурсы. Самое главное назначение Active Directory в небольшой сети — это регистрация пользователей, компьютеров и принтеров, определение прав пользователей на доступ к ресурсам сети и на режим работы в ней (можно разрешить работу пользователя в сети только в рабочие дни и только в рабочее время).

Практически все возможности сервера определяются его операционной системой. Существует множество сетевых ОС, которые в той или иной мере пригодны для работы на сервере. Но по широте своих возможностей, и в то же время по простоте администрирования на настоящий момент трудно найти конкурента для Windows Server 2003. Кто-то скажет, что Linux обладает тоже очень широкими возможностями, но никто не скажет, что администрировать такой сервер сможет начинающий администратор. Следует учитывать и то, что малые сети нередко становятся частью больших сетей. Так,

наша сеть, состоявшая когда-то из двадцати рабочих станций, теперь влилась в сеть, которая объединит более тридцати предприятий. Применяемое программное обеспечение требует, чтобы все сети были основаны на системах Windows. Да и ваша сеть, поскольку вы еще не прекратили чтение этой книги, построена на Windows.

Windows Server 2003

В *главе 2* мы уже рассматривали некоторые особенности этой операционной системы, даже применили ее на рабочей станции. Теперь начнем работу с ней, как с настоящей серверной операционной системой. Обычно на сервере сети (если это не сервер приложений) недопустима повседневная работа пользователей, как на обычной рабочей станции. Это связано с обеспечением бесперебойной работы сервера. Операции, выполняемые локальным пользователем на сервере, могут быть, как просто ресурсоемкими, так и потенциально опасными для сервера и сети в целом. Следовательно, для работы в качестве сервера следует выделить отдельную машину. Если сервер требуется в домашней сети, пользователями которой являются жители нескольких квартир, — придется договариваться или находить другие пути финансирования, чтобы приобрести компьютер-сервер. Характеристики приобретаемого компьютера должны обеспечивать возможность установки Windows Server 2003.

Некоторые отличия Windows Server 2003 от Windows 2000 Server

Windows Server 2003 Standard Edition — это наиболее подходящая для малых сетей версия Windows Server 2003. Если вам приходилось иметь дело с Windows 2000 Server, то в большинстве случаев общения с сервером вы будете встречаться с уже знакомыми операциями и функциями. Тем не менее, будут заметны и отличия.

Прежде всего, сервер на базе Windows Server 2003 более стабилен и более защищен по сравнению с Windows 2000 Server. Многие положительные качества Windows XP перенесены в новую серверную систему, что увеличило ее устойчивость и защищенность. Пользователям малых сетей не придется приобретать дополнительное программное обеспечение для организации надежной защиты сети со стороны Интернета, для организации достаточно удобного почтового сервера. В Windows 2000 Server эти возможности отсутствовали. Возможное объединение вашей сети с другими, более крупными сетями может потребовать изменения некоторых параметров уже работающей сети или настройки взаимодействия объединяемых сетей, чтобы обес-

печить совместную работу пользователей. Такие преобразования в Windows Server 2003 требуют меньше усилий и времени, чем в Windows 2000 Server. В отдельных случаях, можно увидеть более удобные средства управления учетными записями пользователей в сети. Другие преимущества новой ОС могут быть заметны разработчикам новых интернет-приложений с использованием языка XML.

Тем не менее, вполне возможно сосуществование в одной сети обеих операционных систем. Так, если у вас уже работает сервер с настроенным контроллером домена под управлением Windows 2000 Server, то вы вполне можете применить Windows Server 2003 в качестве второго сервера, обеспечивающего разнообразные Web и почтовые сервисы, может быть и сервер печати, и сервер архивов, а также другие необходимые в вашей сети функции. Возможности ОС позволяют отказаться от приобретения дополнительного оборудования для настройки маршрутизации и NAT, обеспечивая доступ вашей сети к другим сетям и Интернету, а также работу сетевых приложений.

Установка

Мы будем исходить из предположения, что ваша сеть еще не имеет сервера и работает одноранговая сеть. Вам решать — использовать описанные далее настройки сервера или применять другие средства, обеспечивающие описанные возможности программными или аппаратными средствами, если они у вас уже работают. Но при отсутствии других средств вы можете настроить работу сети, основываясь только на возможностях операционной системы.

Начиная модернизацию одноранговой сети до сети с выделенным сервером, можно выбрать различные планы перехода. Можно начать с установки Active Directory, чтобы обеспечить простоту управления учетными записями, но можно сначала настроить и дополнительные функции сервера, обеспечивающие связь с внешним миром. Мы начнем именно с этих дополнительных функций. Это позволит тем, у кого уже работает Active Directory, приступить к установке второго сервера. Мы будем считать этот сервер своим первым сервером. Само собой разумеется, что начать придется с установки ОС. Но описывать процесс первоначальной установки мы здесь не будем. Он мало отличается от подобных процедур для других операционных систем. Главные отличия появляются уже после установки ОС, когда сервер предлагает настроить свои роли в сети.

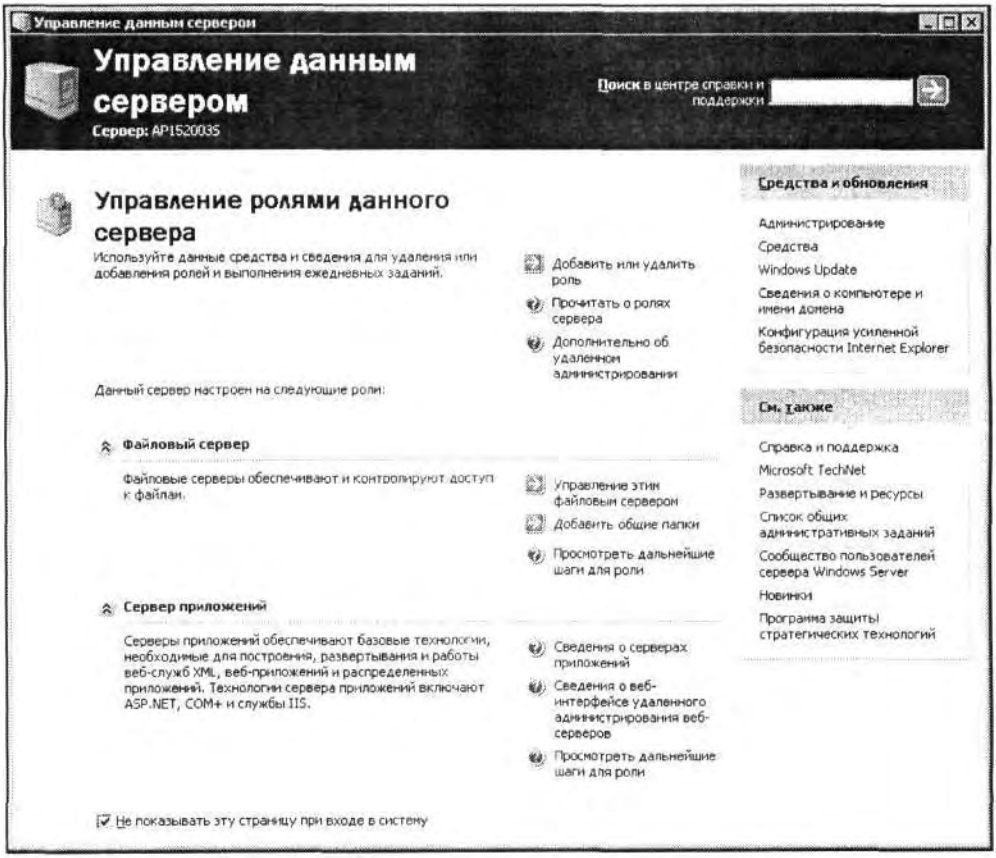


Рис. 7.1. Окно **Управление данным сервером**

После установки ОС окно **Управление данным сервером** (рис. 7.1) появляется автоматически. Если вы отказались от показа этой страницы при входе в систему, то позднее ее можно открыть, выбрав пункт меню **Администрирование | Управление данным сервером**. В этом окне нас на начальном этапе будет интересовать пункт меню **Добавить или удалить роль**. Перед выбором роли сервера вы можете в том же окне воспользоваться ссылками на справочные материалы. Это позволит более подробно познакомиться с возможностями вашего сервера.

При выборе пункта меню **Добавить или удалить роль** мастер настройки сервера (рис. 7.2) сразу предложит проверить все условия, которые должны быть выполнены перед продолжением настройки.

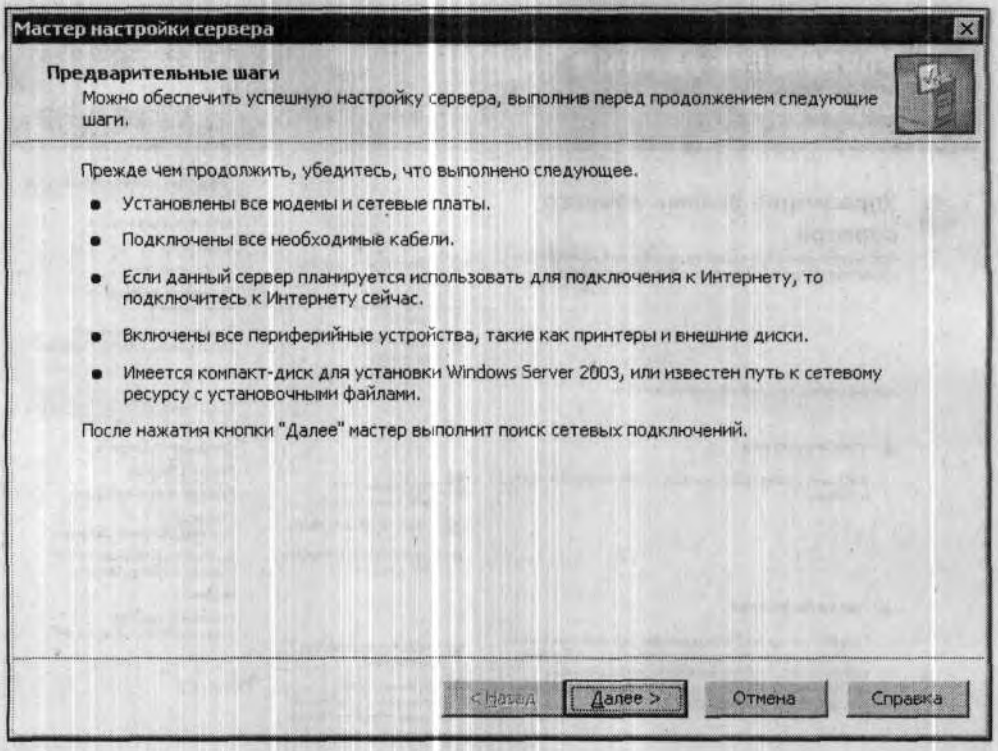


Рис. 7.2. Окно **Мастер настройки сервера**

Подключение сети к Интернету

В данном примере мы будем рассматривать не совсем обычный вариант подключения, который продемонстрирует достаточно широкие возможности сервера в сети и возможности конфигурирования локальной сети. Сеть, в которой работает этот сервер, уже имеет выход в Интернет через аппаратные средства. А доступ через сервер предоставляется еще одной сети, подключаемой к серверу через отдельный интерфейс (второй сетевой адаптер). При подключении к Интернету единственной сети через ADSL-модем, подключенный к серверу, изменятся только IP-адреса. Процедура настройки подключения останется совершенно такой же.

В данном примере (рис. 7.3) компьютер-сервер имел до проведения настроек роль обычной рабочей станции в сети 192.168.1.0. Роль этого компьютера повышается до сервера, но для второй сети, которая только что устанавливается, и будет использовать для доступа в Интернет уже работающий сервер. Маршрутизатор, применяемый для доступа в Интернет одноранговой

сети 192.168.1.0, имеет внешний IP-адрес, назначенный провайдером. Для сети 10.15.2.0 провайдером будет сеть 192.168.1.0. Адрес, назначенный для выхода в Интернет второй сети, 192.168.1.7. Это адрес сетевого адаптера сервера, обращенный в первую сеть. Сервер для второй сети в данном случае играет роль маршрутизатора. Причем рассматриваемый пример предполагает настройку NAT, что приведет к тому, что все компьютеры второй сети (10.15.2.0) будут подключаться к Интернету, и даже в первую сеть с одним общим IP-адресом. На этом, собственно говоря, и основана работа NAT.

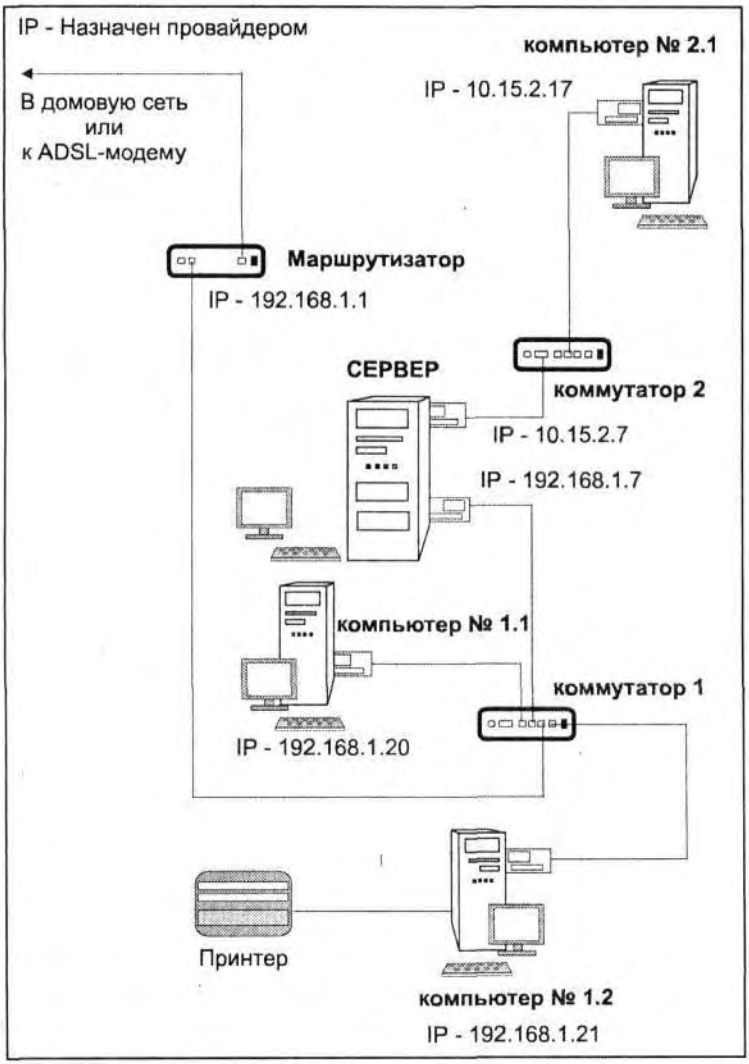


Рис. 7.3. Подключение сети 10.15.2.0 к Интернету через сервер

Примечание

Если вы не имели опыта работы с сетями подобного рода, рекомендуем внимательно разобраться в описываемом примере. Это позволит в дальнейшем понять работу своей реальной сети и принять верные решения при ее настройке и модернизации.

На рис. 7.3 показана только одна рабочая станция из сети 10.15.2.0, но реально их число может быть любым допустимым в сети и ограничивается маской подсети.

Мастер предлагает уже сейчас, перед продолжением настроек, подключить сервер к Интернету. Этот момент нашей работы следует предварить важным замечанием.

Замечание

Подключение к Интернету без соблюдения мер предосторожности может привести к неприятным последствиям. Активность различных вирусов, существующих в сетях, меняется и иногда достигает угрожающих значений. Первое подключение сервера к Интернету следует делать при отключенной локальной сети. Обязательно следует включить брандмауэр.

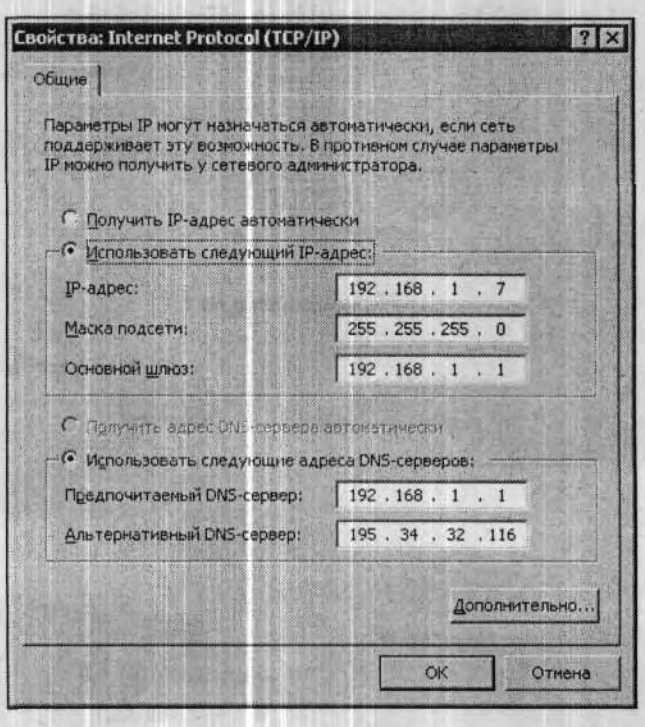


Рис. 7.4. Окно **Свойства: Internet Protocol (TCP/IP)** для внешнего сетевого адаптера сервера

Конечно, если вы повторяете описываемый пример полностью, то угрозы неожиданного заражения уже практически не существует, ведь реальное подключение к Интернету уже настроено. Но подключение единственной сети с единственным сервером требует осторожности.

Продолжим настройки.

Сетевой адаптер, смотрящий во внешнюю сеть, должен быть настроен до продолжения работы мастера.

На рис. 7.4 показаны настройки внешнего сетевого адаптера сервера. Еще раз отметим, что при использовании подключения через ADSL-модем необходимо указать значения IP-адреса, маски подсети, основного шлюза и DNS-серверов, предоставленные провайдером. Но в нашем случае эти параметры выбраны в соответствии с параметрами внешней (для настраиваемой) сети.

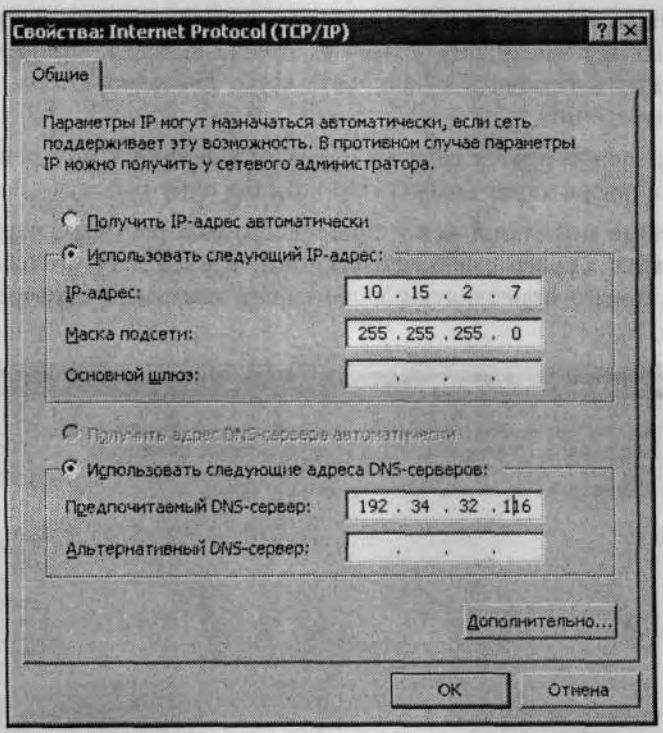


Рис. 7.5. Окно **Свойства: Internet Protocol (TCP/IP)** для внутреннего сетевого адаптера сервера

Кроме настройки подключения сервера к Интернету, мастер настройки сервера требует подключения всех кабелей и установки всех сетевых адаптеров.

Проверим настройку второго сетевого адаптера, который будет соединять сервер со второй сетью (рис. 7.5).

Для этого адаптера нет необходимости указывать основной шлюз. Если в вашей сети уже настроен DNS-сервер, то можно указать его адрес в качестве альтернативного. Основной DNS-сервер в нашем случае имеет адрес, предоставленный провайдером.

Примечание

Для доступа в Интернет можно использовать адреса любых DNS-серверов. Но серверы, не имеющие отношения к провайдеру, могут быть не доступны в процессе установления соединения.

Возможно, что вы обратили внимание на то, что маска подсети, используемая в этом примере, не соответствует обычному значению для сетей класса A, которые обычно имеют адреса вида 10.X.X.X. У каждого правила есть исключения. Ведь нам не требуется такого количества компьютеров в сети, которое позволяет иметь сеть класса A. Маска подсети, примененная нами, дает возможность включать в нашу сеть всего 254 компьютера, но нам этого более чем достаточно.

Остается проверить работу сети 10.15.2.0, подключив к внутреннему сетевому адаптеру сервера через коммутатор хотя бы одну рабочую станцию.

Если вы можете подключиться к общедоступным ресурсам сервера или можете "пинговать" сервер с рабочей станции, и `ping` дает положительные результаты, то можно приступать к дальнейшей настройке сервера.

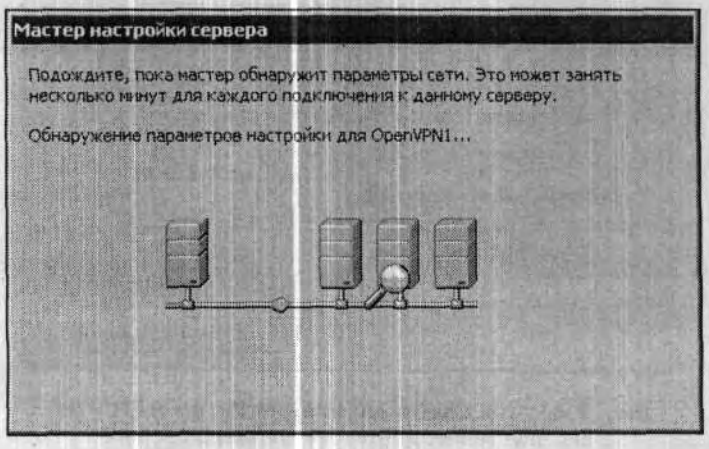


Рис. 7.6. Мастер настройки сервера определяет параметры подключений

После нажатия кнопки **Далее** в окне мастера настройки сервера начнется сбор информации о параметрах сети (рис. 7.6). Проанализировав сеть, мастер настройки сети покажет следующее окно (рис. 7.7), в котором перечислены уже применяемые или не применяемые роли сервера.

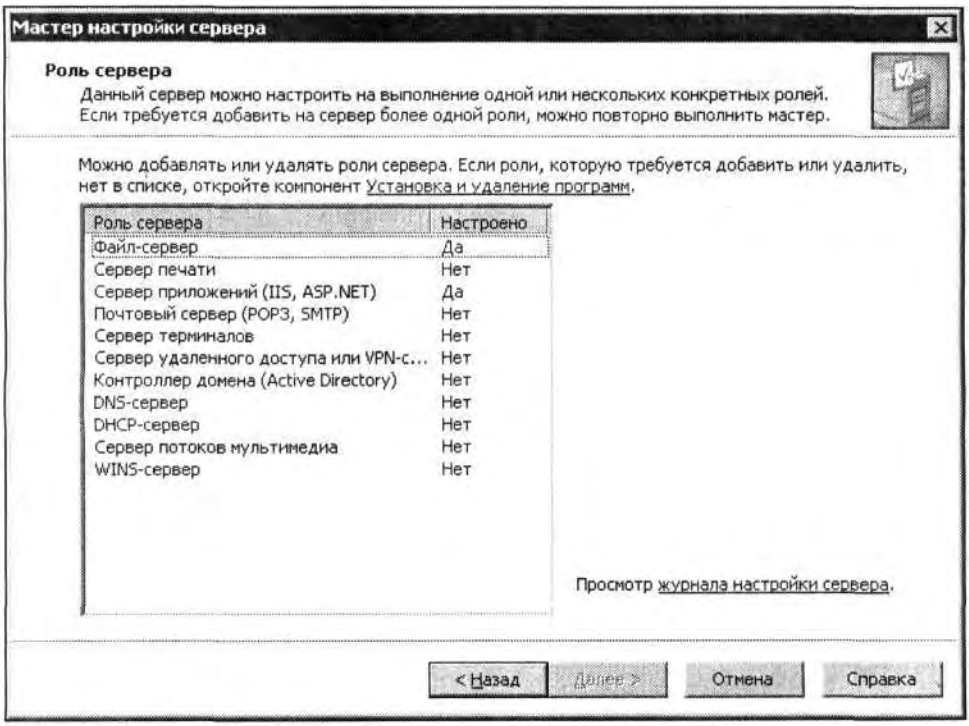


Рис. 7.7. Мастер настройки сервера — роль сервера

На данном сервере уже работает общий доступ к файлам и создан Web-сервер. Поэтому роли **Файл-сервер** и **Сервер приложений** отмечены как настроенные. Нас в приведенном списке интересует строка **Сервер удаленного доступа или VPN-с**. Выбрав этот пункт, нажимаем кнопку **Далее**. Появится окно с информацией о том, что после нажатия кнопки **Далее** будет запущен мастер настройки маршрутизации и удаленного доступа. Нажимаем кнопку **Далее**.

Мастер настройки маршрутизации и удаленного доступа предлагает выбрать вариант продолжения настроек (рис. 7.8). В соответствии с нашей задачей выбираем **Преобразование сетевых адресов (NAT)**. Конечно, опять нажимаем кнопку **Далее**. Мастер снова предлагает выбор (рис. 7.9). На этот раз нужно выбрать общедоступный сетевой адаптер или создать интерфейс для нового

подключения по требованию. Второй вариант можно выбрать, если вы решили настроить подключение через коммутируемый доступ к Интернету или другое подключение, которое должно включаться по требованию. Но в данном примере мы настраиваем доступ через постоянное подключение к Интернету. Поэтому выбираем сетевой адаптер, который смотрит в подключаемую сеть. В нашем примере IP-адрес этого адаптера 10.15.2.7.

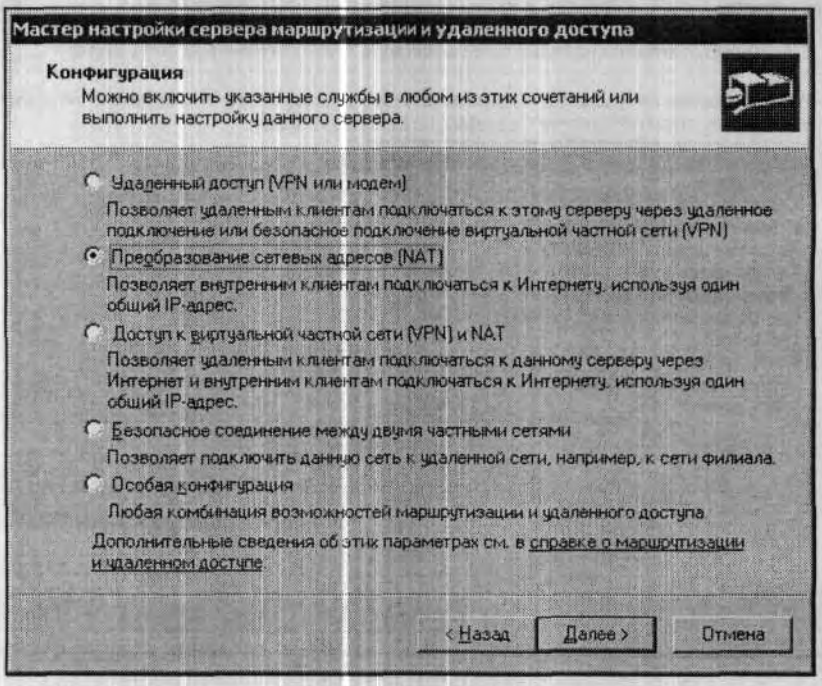


Рис. 7.8. Окно **Мастер настройки сервера маршрутизации и удаленного доступа**

При настройке подключения напрямую в Интернет обязательно отмечаем флажок **Обеспечить безопасность на данном интерфейсе, установив брандмауэр**.

В следующем окне выбираем соединение, через которое сервер подключен к Интернету (рис. 7.10). В нашем случае это адаптер с адресом 192.168.1.7.

Далее наступает завершающий этап работы мастера. Он предупреждает, что должны быть правильно настроенные службы DNS и DHCP. Пока не обращаем внимания на эти предупреждения. Ведь при отсутствии какой-либо службы сервер не взорвется. Но имеем пока в виду, что все адреса компьютеров наших сетей мы назначили сами. С серверами DNS и DHCP разбираться будем несколько позднее.

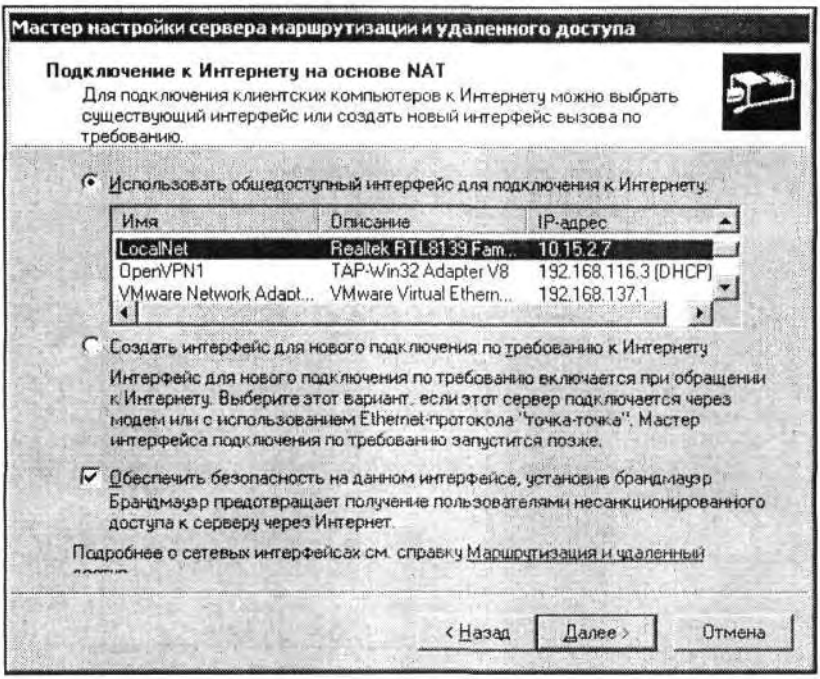


Рис. 7.9. Окно **Мастер настройки сервера маршрутизации и удаленного доступа** (подключение к Интернету на основе NAT)

Последним шагом мастера настройки будет запуск службы маршрутизации и удаленного доступа и сообщение о том, что сервер настроен в качестве сервера маршрутизации и удаленного доступа.

Пробуем подключение к Интернету с компьютера 10.15.2.17. Ничего не получилось! Проверяем весь путь наших настроек. Если вы делали реальные настройки, то, вероятно, документировали их. Просмотрим наши записи или текст в книге. Во время работы мастера были перепутаны интерфейсы сервера!

Подключение к Интернету выбранной подсети происходит на самом деле через адаптер с адресом 10.15.2.7, а общедоступный интерфейс 192.168.1.7. Что ж, ошибки всегда возможны. Обнаруживаются они обычно потому, что не работает то, что мы настраивали. Исправим ошибку. Откроем **Администрирование | Маршрутизация и удаленный доступ**. Появится окно **Routing and Remote Access** (рис. 7.11).

Выберите в дереве объектов в левой части окна **NAT/Простой брандмауэр**. В правой части окна проверьте свойства интерфейсов, которые подключены на сервере. В данном случае это **LocalNet**, смотрящий в новую сеть 10.15.2.0, и **DOM**, имеющий адрес 192.168.1.7.

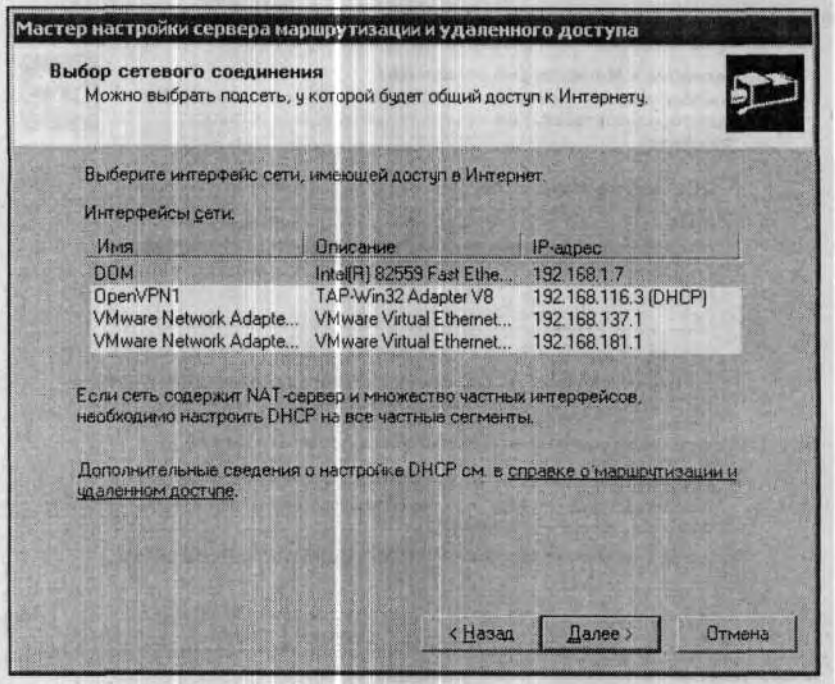


Рис. 7.10. Окно **Мастер настройки сервера маршрутизации и удаленного доступа** (выбор сетевого соединения)

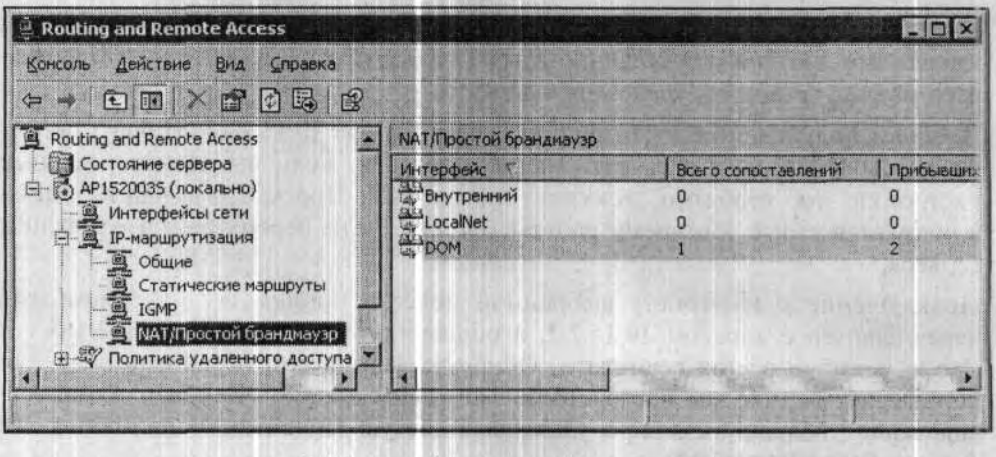


Рис. 7.11. Окно **Routing and Remote Access**

Для **LocalNet** окно свойств должно выглядеть, как на рис. 7.12, а для **DOM**, как на рис. 7.13. Имена сетевых подключений на вашем сервере могут быть

иными. Лучше, если вы их переименуете для того, чтобы легче ориентироваться в их назначении, когда идет настройка сети.

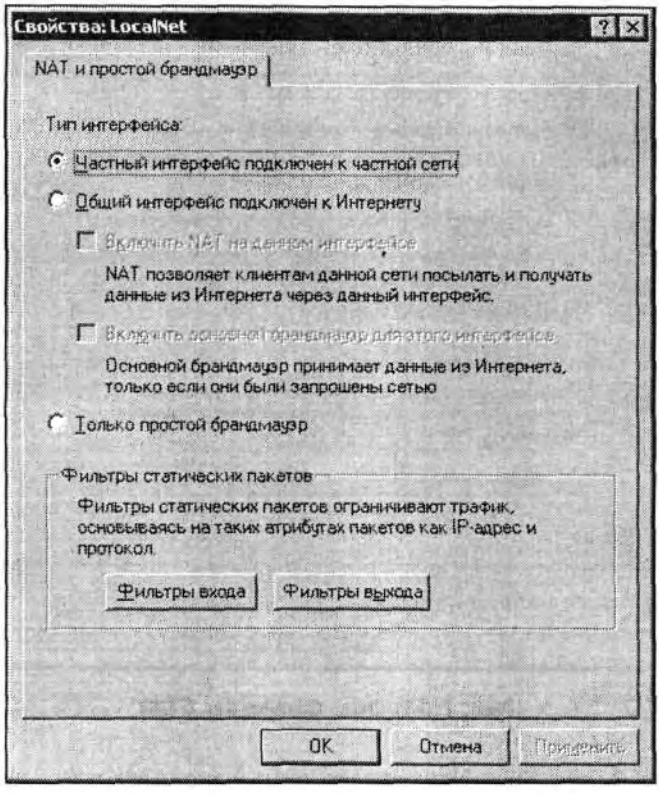


Рис. 7.12. Окно **Свойства: LocalNet**

Простое изменение состояния переключателей и флажков в этих окнах приведет сразу к возможности выхода в Интернет с компьютеров второй сети (10.15.2.0). В частности, с компьютера с адресом 10.15.2.17, который участвует в примере.

Окно **Routing and Remote Access** (см. рис. 7.11) еще не раз нам понадобится для проведения достаточно интересных настроек сети. Можно было вообще все настройки выполнить из этого окна, но для этого надо было бы точно знать, как и что изменить. Мастер настройки сделал это за нас. С помощью данного окна и некоторых дополнительных средств можно будет настроить доступ к вашей сети из Интернета, например, из другой сети, имеющей постоянное подключение к Интернету. Но об этом позднее.

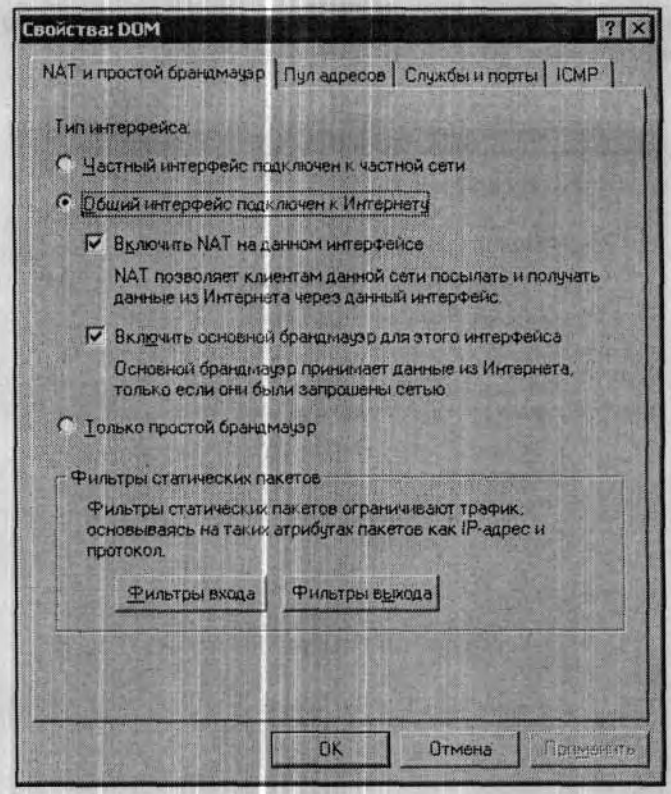


Рис. 7.13. Окно **Свойства: DOM**

Все в мире относительно. Наш сервер стал выполнять одну из своих ролей для второй сети (10.15.2.0). Для сети с адресом 192.168.1.0 этот компьютер остался рядовым.

Рассмотрим настройку еще одного очень полезного компонента — почтового сервера.

Почтовый сервер

Для того чтобы настроить сервер для работы в качестве почтового сервера, можно воспользоваться различными средствами, в том числе и встроенными в операционную систему. Эти средства в большинстве случаев обеспечивают основные потребности сети. Когда работа с электронной почтой составляет одно из основных занятий пользователей сети, лучше применять программы, разработанные для этой цели. Пользователи нашей сети не испытывают никаких неудобств при работе с почтовым сервером, который входит в со-

став Windows Server 2003. Почта у нас используется по своему прямому назначению — пользователи общаются с внешним миром. Для того чтобы иметь возможность получать почту на ваш почтовый сервер, необходимо зарегистрировать ваш домен в Интернете. Для этого есть много возможностей. Одна из них — получить домен второго уровня. Очень часто это предлагается сделать бесплатно. Если ваш провайдер выдает вам динамический IP-адрес, который изменяется с каждым подключением или просто периодически, то можно воспользоваться службами типа DinDNS (**http://www.dyndns.org**) или другими подобными. При условии, что ваш сервер практически постоянно подключен к Интернету, вы сможете всегда найти его из Интернета по символьному адресу. А для работы почты большего и не требуется. Мы не будем рассматривать технологии, которые используются для этих целей, но отметим, что подобные услуги часто бесплатны в объеме, достаточном для наших целей.

Перед настройкой собственно почтового сервера немного подправим работу маршрутизатора (рис. 7.14). Это в уже известном нам окне **Routing and Remote Access**, но на этот раз следует добавить **Статические маршруты**. Это маршруты, которые будет использовать сервер для общения с внешним миром — Интернетом.

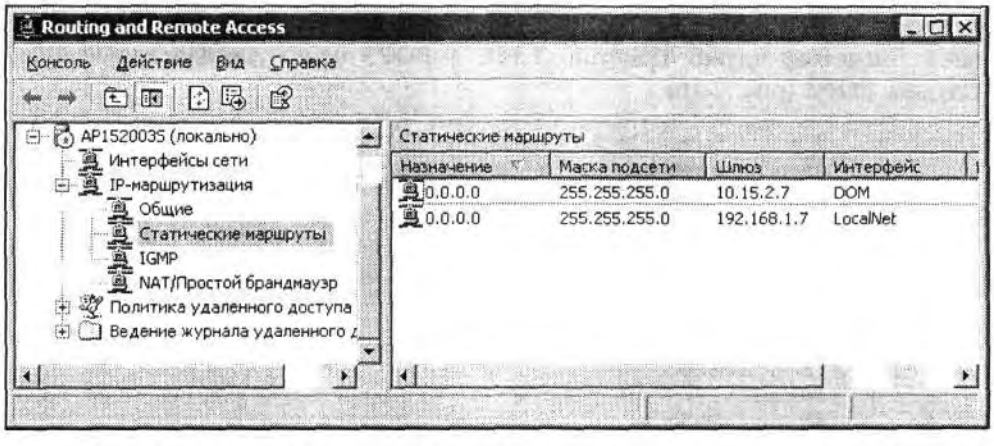


Рис. 7.14. Окно **Routing and Remote Access** (статические маршруты)

Для каждого из двух сетевых интерфейсов противоположный интерфейс становится шлюзом. Адрес назначения 0.0.0.0 обозначает, что нет никаких ограничений для адресов с обеих сторон маршрутизатора. Ограничения накладываются лишь адресом шлюза и маской подсети. В данном примере интерфейс DOM имитирует внешний интерфейс, смотрящий в Интернет. Скорее всего, для такого интерфейса маска подсети будет иной

(255.255.255.252 — наиболее частый вариант), а адрес интерфейса будет соответствовать допустимому в Интернете.

Почтовый сервер начнем настраивать так же, как настраивали доступ в Интернет — воспользуемся мастером настройки сервера. На странице ролей (см. рис. 7.7) выберем **Почтовый сервер**. На следующем шаге нам будет предложено выбрать метод проверки подлинности пользователей и имя домена электронной почты. Для проверки подлинности отметим **Локальные учетные записи Windows**. Это позволит идентифицировать пользователя почты, как учетную запись на сервере. Имя домена электронной почты может быть любым, если предполагается только внутреннее применение сервера, и совершенно определенным, зарегистрированным в Интернете, если сервер будет применятся для внешней связи. Для настройки примера с помощью DinDNS я зарегистрировал домен `okobox.homeip.net`. Поскольку в сети, где настраивается этот пример, почтовые серверы уже есть, мы воспользуемся нестандартным значением порта для SMTP-сервера. Это может быть полезно и в случае, когда вы хотите сделать почтовый сервер недоступным для большинства пользователей Интернета, применяя его в каких-либо специальных целях. Итак, в примере почтовый домен `okobox.homeip.net`. После ввода данных и нажатия кнопки **Далее** начнется процесс установки, во время которого может потребоваться дистрибутив системы. После завершения установки требуется ручная подстройка сервера. Для чего нужно открывать отдельно SMTP и POP3-серверы. SMTP открывается через **Администрирование | Диспетчер служб IIS** (рис. 7.15), а POP3 через **Администрирование | Служба POP3** (рис. 7.16).

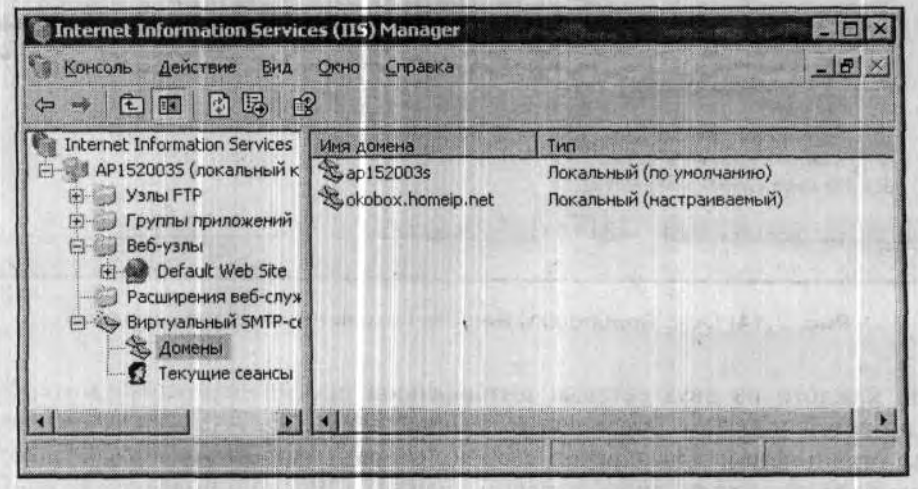


Рис. 7.15. Окно **Internet Information Services (IIS) Manager** (управление SMTP-сервером)

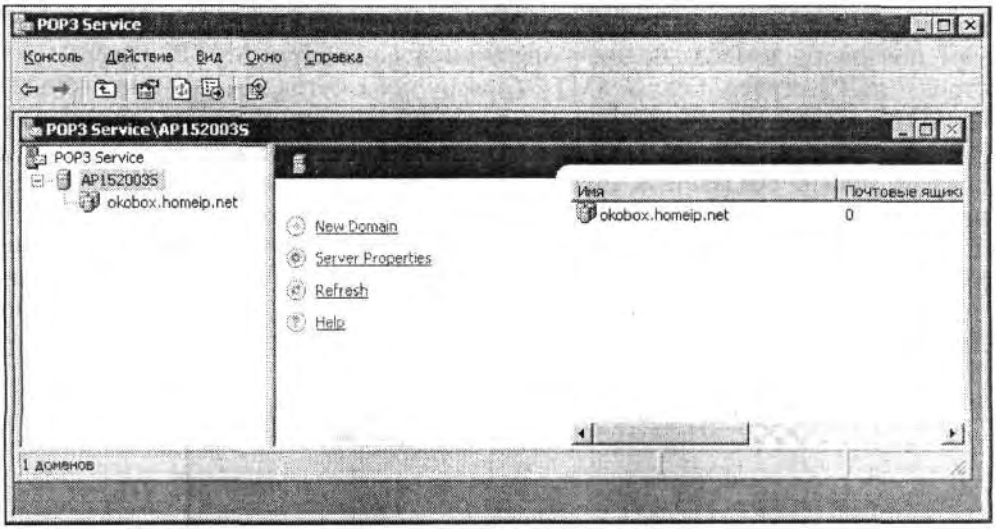


Рис. 7.16. Окно **POP3 Service**

Для настройки порта SMTP-сервера откройте из окна **Internet Information Services (IIS) Manager** (рис. 7.15) окно свойств виртуального SMTP-сервера (из контекстного меню), а в этом окне выберите вкладку **Доставка**. В нижней части вкладки есть кнопки **Подключения** и **Дополнительно**. Нажав кнопку **Подключения**, вы откроете окно **Исходящие подключения** (рис. 7.17).

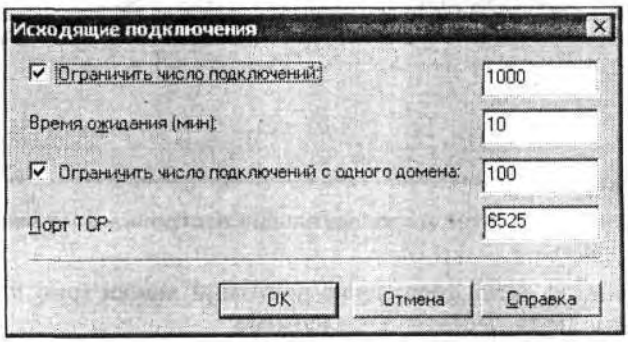


Рис. 7.17. Окно **Исходящие подключения**

В данном окне при необходимости можно изменить значение порта для этого сервера. В примере стандартный порт 25 заменен значением 6525.

Нажав кнопку **Дополнительно**, вы откроете окно **Дополнительная настройка доставки** (рис. 7.18), в котором можно указать **Имя подменяющего домена**,

предназначенное для замены имени компьютера зарегистрированным именем почтового домена. Внеся изменения в параметры SMTP-сервера, настроим POP3-сервер. Если к SMTP-серверу пока метод доступа анонимный, то POP3-сервер мы настроили для проверки подлинности по локальным учетным записям Windows. Значит, для каждого пользователя почтового сервера должна создаваться учетная запись на этом компьютере. К счастью, данный процесс автоматизирован, и учетная запись может создаваться вместе с почтовым ящиком. Для создания почтового ящика достаточно в окне **POP3 Service (POP3 Service\ AP152003S)** (см. рис. 7.16) выделить значок почтового домена в левой части окна, а в правой выбрать пункт меню **Add Mailbox** (Добавить почтовый ящик).

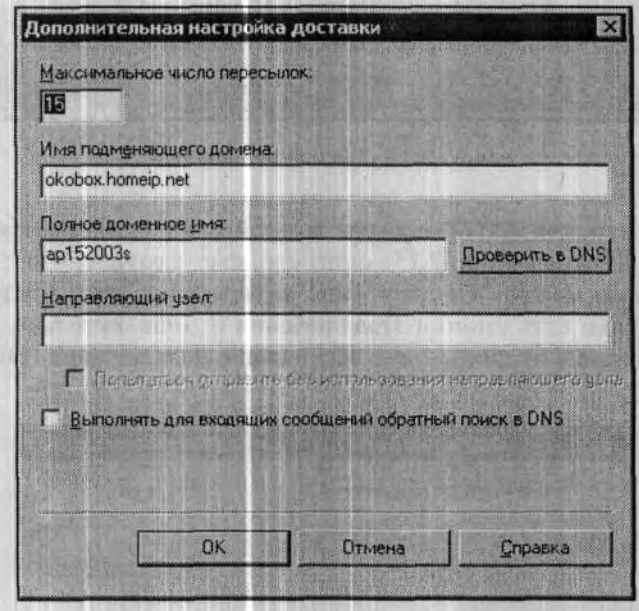


Рис. 7.18. Окно **Дополнительная настройка доставки**

При этом откроется окно **Добавление почтового ящика** (рис. 7.19). Внесите в соответствующие поля необходимые данные.

Все. Почтовый ящик для учетной записи braginsky создан. Остается совсем немного. Следует открыть порт 110 для доступа к почтовому серверу из Интернета или из первой сети.

Для этого в окне **Routing and Remote Access** (см. рис. 7.11) откройте окно свойств общего интерфейса и на вкладке **Службы и порты** (рис. 7.20) отметьте **Протокол Post-Office Protocol, версия 3 (POP3)** и укажите IP-адрес сервера, когда соответствующее поле станет доступно.

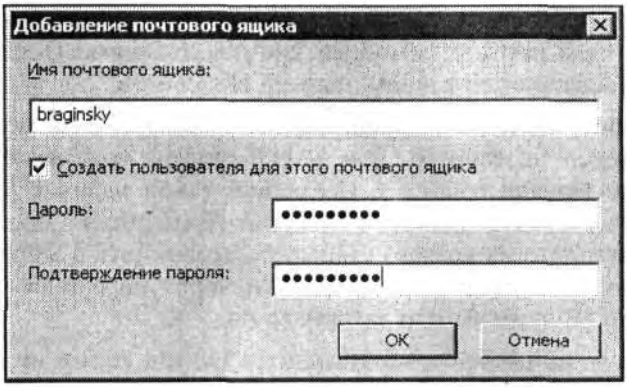


Рис. 7.19. Окно **Добавление почтового ящика**

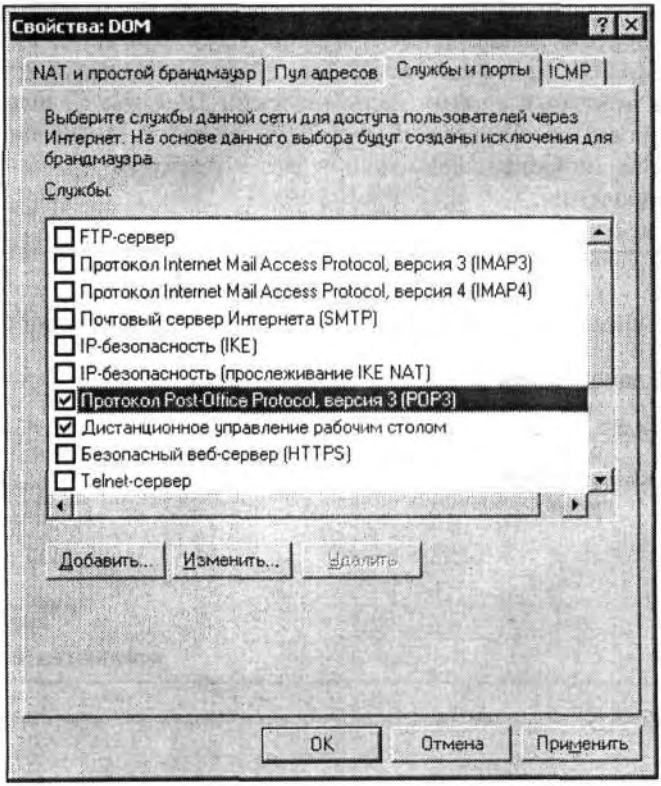


Рис. 7.20. Окно **Свойства: DOM**
(свойства интерфейса подключения к интернету)

Для доступа к SMTP-серверу придется создать новую службу SMTP с измененным значением порта с помощью кнопки **Добавить**. После выполнения этих действий сервер станет доступным из Интернета.

Настраивая работу почтовых служб, обратите внимание на способ авторизации пользователей на сервере. Для SMTP-сервера есть возможность работать анонимно. Но для работы в Интернете такой вариант не годится. Вы сразу почувствуете, что вашим сервером пользуются. Доступ к SMTP-серверам в Интернете их хозяева стараются ограничить с целью недопустить массовые несанкционированные рассылки через него (спам). Используют ограничения по IP-адресам или авторизацию.

В рассмотренном примере сервер находится внутри сети и не имеет прямого выхода в Интернет. Почтовый сервер в таком случае будет действовать только в пределах локальной сети, для которой он настроен. Для работы сервера в Интернете, для обеспечения возможности обмена почтовыми сообщениями с пользователями Интернета необходимо, чтобы внешний интерфейс сервера был действительно внешним (рис. 7.21). Кроме того, подключение через Стрим (ADSL для физических лиц в Москве) затрудняет полноценно использовать почтовый сервер. Динамический IP-адрес невозможно прописать в маршрутизаторе Windows Server 2003. Доступ в Интернет для компьютеров сети, тем не менее, возможен в рассмотренном примере при любом способе подключения.



Рис. 7.21. Вариант подключения сети к Интернету через сервер

Управление почтовым сервером

SMTP-сервер обычно не требует специального управления. Все пользователи почтового сервера могут использовать SMTP-сервер для отправки сооб-

щений. Другое дело POP3-сервер. Он используется для получения почты, а значит должен знать своих клиентов. Как создавать почтовые ящики в локальном интерфейсе сервера, мы уже рассмотрели. Но у Windows Server 2003 есть и Web-интерфейс для управления почтовым сервером. Проверьте компоненты E-mail Services (рис. 7.22), которые установлены в вашей системе. Если не установлен компонент **POP3 Service Web Administration**, то доустановите его.

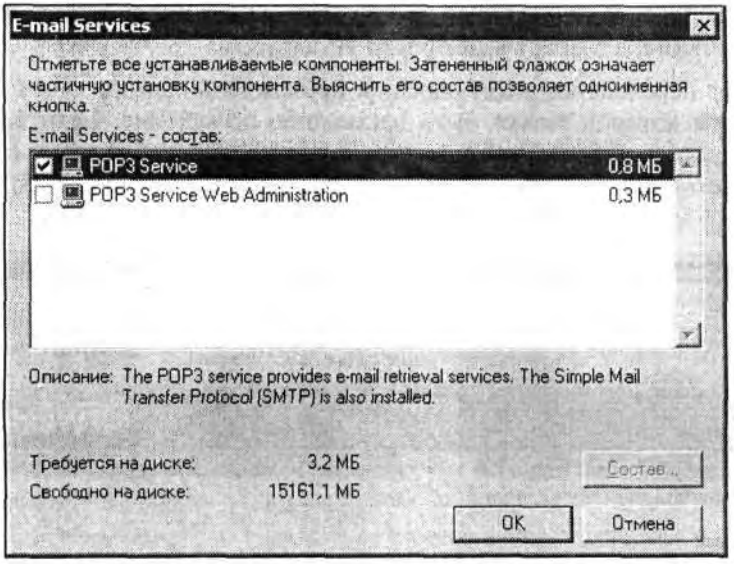


Рис. 7.22. *Окно* **E-mail Services**

После установки этого компонента вы получите возможность управлять почтовым сервером из Интернета через Web-интерфейс. Управление сервером таким способом несколько удобнее, чем через локальный интерфейс. Поэтому на своих серверах мы часто используем Web-интерфейс даже при локальной работе с сервером. Через этот интерфейс вы можете получить доступ к управлению не только программным почтовым сервером, но и по многим параметрам сервера в целом. Это один из способов удаленного администрирования сервера, причем хорошо защищенный.

Web-интерфейс

К сожалению, Web-интерфейс почтового сервера не имеет локализованного варианта. Даже в русской версии Windows Server 2003 он выполнен на английском языке. Тем не менее, после предварительного знакомства с этим инструментом он становится абсолютно понятным и удобным.

Web-интерфейс управления сервером — это Web-сайт на вашем сервере. Для того чтобы вы имели возможность поместить на сервер и свой собственный сайт, доступ к интерфейсу управления организован по специально выделенному для этого порту. Набирая в браузере адрес своего сервера без указания номера порта, вы сможете подключаться к Web-сервисам, работающим на порте номер 80. Для управления сервером следует после адреса указать порт 8098, а протокол HTTP изменить на HTTPS. Пример адреса для подключения к интерфейсу управления сервером: **https://www.myserver.ru:8098**. Адрес, конечно, должен быть вашим, причем он может быть и внутренним (из имени компьютера в сети) или просто IP-адресом.

Сразу после перехода по этому адресу и прохождения авторизации вы увидите страницу, на которой может быть какое-либо сообщение. Если все работает нормально, то сообщений обычно нет, и можно выбрать вкладку с необходимыми средствами управления. Например, вкладку **E-mail** (рис. 7.23).

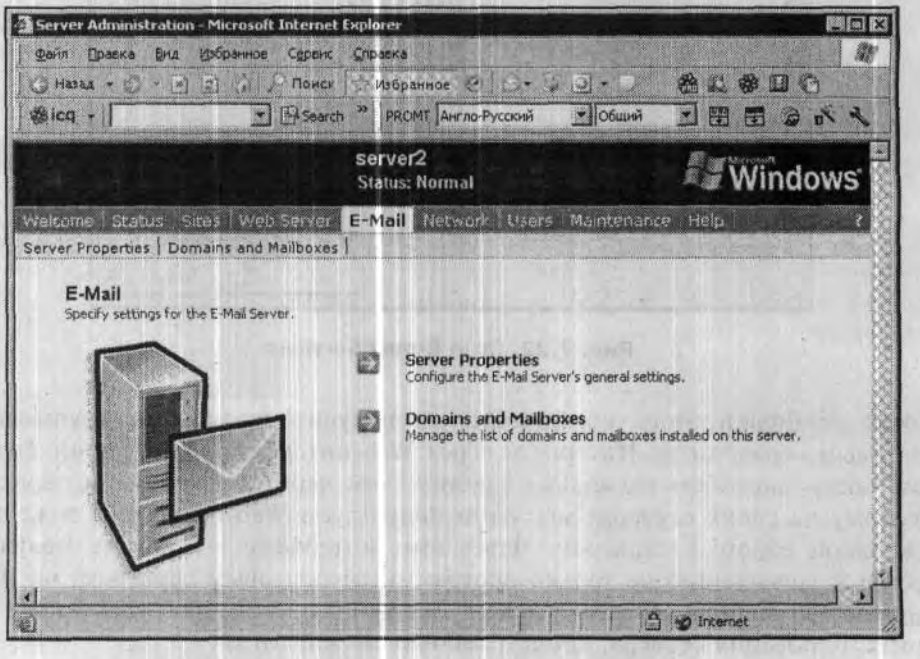


Рис. 7.23. Окно **Server Administration - Microsoft Internet Exporer**, вкладка **E-Mail**

На этой вкладке доступны два пункта меню. **Server Proprties** — свойства сервера и **Domains and Mailboxes** — домены и почтовые ящики. В большинстве случаев их достаточно для повседневного администрирования почтового сервера. Выберем **Server Proprties** (рис. 7.24).

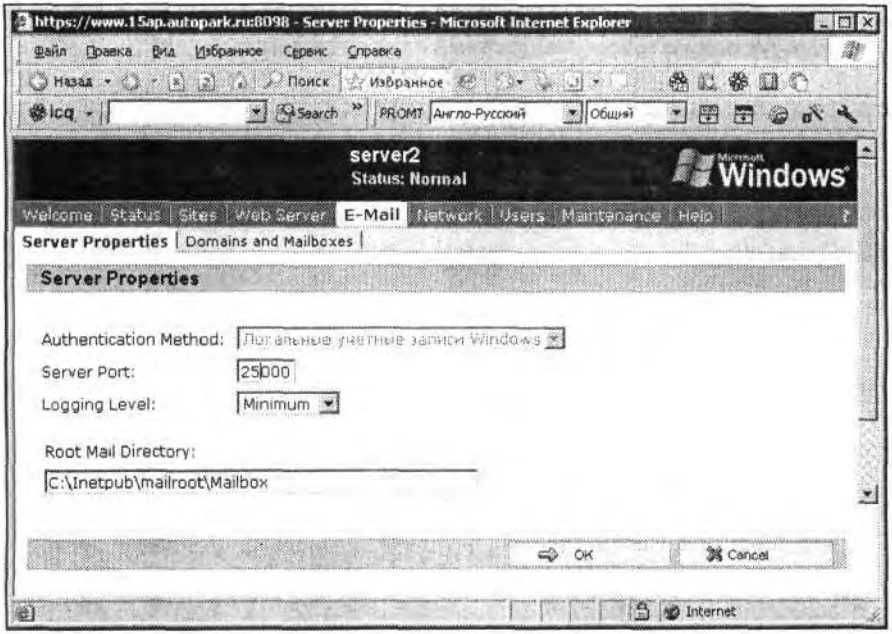


Рис. 7.24. Вкладка **Server Properties**

На открывшейся странице мы имеем возможность изменить каталог, содержащий почтовые ящики, изменить уровень протоколирования событий сервера и поменять порт, используемый сервером POP3. Изменив порт относительно стандартного значения, мы повысим защищенность сервера, поскольку только посвященные пользователи будут его знать. Кроме того, мы получаем возможность применения в той же сети и даже на том же сервере еще одного почтового сервера. Зачем это нужно? Таких ситуаций может быть много. Это и различные серверы для внешней и внутренней почты, и серверы управления, позволяющие передавать в виде почтовых сообщений команды управления сервером сети. Само собой, подобный сервер должен быть лучше защищен, чем обычный почтовый. Адреса и учетные записи такого сервера не должны быть доступны всем пользователям сети. Необходимость во втором почтовом сервере может никогда не возникнуть у многих пользователей и администраторов сети, но когда она возникнет, мы можем беспрепятственно устанавливать его, не опасаясь, что возникнет конфликт с уже существующим почтовым сервером.

Примечание

Работая с несколькими почтовыми серверами, расположенными на одном компьютере, следует помнить, что два POP3-сервера должны иметь различные значения портов. Нельзя установить два сервера, применив для их работы

стандартные порты. В то же время два SMTP-сервера могут сосуществовать, используя один и тот же стандартный или нестандартный порт.

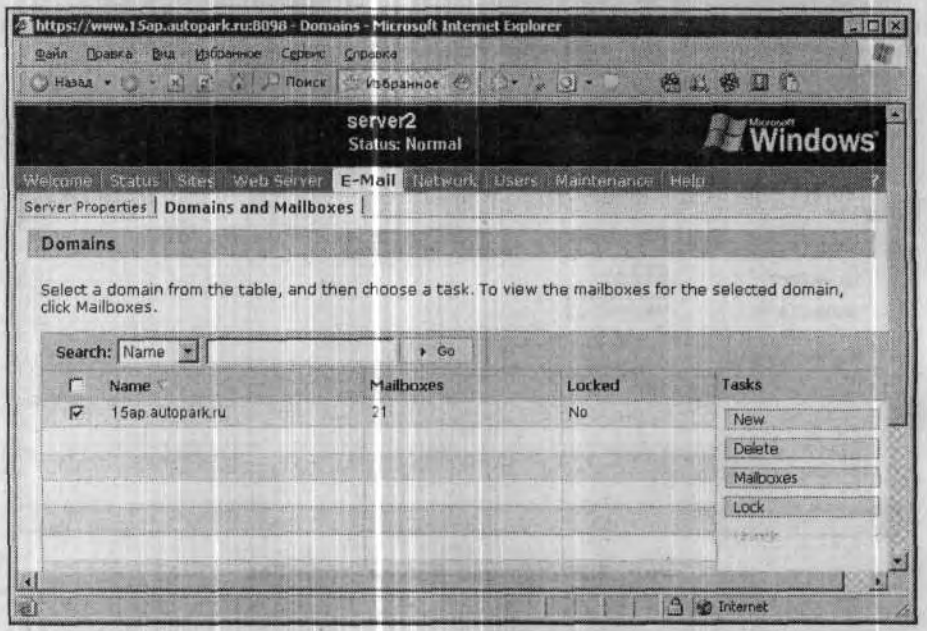


Рис. 7.25. Вкладка **Domains and Mailboxes**

На вкладке **Domains and Mailboxes** (рис. 7.25) мы можем получить доступ к созданию или удалению и блокированию почтовых доменов, а также можем перейти на страницу управления самими почтовыми ящиками. Интерфейс этих страниц настолько понятен, что нет смысла подробно его рассматривать. Кроме управления доменами и почтовыми ящиками через Web-интерфейс мы можем получить доступ к управлению локальными учетными записями пользователей сервера, перейдя на вкладку **Users | Local Users on Server** — Пользователи | Локальные пользователи сервера (рис. 7.26).

Здесь мы можем создавать, удалять и модифицировать учетные записи. Если сервер работает только как почтовый сервер, то этот интерфейс обеспечивает доступ ко всем необходимым свойствам учетных записей пользователей почты. Но не только учетными записями пользователей почты можно управлять с этой вкладки. Вы можете создавать учетные записи, наделяя их любыми правами, или предоставлять и ограничивать права для существующих учетных записей.

Кроме управления почтовым сервером, Web-интерфейс позволяет управлять и Web-серверами с вкладки **Sites | Web Site Configuration** — Сайты | Конфигурация Web-сайтов (рис. 7.27).

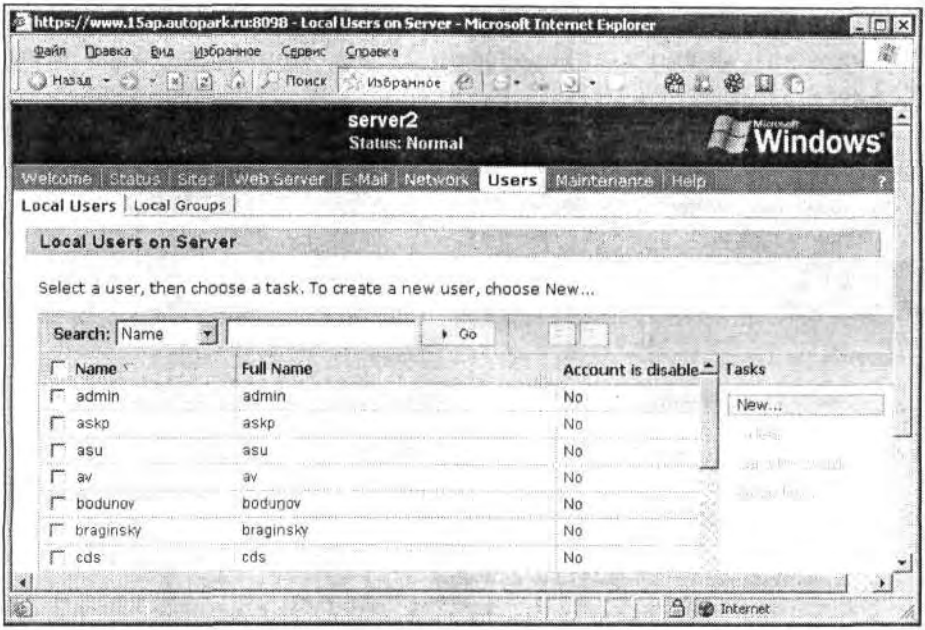


Рис. 7.26. Вкладка **Local Users on Server**

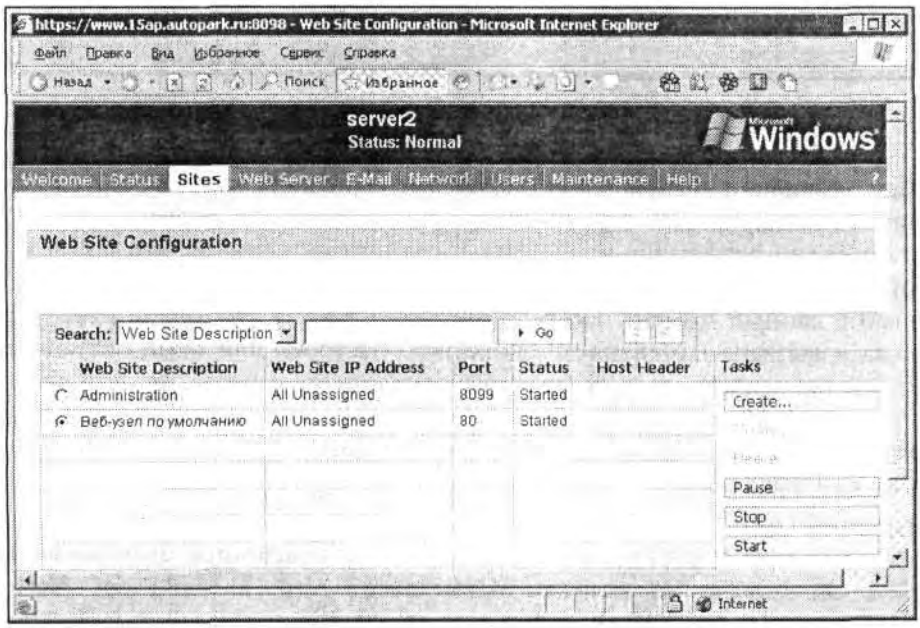


Рис. 7.27. Вкладка **Web Site Configuration**

А с вкладки **Date/Time | Date and Time Setting** (Дата и время | Установка даты и времени) можно контролировать работу системных часов сервера (рис. 7.28).

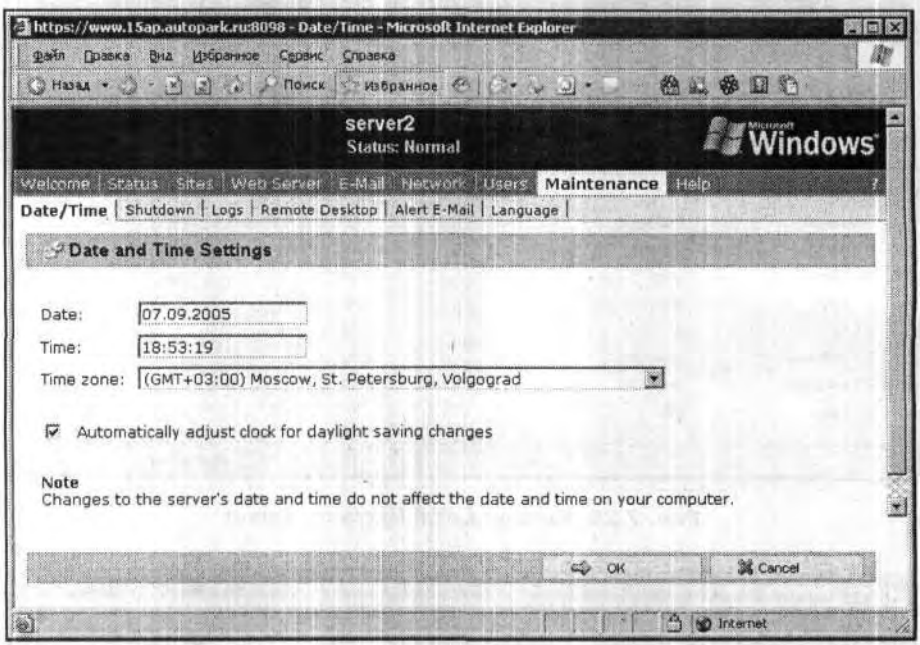


Рис. 7.28. Вкладка **Date and Time Setting**

Вкладка **Shutdown** (Выключение) позволяет выполнять перезагрузку, выключение и планирование выключения или перезагрузки сервера (рис. 7.29). Эти операции достаточно рискованны, если вы не уверены, что после перезагрузки работа сервера восстановится, а выключение действительно необходимо в данный момент. Но если вы точно знаете, что перезагрузка необходима и вызвана изменением каких-либо настроек или иной ситуацией, а сами вы находитесь на значительном удалении от сервера, то этот инструмент очень удобен. Кроме собственно перезагрузки и выключения, вы можете назначить сообщения, которые сервер будет отсылать вам при перезагрузке или выключении.

Установить связь сообщений с различными типами событий, указать адрес для их отправки и SMTP-сервер, которым необходимо при этом воспользоваться, вы можете на вкладке **Maintenance | Alert E-Mail | Set Alert E-Mail** (Обслуживание | Предупреждения по электронной почте | Настройка предупреждений по электронной почте).

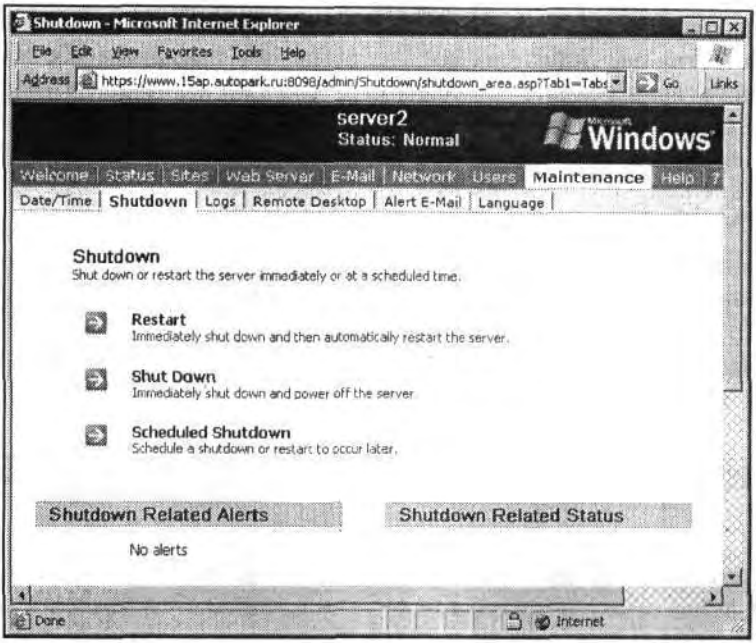


Рис. 7.29. Вкладка **Shutdown**

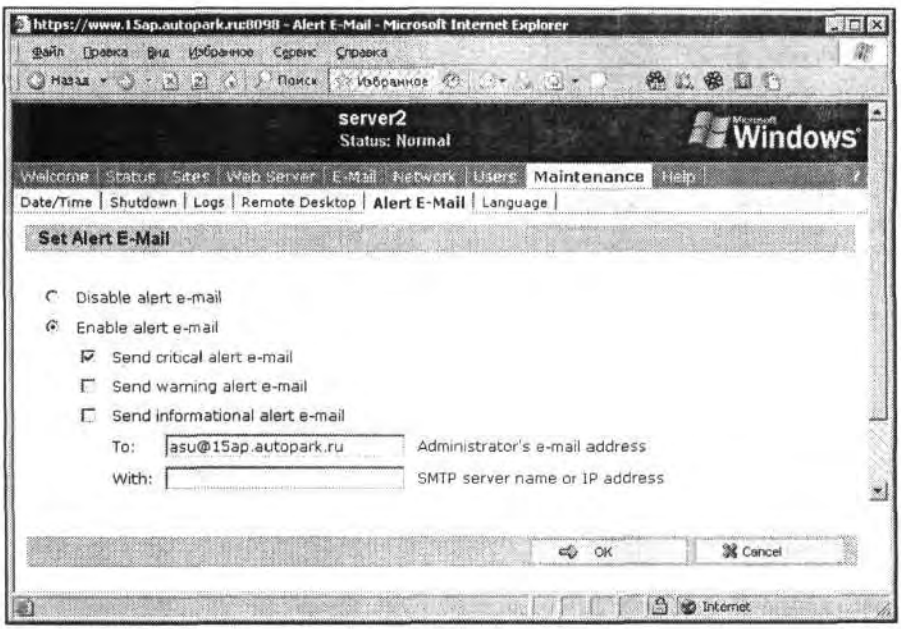


Рис. 7.30. Вкладка **Set Alert E-Mail**

Рассмотрите самостоятельно остальные возможности этого интерфейса. Вероятно, именно вас заинтересуют и другие его функции. Их достаточно, чтобы иметь возможность в удаленном режиме выполнять необходимые операции на почтовом сервере. Если вы сталкивались ранее со средствами управления маршрутизаторами и другими сетевыми устройствами по HTTP-протоколу, и вам нравился такой метод управления этими устройствами, то Web-интерфейс управления сервером вам обязательно понравится.

В заключение описания Web-интерфейса для управления сервером посмотрим еще на одну вкладку **Take Tour | Server Identity** (Начальные настройки | Идентификация сервера) (рис. 7.31). Из этого окна вы можете переименовать сервер, изменения его принадлежности к тому или иному домену либо рабочей группе.

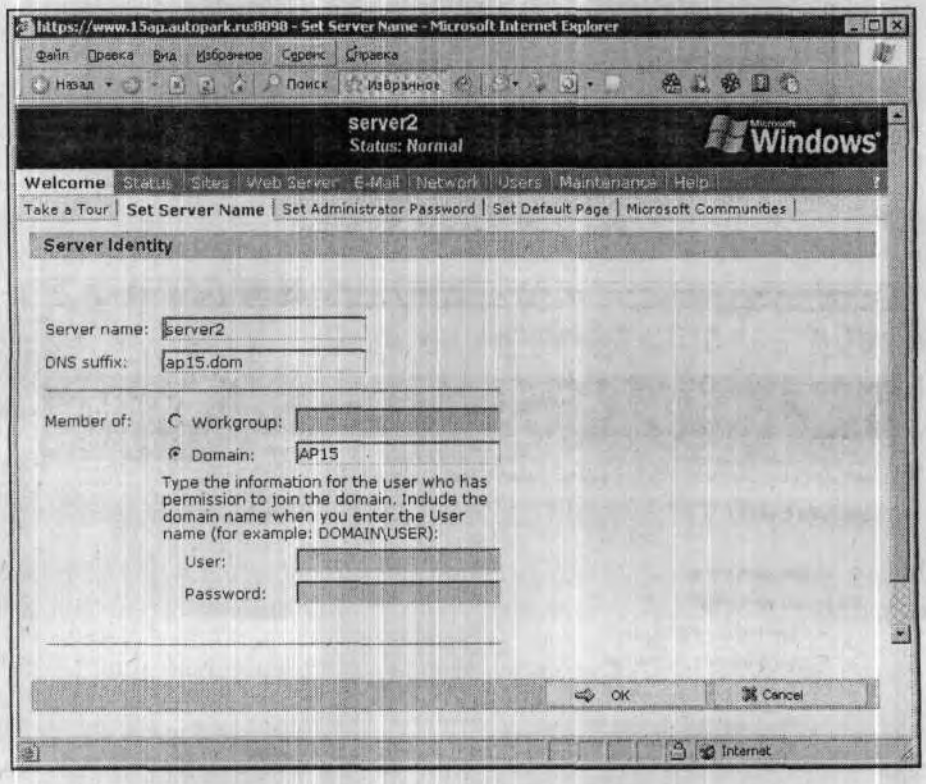


Рис. 7.31. Вкладка **Server Identity**

Таким образом, в ваших руках мощнейшее средство для управления сервером, применяя которое, необходимо соблюдать осторожность и не пытаться

экспериментировать, если вы находитесь на значительном удалении от сервера и не сможете исправить ошибку при потере связи с сервером.

Для тех, кто только что начал знакомство с Windows Server 2003, Web-интерфейс может показаться некоторым излишеством. Но со временем вы им начнете пользоваться достаточно активно, чтобы ощутить его необходимость в работе администратора сети.

Если вы решили, что будете использовать почтовый сервер в вашей сети, имеющей полноценный (с постоянным IP-адресом) выход в Интернет, то следует установить еще некоторые средства на нашем сервере.

В следующей главе мы поговорим о серверах DNS, DHCP, WINS. А сейчас есть смысл продолжить разговор.

О неисправностях

Рассмотрим наиболее типичные проблемы, которые могут возникнуть при эксплуатации сервера, подключенного к Интернету и содержащего почтовый сервер. Решение этих проблем предполагает предварительный анализ ситуации, и лишь после выявления предполагаемой причины проведение работ по настройке сервера. Попытки решить проблему методом "научного тыка" могут привести к еще более серьезной и запутанной ситуации.

Не работает подключение к Интернету с компьютеров сети

Эта ситуация встречается довольно часто. Она может быть вызвана причинами, которые собственно к серверу не имеют никакого отношения. Поэтому решение проблемы следует начинать с проверки — работает ли подключение к Интернету на других компьютерах сети.

Если на других компьютерах сети тоже нет подключения к Интернету, но все только что работало, — не торопитесь изменять какие бы то ни было настройки. На всех уровнях сети Интернет работают компьютеры и люди. Всегда есть вероятность сбоев. Следует подождать несколько минут, проверить связь с модемом или маршрутизатором. Если, например, связь с глобальной сетью осуществляется ADSL-модемом с Ethernet-портом на стороне вашей сети, то должен проходить `ping` до внешнего IP-адреса модема (в нем встроен маршрутизатор). При подключении вам должны были выдать адреса подсети, в которой работает маршрутизатор модема. По крайней мере, один адрес принадлежит самому модему. Если `ping` по этому адресу проходит нормально, то, скорее всего, на вашей стороне все исправно. При длительном перерыве связи с Интернетом позвоните в службу поддержки.

Если с других компьютеров сети связь есть, а с одной рабочей станции нет, то следует проверить, прежде всего, подключение к локальной сети, работоспособность сетевого адаптера, правильность настроек сетевого подключения, а также настроек подключения применяемого браузера. Возможно, что на данном компьютере применяется не одно подключение к Интернету (особенно вероятно на ноутбуках). Вполне вероятно, что пользователь не изменил вид подключения к Интернету, начав работу в локальной сети.

Если проверка доступности внешнего IP-адреса маршрутизатора дала отрицательный результат, то попробуйте перезагрузить модем (маршрутизатор). Если вы сами имеете доступ к настройкам ADSL-модема, то убедитесь, что вы их не изменяли и они корректны.

Если вы проводили изменение настроек на сервере, к которому подключен ADSL-модем, то придется вернуть настройки в исходное состояние. Для того чтобы это было возможно, документируйте каждый шаг новых настроек — что было, как изменилось. Подключение должно восстановиться. Затем пошагово повторите требуемые настройки, проверяя на каждом шаге наличие подключения. Таким образом вы обнаружите ошибочные действия и сможете изменить их.

Не удается принять или отправить почту с внешнего почтового сервера

Прежде всего, проверьте подключение к Интернету. Если все нормально, то возможно произошел временный сбой на внешнем сервере. Это достаточно часто случается на бесплатных почтовых серверах. Но такие сбои непродолжительны. Если не удается отправить или принять почту только с одной рабочей станции, то вероятнее всего нарушены настройки почтового клиента. Чаще всего это происходит при замене почтового клиента пользователем. На почтовом сервере авторизация для POP3- и SMPT-сервера может настраиваться раздельно, и пользователи могут ошибиться при повторении настроек почтового клиента.

Не удается принять или отправить почту с почтового сервера своей сети

На почтовом сервере Windows Server 2003 авторизация для POP3- и SMPT-сервера обычно настраивается раздельно, и пользователи могут ошибиться при повторении настроек почтового клиента, если делают это самостоятельно. Возможно, настройки вашего сервера не позволяют отправлять и принимать почту большого объема или превышено число отправляемых сообщений за один сеанс. Внимательно просмотрите настройки серверов SMTP и POP3. Это два самостоятельных сервера. Каждый из них настраивается

отдельно и имеет независимые от другого сервера параметры. Если ваш сервер не смог отправлять или принимать почту сразу после настройки, то очень вероятно, что вы выбрали слишком жесткие или даже несовместимые с возможностями почтового клиента условия авторизации. Попробуйте начать с самых простых настроек с Windows-проверкой подлинности. При этом наличие учетной записи пользователя, входящего в группу пользователей POP3, должно обеспечить работу с почтой. Более высокий уровень контроля подлинности пользователя следует устанавливать осторожно, проверяя возможности почтового клиента. Особенно это касается требований шифрования паролей.

Для всех вариантов работы с почтой требуется поддержка со стороны внешних или ваших внутренних серверов DNS. Проблемы на этих серверах также могут быть причиной проблем при работе с почтой. Если вы пользуетесь внешним DNS-сервером и он всего один (не указан резервный), попробуйте добавить адрес второго DNS-сервера в настройки подключения к Интернету. Имея свой собственный DNS-сервер, также следует использовать и какой-либо внешний.

Работа DNS-сервера будет рассмотрена в следующей главе.

А сейчас случай из жизни. Может быть, и вы найдете в нем для себя полезную информацию.

Москва? Петербург на проводе! HELP ME!

Почти все имена, адреса и личные сведения вымышлены.

Современные средства связи позволяют сократить расстояния, исчисляемые сотнями и тысячами километров, до нескольких сантиметров. Один из моих знакомых начинающих сисадминов проживает в Петербурге. До этого славного города не тысячи километров от меня, но это не имеет значения. При наличии ICQ и сервера терминалов Admin (далее собеседников будем обозначать "никами" из "Аськи", мой "ник" — Beard) мог бы находиться даже в Африке, и при этом ничего в данной ситуации не изменилось бы.

В один из сеансов связи по "Аське" Admin радостно сообщил, что у него появился сервер Windows Server 2003. Он решил применить этот сервер для организации подключения локальной сети к Интернету. Благо, кроме сервера у него установили ADSL-модем и оставили записку с парой IP-адресов. У тех, кто имеет лишь аналоговый модем для связи с внешним миром, вероятно, уже потекли слюнки — повезло же Admin'у! Но для нашего Admin'а ADSL-модем был не совсем понятным устройством.

Проблема оказалась и в том, что Admin только начал осваивать премудрости устройства сети. "Зубры", которые раньше настраивали эту сеть и поддержи-

вали ее здоровье, ушли на более доходное место. Нет крепкого плеча рядом, а сеть живет, требует к себе внимания, растет...

Вот и канал в Интернет появился, но как его использовать?

Мир не без добрых людей (немного не скромно, но это я о себе). Мы договорились, что, как только я освобожусь, то помогу с настройкой подключения дистанционно. И вот нашлось время для первого достаточно продолжительного сеанса связи.

Ввиду обоюдного дефицита времени настройки пришлось делать в два этапа, их "шлифовку" Admin'у предстоит выполнить самостоятельно, но самое основное было сделано во время этих двух сеансов связи.

Первое включение

Здесь опущены приветствия и разнообразные вводные фразы. Сразу переходим к основной части сеанса связи.

Beard:

Если есть конкретный вопрос — задавай.

Если много вопросов, то лучше по почте. Вечером спокойно отвечу.

Admin:

Насчет вопросов очень сложно. Я ж сервер поставил, который хочу подключить к интернет-каналу. А кабель от второй сетевой платы на сервере надо непосредственно в устройство втыкать или в маршрутизатор?

Beard:

Если сказали, что обычный компьютер можно включать в это устройство, то в него. Маршрутизация настраивается на сервере, а сеть через вторую карточку.

Admin:

Ну, это устройство выглядит как ADSL-модем...

Beard:

Вход Ethernet?

Admin:

Да.

Beard:

Тогда все так, как сказано раньше.

Admin:

Сервер я ввел в свой домен, теперь дело за маршрутизацией?

Beard:

Тот IP, что тебе передали, будет у карточки, подключенной к устройству.

Второй карточкой включаемся в свою сеть. Настраиваем NAT — можно мастером для начала. Шлюзом для пользователей становится внутренний адрес сервера. Для тех, кто по другому каналу, старые настройки.

Admin:

Причем ISA и NAT не будут конфликтовать?

Beard:

Для ISA требуется указывать шлюз у пользователя.

У меня сейчас в системе три шлюза, использовать их можно только по одному, но в сети конфликтов не будет.

Admin:

Вообще-то для ISA указывается тот сервер, где он стоит.

Я сейчас запустил сервер.... Попытаюсь маршрутизацию сделать.

Beard:

Значит, для ADSL тот сервер, где ADSL. Если надо и то и другое, то можно шлюз переключать. Можно "батником":

---

netsh int ip reset "C:\resetip.txt"

netsh int ip add address "LocalNet" gateway=192.168.0.X gwmetric=2

Admin:

Мне дали два IP, шлюз, MAC, и два DNS.

Beard:

Два IP — это для самого сервера и для маршрутизатора, который вместе с модемом ADSL. MAC на всякий случай (от ADSL, наверное), DNS — как обычно от провайдера.

Примечание

В предыдущем сообщении я не рассмотрел слова шлюз, что привело к некоторому увеличению времени на разбор ситуации. Но и Admin мог бы сразу указать параметры подключения, предложенные ему. В этом случае недопонимание с моей стороны было бы исключено.

Admin:

Пошел мастер. Выбрать ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ? NAT?

Beard:

Да.

Admin:

Или доступ через VPN и NAT?

Beard:

Давай NAT. Позднее проверим результат. Его можно корректировать вручную.

Admin:

Хорошо. Теперь я на пункте ОБЩИЕ. Настроить конфигурацию той сетевой карты, что смотрит на устройство?

Стоит IP-адрес получить автоматически? Разумеется, надо ставить тот IP, что дал провайдер.

Beard:

В свойствах подключения надо установить параметры, которые тебе дали. Шлюз — один из тех IP (скорее всего меньший). Еще должны были маску дать.

Admin:

Маска есть. Поставил. Границы многоадресной области?

Что за пульс многоадресной области?

Beard:

Оставь пустым.

Admin:

Все. Сделано вроде все? А куда "пихать" DNS-адреса?

Beard:

В свойства подключения (внешнего), как при обычной настройке карточки. Сам сервер должен иметь возможность выхода в Интернет после настройки внешнего подключения

Admin:

Все.... И как проверить? "Пингануть"?

Beard:

Набери в адресе безопасное что-нибудь, www.google.ru, например.

Admin:

Мда, а что писать в параметрах настройки обозревателя?

Beard:

По сети, и никаких настроек.

Admin:

Ни автоматических, ни прокси не приписывать???

Beard:

Нет

Admin:

Грузится... Поехала машинка.

Но очень медленно...

Beard:

Это только начало.

Admin:

Притом, если "пинганути". То 119 мс.

У меня сервер все-таки через switch 5 портовый подключен с сетке... Может в этом причина?

Beard:

Сейчас главное, что работает в принципе. Остальное зависит от тарифа, скорости, качества линии и т. д. Можно будет с их инженерами поговорить.

Сервер подключен через коммутатор с внутренней карточки, а настраиваем внешнюю.

Надо проверить настройки NAT и поправить их.

Admin:

Оба кабеля воткнуты в switch.

Beard:

Убрать!

Внешняя должна быть сама по себе, только в ADSL!

Admin:

Уберу... Я сервер выключу.

Beard:

До встречи.

Второе включение

Admin:

Сервер уже подключен. К устройству. Маршрутизация тоже... Теперь настроить надо что-то? NAT?

Beard:

Да, надо проверить его работу. Если на клиенте поставить шлюз — адрес сервера (внутренний), то должен быть Интернет. Если нет, то проверить настройки. Посмотри. Скажешь, если не работает.

Admin:

Ерунда получается.... Кстати, с какого IP я с тобой соединяюсь? И жутко медленно все грузится...

Включил команду `tracert`, везде пишет... превышен интервал ожидания для запроса...

Beard:

Какие у тебя выданы IP?

Admin:

Два постоянных.

Beard:

Какие?

Если скрываешь, то у компьютера (сервера) должен быть больший, а у модема — меньший. Обычно так. На внешней карте в качестве шлюза — меньший из выданных провайдером адресов. Для внутренних компьютеров в качестве шлюза — внутренний адрес сервера, через который подключаем Интернет.

В маршрутизации и удаленном доступе (через администрирование) надо посмотреть правильно ли поставлены роли адаптеров.

Admin:

Да не скрываю. Дали два IP 222.333.444.130 и 222.333.444.134... Для внешнего использовал 222.333.444.130.

Заработала... Но все равно что-то очень медленно...

Beard:

У тебя ADSL?

Обычно дают четыре адреса из сети 255.255.255.252.

Два крайних не используются, два средних — модему и серверу.

У тебя сейчас сам сервер выходит в Интернет через ADSL?

Если да, то посмотри адрес внешнего адаптера и его шлюз (какие установлены). Может быть, тебе давали и другие параметры? Маску, например.

Admin:

Маска есть. Если хочешь, можешь зайти на сервер. Сейчас организую доступ.

Beard:

У меня нет `ping` на твой модем. Обычно они "пингуются" без проблем.

Дашь доступ, посмотрю настройки сам.

Есть `ping` на 129. Может быть это модем?

Admin:

XyYxXy.

12ZzWw3.

IP 222.333.444.130.

Ну как?

Beard:

Пока не удалось подключиться. Или закрыты порты или...

У него по мастеру установлен брандмауэр. Он не пустит. Попробуй на время отключить его. Это в администрировании, маршрутизация и удаленный доступ.

IP-маршрутизация, NAT, простой брандмауер, интерфейс тот, что в Интернет смотрит в свойствах.

Примечание

Вообще говоря, это не лучшее решение. Лучше открыть только необходимые порты. Но для объяснения того, как открыть порт для терминального сервера, времени потребовалось бы намного больше.

Admin:

Отключил.... Но NAT оставил.

Beard:

Сейчас, вхожу...

Пароль или имя.

Не идет.

Admin:

Сейчас проверю. Но окно терминала выскочило?

Beard:

Да.

Admin:

XyYxXy.

12ZzWw3.

... Понял. Я ж не включил его на этом сервере! Сейчас.

Включил.

Beard:

Не пускает.

XyYxXy.

12ZzWw3.

Домен BALTIC.

Это локальный администратор?

Он должен быть в группе администраторов обязательно.

Admin:

Может, я пароль неправильно набил. Сейчас проверяю.

Мда... что-то не могу найти локальных администраторов... на этом сервере...

Beard:

Через управление компьютером... пользователи. Находим этого, а в его свойствах добавляем группу администраторов.

Если локальные пользователи запрещены, то сервер уже контроллер домена. Тогда данному пользователю (он сетевой) даем права на администрирование, вводим его в группу локальных администраторов или администраторов этого домена.

Admin:

Попробуй другой.

admin.

trXXXX22.

Открылся...

Beard:

Вошел.

Значит, как я и предположил, модем 129.

На клиентах ставим шлюз 192.168.0.6.

DNS 222.333.55.33, как второй или третий.

IP на клиенте поставь пока свободный и фиксированный.

Admin:

В смысле? Пустой?

Beard:

Нет. 192.168.0.X, который свободен в сети.

Admin:

Я ставил тот, под которым сам клиент.

Beard:

Ну и...

DHCP с этого сервера лучше снести, если работает на другом. Должен быть один на сеть.

Могу и сам снести... если согласен.

Admin:

Сноси. Только как?

Beard:

Через управление данным сервером.

Начинаю.

Вставьте SP1 CD-ROM в устройство N.

Если дистрибутив есть на самом сервере, то найду. Только скажи.

?

Admin:

Да я бегал. Диск вставлял. В устройство N.

Beard:

Копирование файлов.

Роль DHCP удалена.

Проверяй с клиента.

Вижу попытку с 192.168.0.65.

Admin:

Да это я соединяюсь....

Ну что там с сервером?

Beard:

А что с клиентом? Я жду пробы и результатов.

Admin:

Ааа... да все нормально уже... Пока, правда, не ясно — как скорость, но не тормозит по крайней мере.

Beard:

У тебя должны быть 130.131.132.134.

Это адреса, которые могут иметь серверы снаружи.

Пока использован один, и работает. Остальные в резерве.

Могу выходить из терминала?

Или, пока подключен, еще вопросы есть?

Admin:

Да нет. Я умнею уже. Пока все понятно. Эх, нет пока у меня практики.

Beard:

У тебя на этом сервере DNS установлен. Есть смысл почитать про эти серверы и настроить. Но для начала хорошо бы имя в Интернете получить, хотя бы третьего уровня.

Выхожу.

Admin:

Собираюсь.... У нас страничку надо завести. Но я для этого использую хостинг.

Beard:

Вышел. Закрывай брандмауэр.

Admin:

Уже давно закрыл. Кстати. А сервер не открыт снаружи?

Beard:

Если давно закрыл, то соединение поддерживалось до разрыва. Теперь не включится.

`PING` уже не идет, значит и все остальное закрылось.

Завершаем на сегодня?

Admin:

Конечно. Спасибо. С меня магарыч.

Несмотря на некоторые издержки оперативного общения при недостатке времени, проблема решилась. И произошло это значительно быстрее, чем могло бы, пригласи Admin знакомого из соседнего дома — идти было бы дольше. А когда и знакомого такого нет, то удаленная помощь вне конкуренции.

Конечно, кое-что надо уметь даже для получения помощи. Если бы не удалось предоставить прямой доступ к серверу через терминальное подключение, то разговор мог бы тянуться не один день. А дополнительные проблемы, вроде второго DHCP, и недопонимание при переписке могли завести работу в тупик. Но "история не терпит сослагательного наклонения", а желаемый результат достигнут.



Глава 8

Сколько у нас серверов?

У нас заработал сервер. Пока он выполняет лишь функции связи. Пользователи почтового сервера регистрируются прямо на нем, а для выхода в Интернет регистрация не требуется. Для нормальной работы сети необходимы еще некоторые сервисы, которые могут быть предоставлены установленными дополнительно серверами. В данном случае речь идет, конечно, о серверах, реализованных программно. Располагать их можно на одном компьютере, но можно и на разных. Все зависит от ваших возможностей и потребностей. Имея всего один физический сервер (компьютер), можно расположить на нем все программные серверы. Таких программных серверов в одной сети может насчитываться более пяти. Web-сервер, POP3-сервер, SMTP-сервер, DHCP-сервер, WINS-сервер, DNS-сервер, сервер терминалов и др.

DHCP-сервер

До настоящего времени мы должны самостоятельно назначать IP-адреса компьютерам нашей сети. Даже когда была возможность настроить DHCP-сервер на маршрутизаторе, мы этого не делали только потому, что такой сервер должен быть в сети один. Удобнее всего расположить его на сервере сети.

Этот сервер выполняет не очень много функций, но позволяет освободить администратора сети от кропотливого учета IP-адресов, когда число рабочих станций в сети становится достаточно большим, чтобы ходьба от компьютера к компьютеру стала занятием утомительным. Иногда пользователи сети самостоятельно изменяют настройки своих рабочих станций. В этом случае велика вероятность того, что IP-адрес, назначенный пользователем своему компьютеру, совпадет с уже существующим в сети адресом. Тогда работа компьютеров с одинаковыми адресами может быть нарушена. Но вполне возможно автоматическое назначение не только IP-адресов, но и адреса

шлюза в Интернет или в другую сеть. При этом если вы решили изменить способ доступа в Интернет или изменили по какой-либо причине адрес шлюза, или вообще изменили адрес сети, то пользователи не заметят никаких неудобств, а вам не придется перенастраивать рабочие станции. Кроме того, появление новой рабочей станции не потребует выяснения свободного адреса для нее. Исключение или продолжительное отключение рабочей станции на длительный срок позволит использовать освободившийся адрес. Правда, это возможно, если все рабочие станции настроены на автоматическое получение параметров сети.

Итак, DHCP-сервер должен передавать рабочим станциям значения параметров сети. Тем не менее, значения этих параметров определяются администратором сети в соответствии с заранее подготовленным планом IP-адресов. Наверняка отдельные устройства, работающие в сети, а может быть и некоторые рабочие станции потребуют установки статических адресов. Это касается маршрутизаторов, серверов, рабочих станций, которым приходится работать сразу в двух и более сетях. Даже если у вас такой необходимости на данный момент нет, есть смысл оставить некоторый диапазон IP-адресов для назначения статических адресов. Остальные IP-адреса можно раздавать автоматически. Лучше, если эти адреса составляют непрерывный ряд, но если необходимо, то его можно разбить на два и более диапазона.

Рассмотрим конкретный пример настройки DHCP-сервера, который входит в состав ОС Windows Server 2003. Сеть, в которой будем проводить настройку сервера, имеет адрес 192.168.1.0 и маску подсети 255.255.255.0. Автоматически должны присваиваться адреса из двух поддиапазонов: 192.168.1.50—192.168.1.70 и 192.168.1.130—192.168.1.200. Выбор адресов сделан произвольно лишь для иллюстрации возможностей настраиваемого DHCP-сервера. В качестве шлюза в Интернет в сети работает ADSL-модем, с IP-адресом 192.168.1.1. Для DNS-сервера используем 195,34.32.116.

Установка

Для установки DHCP-сервера можно воспользоваться мастером настройки сервера (рис. 8.1) (**Администрирование | Мастер настройки сервера**). Следует добавить очередную роль для нашего сервера. В данном случае это DHCP-сервер.

Отметив соответствующую строку в списке, нажимаем кнопку **Далее**. В процессе установки включается мастер создания области, который создаст область IP-адресов, распределяемых между компьютерами сети.

На этом этапе необходимо задать имя и описание области (рис. 8.2).

В следующем окне (рис. 8.3) необходимо ввести начальный и конечный адреса области, а также маску подсети. Мы решили, что наша область не будет

непрерывной, но на этом этапе задаем начальный адрес 192.168.1.50, а конечный —192.168.1.200.

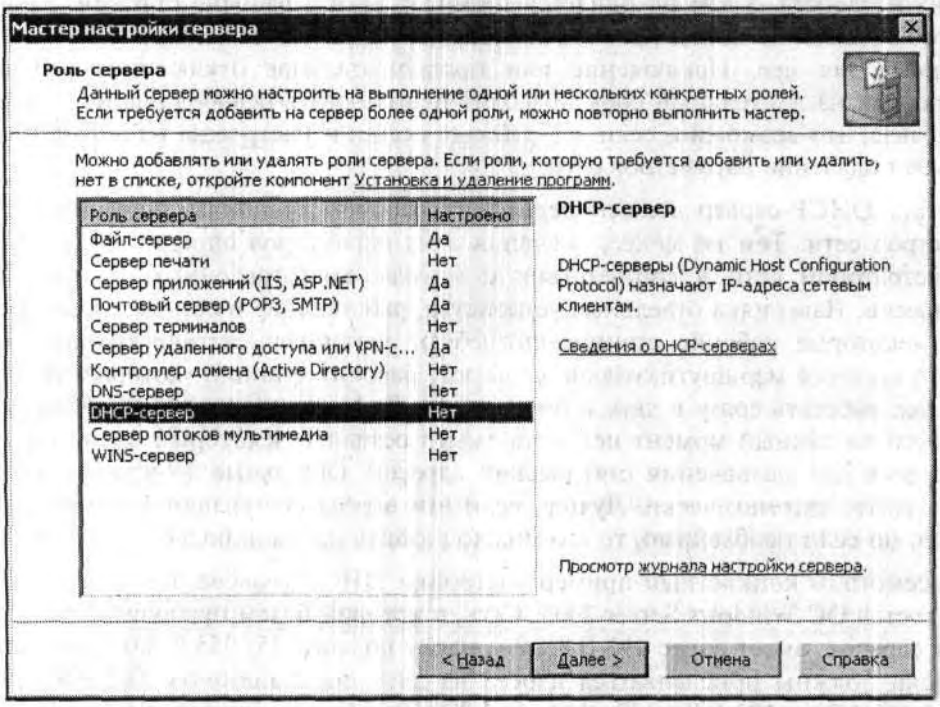


Рис. 8.1. *Окно* **Мастер настройки сервера**

В следующем окне (рис. 8.4) указываем диапазон исключения 192.168.1.71—192.168.1.129.

Далее мастер создания области предлагает настроить дополнительные параметры этой области. В частности, предлагается указать адрес маршрутизатора (шлюза), используемого клиентами. В нашей сети адрес шлюза 192.168.1.1.

На следующем этапе потребуется ввести сведения о домене и DNS-сервере. Но мы еще не включали свой сервер в домен, а DNS-сервер используем тот, что рекомендован провайдером. Поэтому адрес DNS-сервера указываем 195.34.32.116 (рис. 8.5) и нажимаем кнопку **Добавить**.

Также будет запрошено имя WINS-сервера, которого у нас пока нет, поэтому, ничего не вводя, нажмем кнопку **Далее**.

В заключение мастер предложит активизировать созданную область. Если в нашей сети не работают на данный момент другие DHCP-серверы, то можно согласиться с предложением.

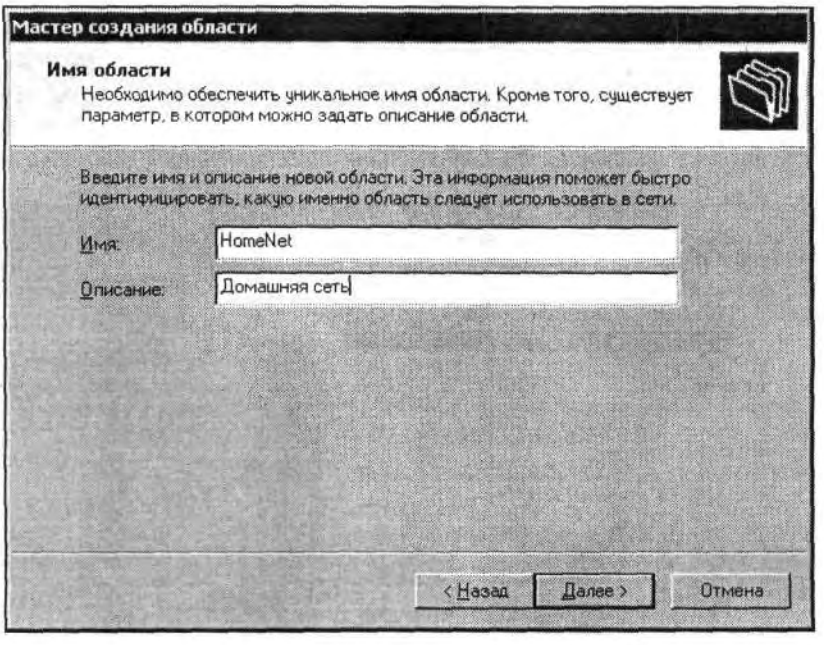


Рис. 8.2. Окно **Мастер создания области**

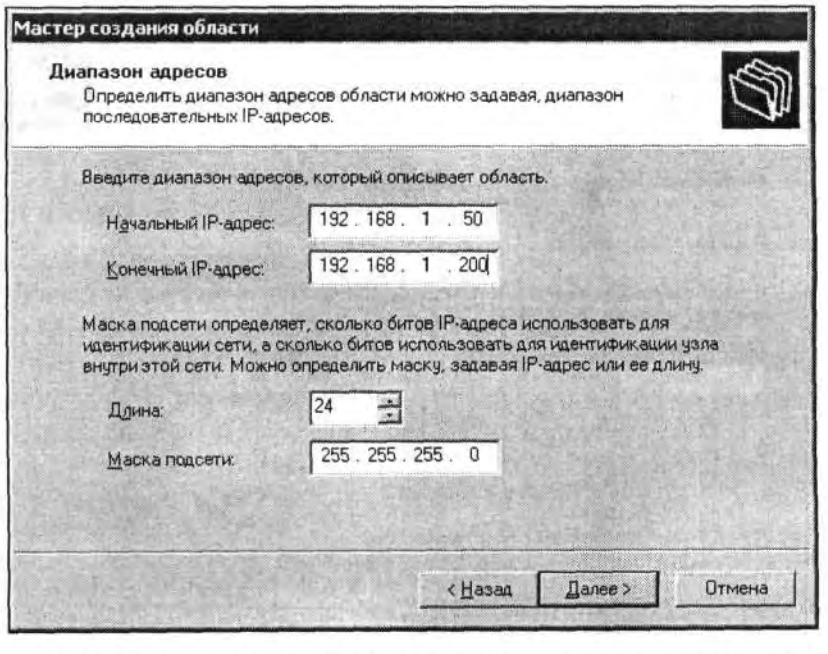


Рис. 8.3. Окно **Мастер создания области — Диапазон адресов**

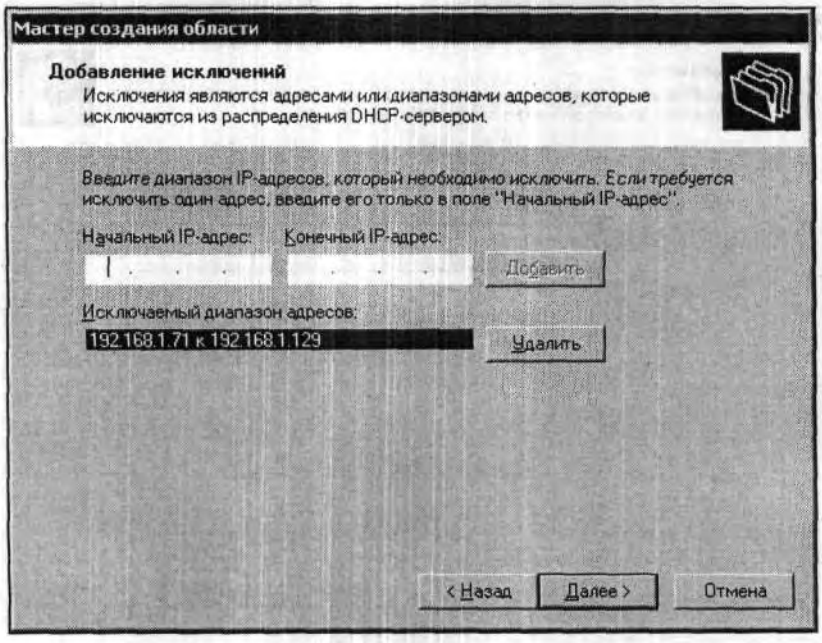


Рис. 8.4. Окно **Мастер создания области — Добавление исключений**

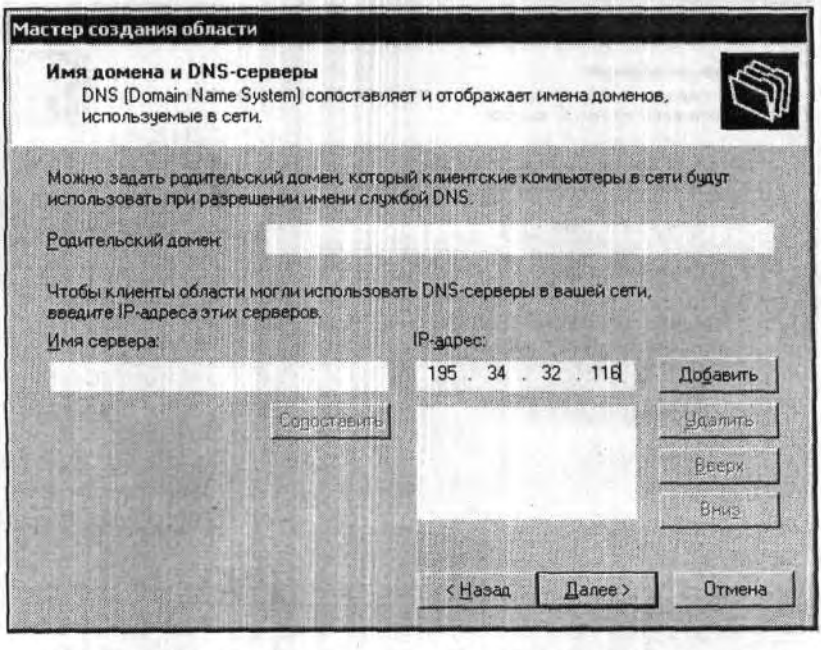


Рис. 8.5. Окно **Мастер создания области — Имя домена и DNS-серверы**

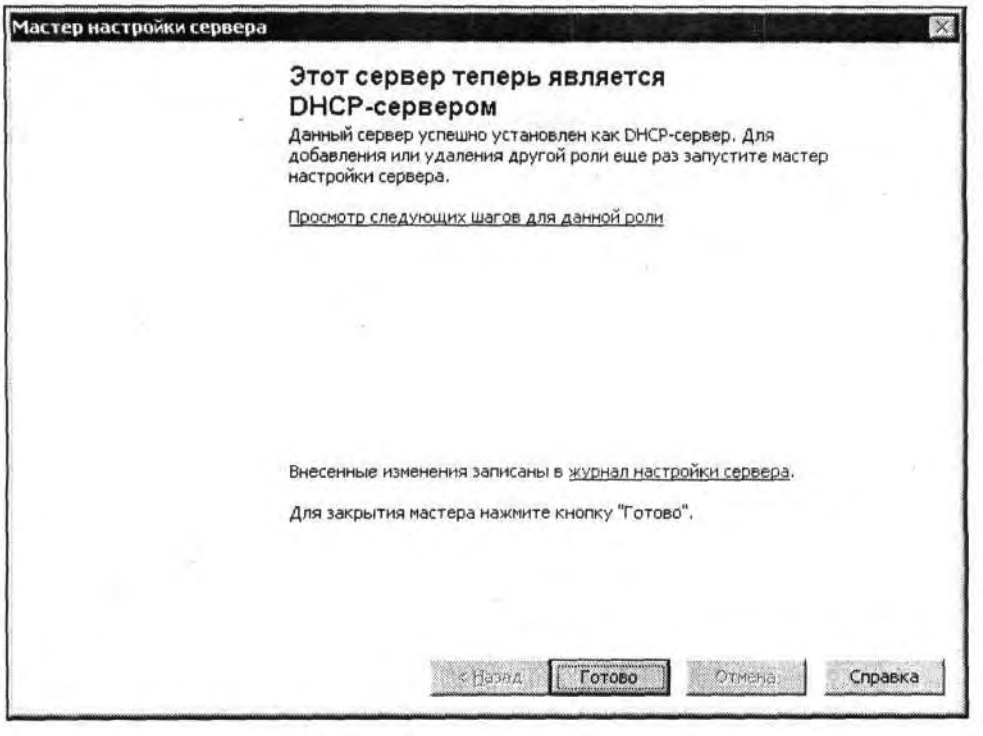


Рис. 8.6. Окно **Мастер настройки сервера** — сообщение об успешной настройке

Теперь можно убедиться в работе DHCP-сервера, установив автоматическое получение IP-адреса и адреса DNS-сервера в свойствах TCP/IP-протокола на любой рабочей станции в сети. Через несколько секунд рабочая станция получит IP-адрес из указанного нами диапазона, адрес DNS-сервера и адрес шлюза в Интернет. Это можно увидеть, посмотрев состояние сетевого подключения (рис. 8.7).

DHCP-сервер работает. Теперь не потребуется перенастраивать параметры TCP/IP-протокола на моем ноутбуке, когда я прихожу домой, или на другом, подключаемом к нашей сети компьютере. Достаточно просто подключить его к сети, а DHCP-сервер все настроит самостоятельно.

В отдельных случаях бывает необходимо, чтобы IP-адрес рабочей станции никогда не изменялся в сети. Для этого следует настроить резервирование IP-адреса на DHCP-сервере. Чтобы получить доступ к его настройкам, достаточно открыть окно DHCP (**Администрирование | DHCP**). На рис. 8.8 показано это окно при первом обращении к узлу **Резервирование** в дереве объектов консоли DHCP. В контекстном меню этого объекта следует вы-

брать пункт **Создать**. На экран будет выведено окно **Создать резервирование** (рис. 8.9).

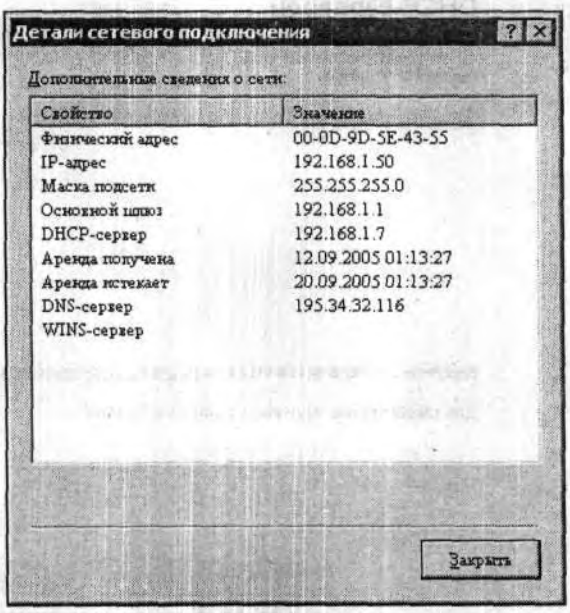


Рис. 8.7. Окно **Детали сетевого подключения**

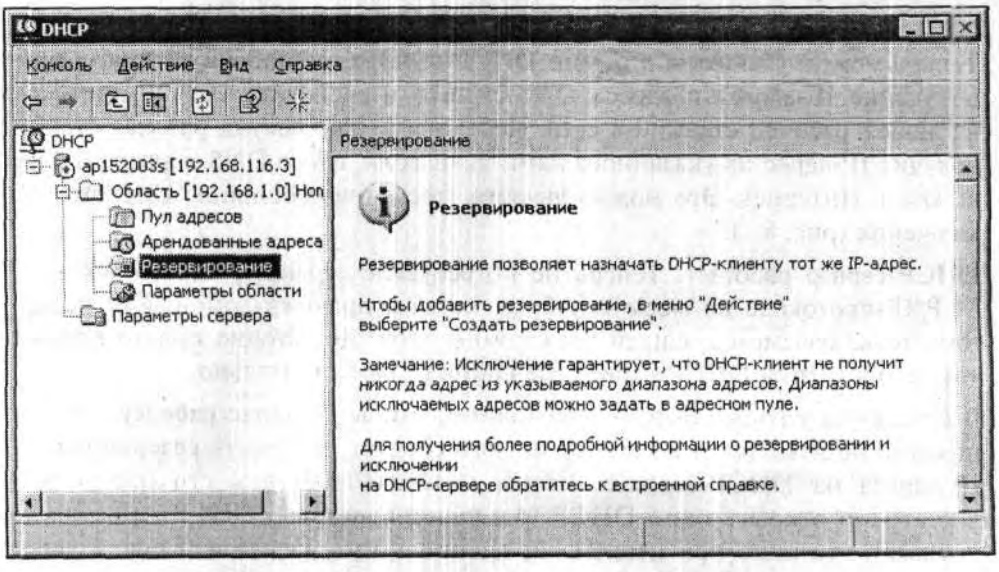


Рис. 8.8. Окно **DHCP** (резервирование)

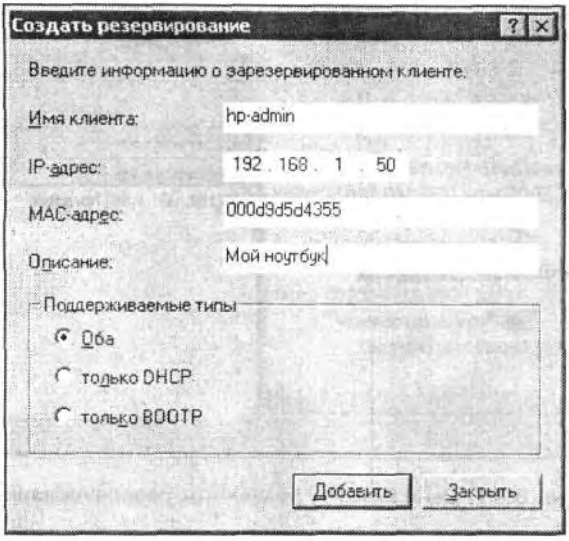


Рис. 8.9. Окно **Создать резервирование**

В этом окне необходимо указать данные компьютера, для которого создается резервирование. Имя компьютера вам известно, IP-адрес можно выбрать из диапазона, с которым работает DHCP-сервер, а MAC-адрес необходимо определить с помощью команды `ipconfig /all`, введенной из командной строки (рис. 8.10).

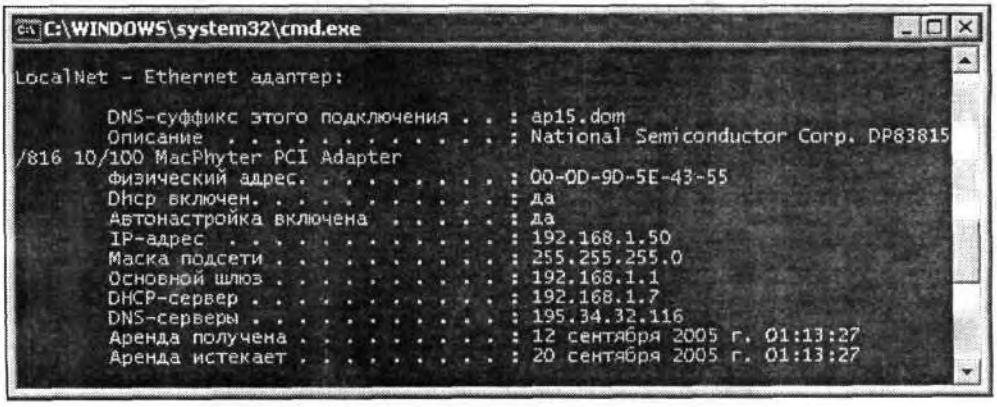


Рис. 8.10. Окно командной строки со значением физического (MAC) адреса

Если на вашем компьютере установлено несколько сетевых адаптеров, то следует выбрать тот, что подключен в данный момент к вашей сети.

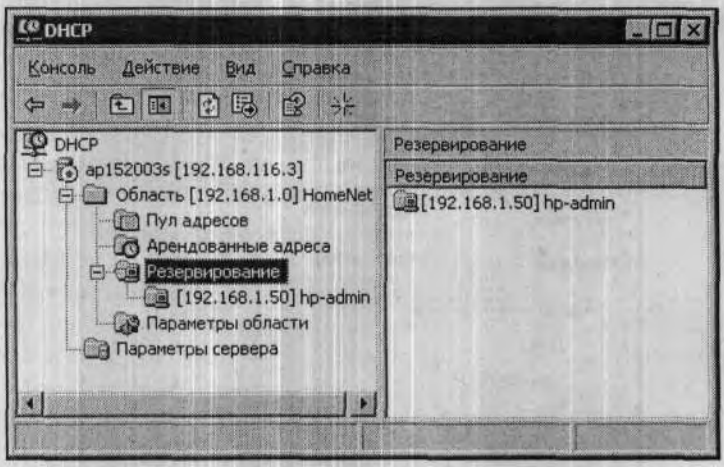


Рис. 8.11. Окно **DHCP** с созданным резервированием

После ввода всех необходимых данных резервирование будет создано (рис. 8.11).

Теперь при каждом подключении к сети компьютер будет получать один и тот же IP-адрес, а в перечне **Арендованные адреса** (рис. 8.12) напротив адреса вашего компьютера будет указано, что это активное резервирование.

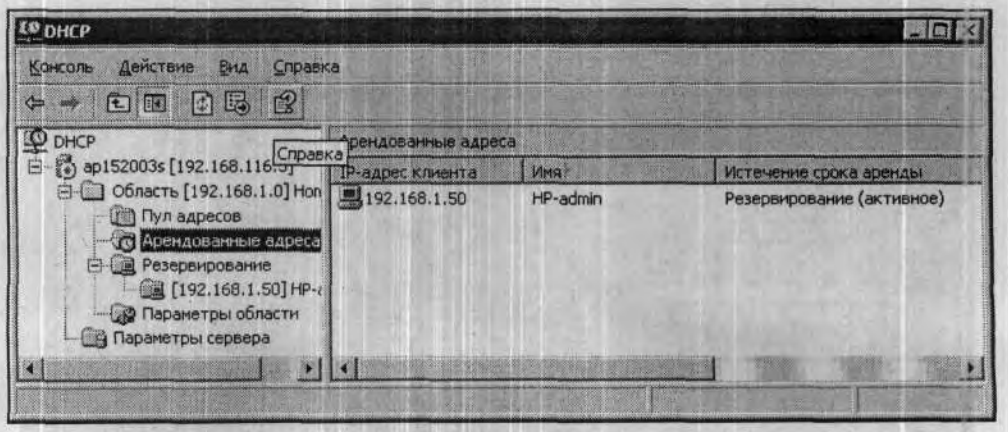


Рис. 8.12. Окно **DHCP** (арендованные адреса)

Покопавшись в настройках DHCP-сервера, вы можете найти для себя еще несколько заслуживающих внимания настроек. Но они могут пригодиться в более сложных сетях, при особых требованиях к DHCP-серверу с вашей стороны. Для нашего случая настройку DHCP-сервера можно считать за-

вершенной. Некоторые дополнительные настройки могут потребоваться после установки DNS и WINS-серверов для того, чтобы клиенты могли автоматически получать их IP-адреса.

Если описанные настройки показались вам слишком сложными, то настоятельно рекомендуем вам просмотреть их еще раз, а при возможности попробовать выполнить их практически. Наличие DHCP-сервера в сети избавит вас от множества проблем в период серьезных преобразований в выросшей сети. Совсем недавно мне пришлось менять сетку адресов для сети, в которой работает более сотни клиентов. Сеть имеет три шлюза в другие сети, множество настроек требуют указания конкретных IP-адресов. Несмотря на большой объем работы, я был доволен тем, что обычные клиенты сети не требовали к себе внимания, поскольку все новые параметры сети были получены ими автоматически.

Настройка сетевых подключений на рабочих станциях при наличии DHCP-сервера выполняется по единому образцу (рис. 8.13).



Рис. 8.13. Окно **Свойства: Internet Protocol (TCP/IP)** (для сетевых подключений рабочих станций)

Как видите, все поля остаются пустыми. Пользователям не надо запоминать IP-адреса и другие параметры сетевых подключений.

DNS-сервер

Свои IP-адреса и адреса важных серверов наши клиенты могут получать автоматически. Но компьютеры сети имеют не только IP-адреса, но и символьные имена. Когда-то основным средством распознавания имен в сети был протокол NetBIOS. В современных сетях этот протокол тоже может применяться, но в сетях Windows он чаще всего работает поверх протокола TCP\IP. В отсутствие других средств для определения имен компьютеров NetBIOS вполне справляется с этой задачей, и в сетевом окружении можно видеть компьютеры рабочей группы с их именами. NetBIOS-имена компьютеров состоят из нескольких символов (обычно не более восьми), и нет возможности по имени идентифицировать принадлежность компьютера к домену — части сети, объединяющей компьютеры в некоторую группу, члены которой могут отличить своего от чужого. Возможно также использование файла LMHOSTS для определения IP-адресов по NetBIOS-именам компьютеров. Но этот файл необходимо заполнять данными вручную. Доменные имена имеют более сложную структуру, чем NetBIOS-имена. Они состоят из частей, разделенных точками. Правая часть имени обычно указывает на корневой домен, а далее влево через точки указываются имена поддоменов. Такие имена принадлежат всей группе компьютеров, всему домену, а не отдельно каждому компьютеру. Для того чтобы получить доступ к компьютеру, обладающему таким именем, необходимо определить его IP-адрес. Эту задачу в сетях решают DNS-серверы. В отличие от DHCP, этих серверов может быть несколько, а располагаться они могут как внутри сети, так и в Интернете. Для доступа в Интернет нам уже приходилось указывать адреса DNS-серверов, которые знают IP-адреса Web-серверов, а также почтовых серверов, работающих в Интернете. Если бы не DNS-серверы, нам пришлось бы запоминать последовательности цифр вместо символьных адресов Web-сайтов.

В локальной сети роль DNS-серверов аналогична. Многие сетевые программы требуют указания IP-адреса или сетевого имени удаленного компьютера. В нашей сети IP-адреса могут изменяться, но имена компьютеров и принтеров могут существовать в неизменном виде годами. Используя имена компьютеров и принтеров сети вместо IP-адресов, мы можем настроить сетевые программы, а также узнать по именам компьютеры в сети при необходимости административного воздействия. В настройках почтовых клиентов тоже можно будет указывать имена почтовых серверов, работающих в вашей сети.

DNS-сервер устроен более сложно, чем DHCP-сервер. Он может работать не только самостоятельно, но и во взаимодействии с другими DNS-серверами, расположенными как в сети, так и в Интернете. Возможна настройка этого сервера в режиме ретрансляции, когда он сам не имеет своей базы данных, но обращается к другим серверам для передачи сведений о соответствии имен IP-адресам запрашивающему их клиенту. Для обращения к DNS-серверу клиент сети должен знать его IP-адрес. Если в сети работает DHCP-сервер, этот адрес может быть передан клиентам автоматически.

Перед установкой DNS-сервера требуется ответить на один важный вопрос — будет ли ваш сервер работать в закрытой сети, не являющейся частью какого-либо домена в Интернете, или такой домен существует, или предполагается его существование в будущем?

От ответа на этот вопрос зависит имя DNS-зоны, которую будет обслуживать ваш сервер. Надо сказать, что сам домен на момент установки сервера может еще не существовать. Для того чтобы в сети существовал домен, требуется установка Active Directory. Но это мы будем делать в следующей главе. Пока мы просто настроим сервер для работы в локальной сети, не имеющей домена. Сервер сможет принимать запросы клиентов на разрешение имен в Интернете, обращаясь для этого к другим DNS-серверам. Но уже сейчас следует понять, как выбрать имя для будущего домена.

Выбирая имя домена, в котором будет работать ваш сервер, следует учитывать, что в Интернете уже существует множество доменных имен. Если имя вашего домена совпадет с уже существующим, а сеть имеет выход в Интернет, то возможны непредвиденные проблемы, связанные с разрешением имен в Интернете и в вашей сети. Так называемые домены верхнего уровня имеют имена, которые зарегистрированы у специально существующих для этого регистраторов имен Интернета. Эти имена не могут совпадать, если имеют отношение к разным доменам, — они уникальны. Так, например, для России существует зона RU. В этой зоне есть зарегистрированное имя AUTOPARK. Полное имя этого домена AUTOPARK.RU. Принадлежит этот домен организации, которая может зарегистрировать у себя домен третьего уровня 15AP.AUTOPARK.RU. Иерархия этих имен может быть понята как иерархия организаций. 15AP подчинена AUTOPARK. Реально административного подчинения может и не быть, но с точки зрения доменов это именно так. Домену AUTOPARK.RU подчинен домен 15AP.AUTOPARK.RU. Эти имена присутствуют в базах данных множества DNS-серверов, поэтому если существует Web-сервер с адресом **http:\\15ap.autopark.ru**, то ваш браузер его быстро найдет в Интернете, обратившись к ближайшему DNS-серверу. Если же вы для своего домена используете именно эти имена, то он не будет найден другими браузерами. Более того, отсылая письма от имени такого домена, вы рискуете попасть в конфликтную ситуацию с организацией-владельцем этих имен.

Если у вас нет списка корневых доменов Интернета, вы можете проверить наличие или отсутствие в Интернете имени, которое вы решили использовать. Попробуйте, подключившись к Интернету, набрать в командной строке `ping www.ru`. Вы увидите отклик от этого сервера, находящегося в зоне RU. Но, как бы вы ни пытались обнаружить домен DOM, вам не удастся его найти. Нет такой зоны в Интернете, а значит, ее можно использовать для закрытого внутреннего домена. Например, ваша сеть может иметь домен с именем MYHOME.DOM.

Теперь ответим еще на один вопрос. Требуется ли доступ из Интернета к вашему домену? Имеется в виду доступ не только к серверу, но и к другим компьютерам сети. Если необходимо, чтобы такой доступ был, то придется у провайдера получать IP-адреса для всех компьютеров сети. В случае с доменом 15AP.AUTOPARK.RU компьютеры смогут иметь полные имена вида COMP1.15AP.AUTOPARK.RU. По этим именам они могли бы быть доступны из Интернета. Но за каждый IP-адрес надо платить. Кроме того, трудно обеспечить безопасность в сети, содержащей такие "самостоятельные" компьютеры.

В условиях локальной сети вполне достаточно иметь изолированный домен, а в Интернете зарегистрировать одно имя, которое сможет использовать Web-сервер и почтовый сервер сети. В этом случае вам потребуется всего один настоящий IP-адрес, а сеть будет работать со своими внутренними адресами и именами. Никаких ограничений относительно доступа в Интернет для рабочих станций не будет, а экономия налицо. При этом DNS-сервер сможет обслуживать компьютеры сети, подсказывая им IP-адреса других компьютеров и адреса Интернета посредством обращения к другим DNS-серверам.

Я думаю, что вам уже стало понятно, как будет организована наша сеть, когда мы установим Active Directory. А сейчас, пока еще не установлена эта служба, мы учтем будущее устройство сети при установке DNS-сервера. В качестве имени домена, которое будет содержать DNS-сервер, сразу укажем такое, какое мы решили дать своему домену. Воспользовавшись мастером настройки сервера, не трудно выполнить первоначальную установку DNS-сервера. Но в дальнейшем, в процессе усложнения сети, добавления новых функций на сервере сети потребуется некоторая корректировка настроек DNS-сервера. Устанавливать DNS-сервер можно, как и DHCP, на любой сервер сети. У нас сервер пока единственный, на него и установим DHCP-сервер.

Если перед установкой DNS-сервера вы решили переименовать компьютер, чтобы согласовать его имя с системой имен, которая будет применена после установки Active Directory, работа уже настроенного сервера DHCP нарушена не будет. До настоящего времени все сетевые службы обращаются к нашему серверу по IP-адресу.

Установка и настройка

Аналогично другим настройкам сервера, устанавливать и настраивать DNS-сервер можно через мастер настройки сервера (**Администрирование | Мастер настройки сервера**). После установки DNS-сервера будет вызван мастер его настройки (рис. 8.14).

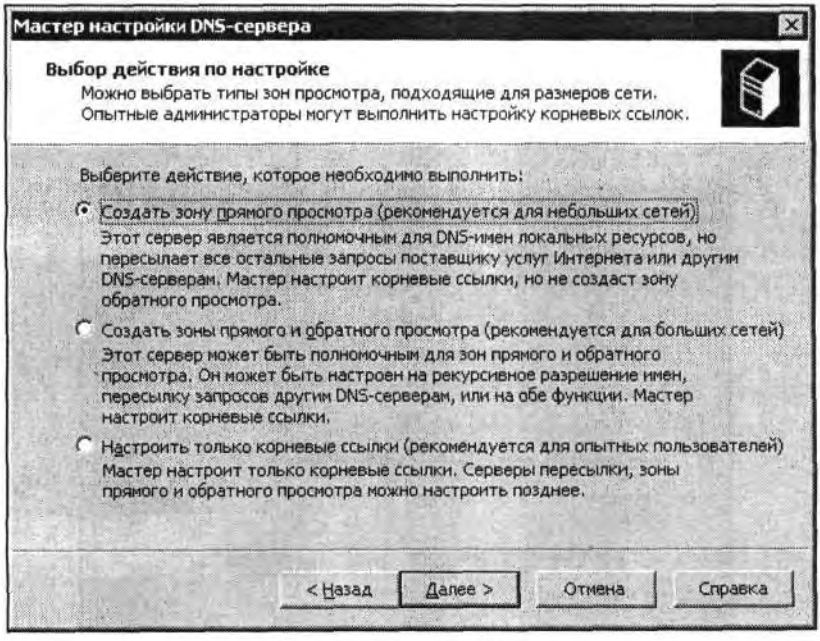


Рис. 8.14. Окно **Мастер настройки DNS-сервера**

Мастер предлагает варианты настроек, а нам остается выбрать наиболее подходящий вариант. Наш сервер до сих пор не может управлять сетью, его роль еще очень похожа на роль рабочей станции. Поэтому для DNS-сервера выбираем достаточно простые функции, которые смогут выполняться в нашей сети. Пока мы не имеем своего домена, и нас интересует в основном выход в Интернет и определение рабочими станциями связи имен компьютеров сети с их IP-адресами. Поэтому выбираем варианты, которые мастер настройки предлагает для небольших сетей.

Во время установки следует отказаться от возможности динамического обновления, зоне прямого просмотра дать понятное имя. Если во время установки что-либо настроено не совсем так, как хотелось, всегда можно исправить ситуацию. Достаточно открыть консоль DNS-сервера (**Администрирование | DNS**) и внести изменения в настройки (рис. 8.15).

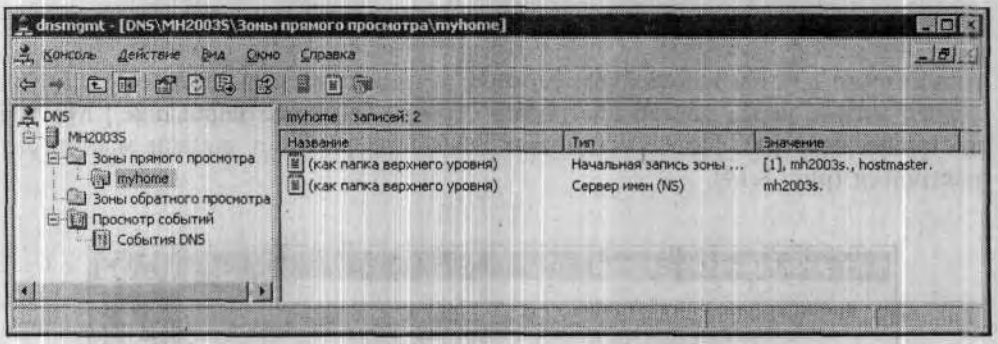


Рис. 8.15. Окно **dnsmgmt**

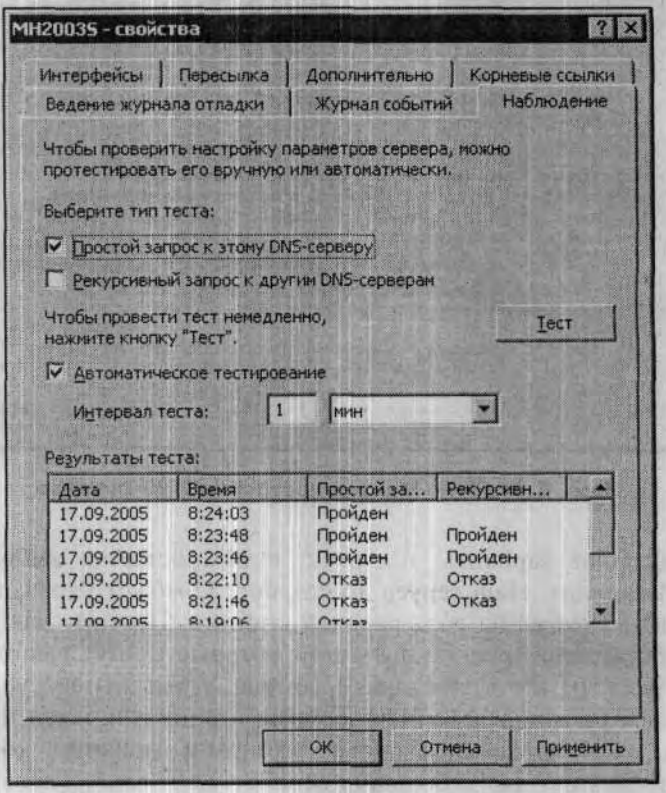


Рис. 8.16. Окно **MH2003S - свойства**, вкладка **Наблюдение**

Чтобы убедиться в том, что ваш сервер работает, необходимо протестировать его. Для проведения тестирования следует открыть окно свойств сервера,

воспользовавшись контекстным меню значка сервера в консоли **dnsmgmt** (управление DNS-сервером).

Выбрав в окне свойств вкладку **Наблюдение** (рис. 8.16), вы можете протестировать работу сервера в автоматическом или ручном режиме. В автоматическом режиме тест проводится через интервалы времени, указанные в поле **Интервал теста**. Если тест показал **Отказ** по запросам к серверу, то следует поискать причину отказа.

Прежде всего, мы знаем, что наш сервер еще не имеет регистрации в Интернете. Следовательно, ему требуется помощь других DNS-серверов для поиска имен в Интернете. Для этого надо указать известные вам адреса DNS-серверов на вкладке **Пересылка** окна свойств сервера (рис. 8.17).

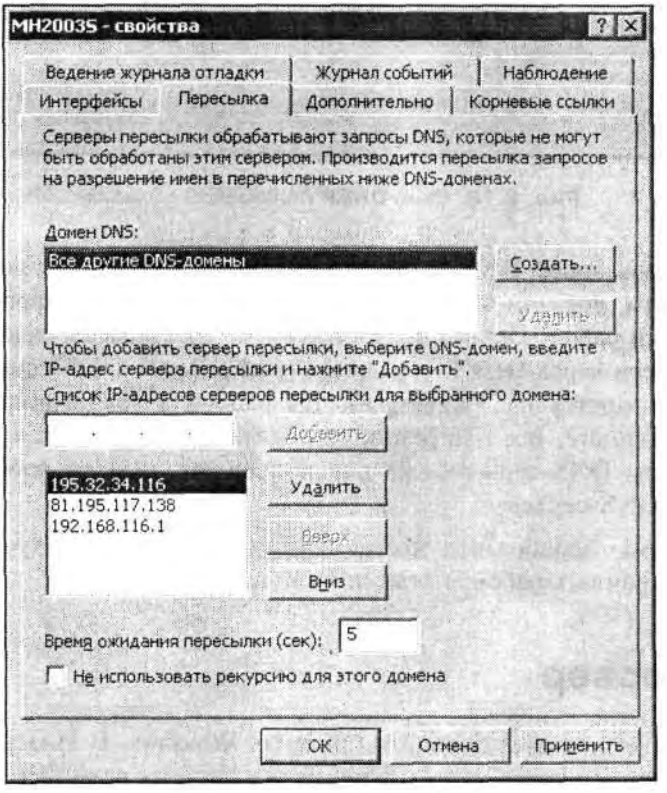


Рис. 8.17. Окно **MH2003S - свойства**, вкладка **Пересылка**

Конечно, убедитесь, что внешние DNS-серверы доступны. Вероятнее всего потребуется подключение к Интернету.

Большинство задач DNS-сервер, входящий в Windows Server 2003, выполняет самостоятельно. Как только вы получили положительный результат теста для DNS-сервера, внесите небольшую корректировку в настройки DHCP-сервера (рис. 8.18).

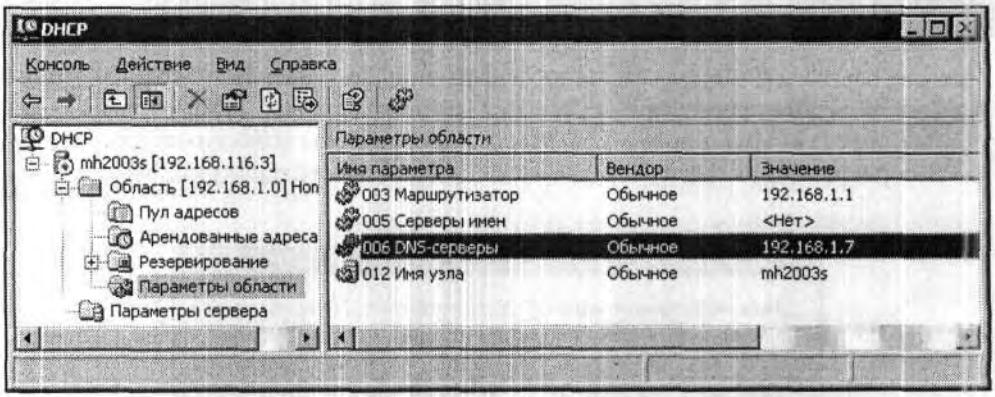


Рис. 8.18. Окно **DHCP** (параметры области)

Следует указать адрес DNS-сервера в параметрах DHCP-сервера и в параметрах области, созданной во время настройки DHCP-сервера. После этой корректировки рабочие станции, настроенные на автоматическое получение параметров сети через DHCP-сервер, получат и адрес DNS-сервера. Рабочие станции не придется настраивать ни для работы в локальной сети, ни для работы в Интернете. Все настройки рабочими станциями будут получены от DHCP-сервера. DNS-сервер будет перенаправлять запросы рабочих станций на внешние DNS-серверы.

Таким образом, поработав с настройками сервера, мы получили возможность не настраивать рабочие станции в нашей сети.

WINS-сервер

WINS-сервер существует только в системах Windows. В Интернете, например, вы не найдете узлов, использующих эту систему разрешения имен в IP-адреса, но провайдеры нередко используют WINS-серверы для организации работы своих сетей с доступом в Интернет. WINS-имена похожи на NetBIOS-имена, но могут иметь существенно большую длину.

Это дает больше свободы в выборе имен для компьютеров в небольшой сети. Но если ваша сеть имеет контакты с другими сетями, основанными на

других операционных системах, то эти длинные имена могут некорректно распознаваться компьютерами данных сетей. Если это для вашей сети не имеет значения, то, применяя WINS-сервер, вы можете использовать имена компьютеров практически любой длины. Но все же, на всякий случай, существенные отличия имен помещайте в их начале. В этом случае усеченные имена, которые можно будет увидеть из другой сети, будут явно отличаться друг от друга. WINS-сервер не трудно установить на вашем сервере. Процедура эта аналогична установке других рассмотренных серверов, но совершенно не требует настроек (рис. 8.19).

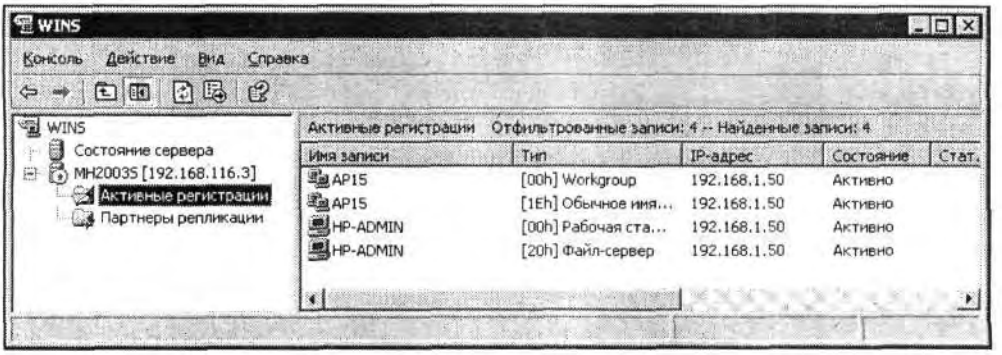


Рис. 8.19. Окно **WINS** (активные регистрации)

Внеся в свойства области DHCP-сервера сведения о WINS-сервере, рабочие станции получат его IP-адрес и смогут регистрироваться на нем. Возможно, что для компьютера с операционной системой Windows XP этот сервер уже лишний с точки зрения его необходимости. Но другие рабочие станции с более ранними версиями ОС Windows, и даже DOS и Linux (если установлена служба Samba), будут надежнее доступны в сети, содержащей WINS-сервер. Но и для новых ОС дополнительный сервер имен не помешает. Клиентов в нашей сети не очень много, и компьютер, содержащий несколько серверов имен, не будет испытывать затруднений при обработке регистраций.

Возможно, на практике следующая информация не пригодится, но известно, что один WINS-сервер может обслуживать до 10 000 клиентов, а на клиентском компьютере можно указывать до 12 различных WINS-серверов. Эта информация, надеюсь, дает представление о возможных размерах сети, применяющей WINS-серверы. Важно лишь, чтобы в настройках TCP/IP-протокола на клиентских машинах было указание на использование NetBIOS через TCP/IP (рис. 8.20).

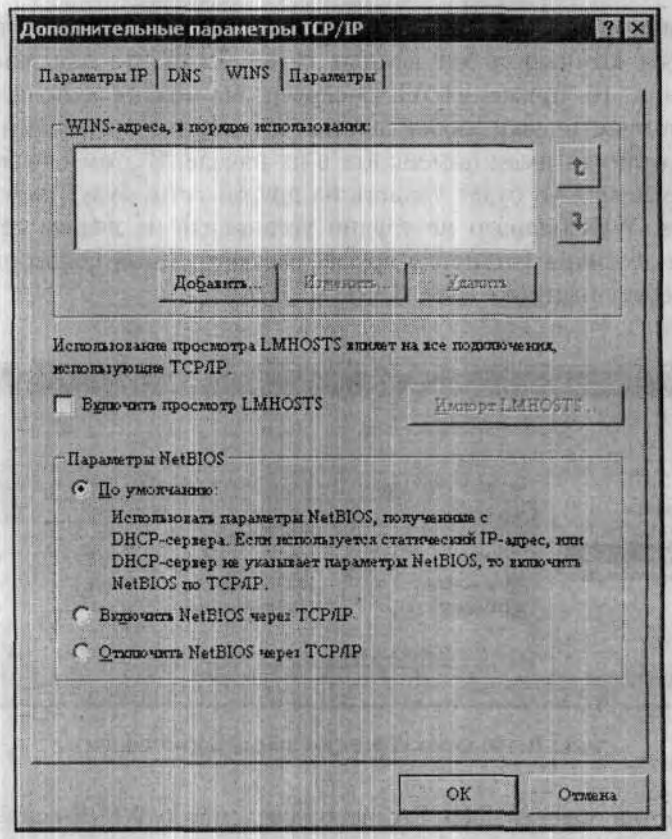


Рис. 8.20. Окно **Дополнительные параметры TCP/IP**

Для более глубокого осмысления и понимания приведенных ранее настроек рассмотрим дополнительно схему локальной сети, в которой эти настройки проводились. Клиентская рабочая станция этой сети получает все сетевые параметры с DHCP-сервера, они могут быть прочтены из окна **Детали сетевого подключения**, доступного через пункт **Состояние** контекстного меню этого подключения (рис. 8.21).

До тех пор, пока ваш сервер работает в экспериментальном режиме, вы можете совершенно свободно изменять различные настройки установленных серверов, наблюдая за результатами ваших действий. Такая "игра" с серверами позволит узнать некоторые особенности их работы, которые могут быть присущи именно вашей сети.

Схема этой сети приведена на рис. 8.22.

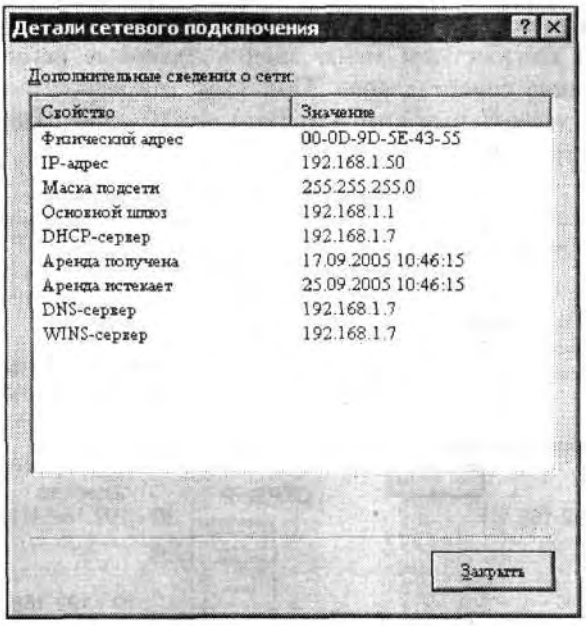


Рис. 8.21. Окно **Детали сетевого подключения**

На схеме показан виртуальный адаптер с IP-адресом 192.168.116.3. Этот адрес можно увидеть в окнах консолей рассмотренных серверов. Причина, по которой серверы выбирают именно этот адрес для своей идентификации, состоит в том, что на данном сервере этот адаптер установлен раньше, чем физический адаптер, который связан с нашей сетью. В составе OpenVPN уже работает один DHCP-сервер. Работает он в сети, состоящей из двух компьютеров, а адрес и маска этой сети существенно отличаются от адреса и маски нашей сети. Ни на какие рабочие параметры сервера это влияния не оказывает. То есть если ваш физический сервер имеет не один сетевой адаптер, то при установке рассмотренных серверов их IP-адрес, указанный в имени сервера в его консоли, может отличаться от реального IP-адреса сетевого адаптера настраиваемой сети, как на рис. 8.18, например.

На рис. 8.20 вы могли заметить, что не отмечена опция **Включить просмотр LMHOSTS**. При выборе этой опции имена компьютеров сети, которые не могут быть сопоставлены их IP-адресам средствами сети, сопоставляются в соответствии с записями, которые вы можете создать в файле LMHOSTS. Но при наличии WINS-сервера в сети такие соответствия можно указывать в общедоступной базе этого сервера. Соответствие будет указано вручную, но информация о нем будет доступна всем рабочим станциям.

Для того чтобы внести сведения о таком соответствии, можно в консоли WINS-сервера в контекстном меню значка **Активные регистрации** выбрать **Создать статическое сопоставление**. При этом откроется окно (рис. 8.23), в котором следует указать имя компьютера и его IP-адрес. Поле **Область NetBIOS** заполнять не обязательно.

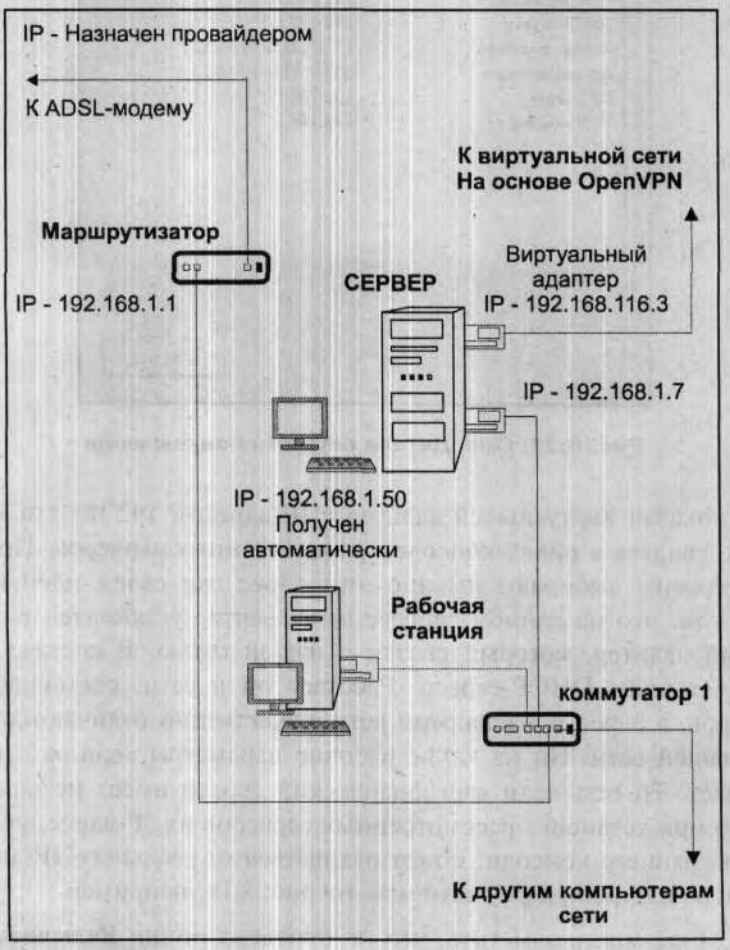


Рис. 8.22. Схема тестовой сети

Эффект от внесения такой записи равнозначен эффекту от внесения подобной информации в файлы LMHOSTS всех компьютеров сети. Если в вашей сети применяется протокол NetBIOS, то вполне возможно, что WINS-сервер вам необходим.

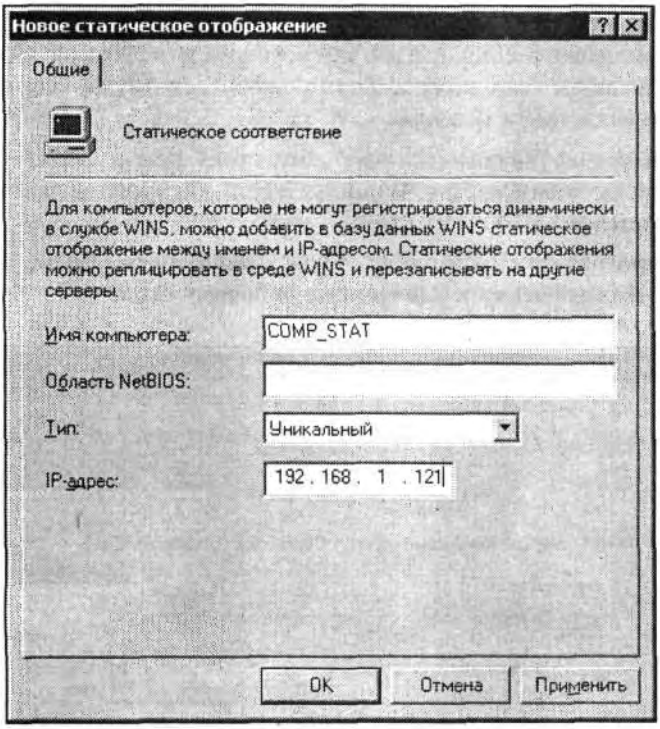


Рис. 8.23. Окно **Новое статическое отображение**

Сервер терминалов

Среди нужных и полезных программных серверов, входящих в состав Windows Server 2003, есть еще один, который для администратора сети может быть просто необходим.

Сервер терминалов — название, которое применялось еще в Windows 2000 Server. ОС Windows Server 2003 стала похожа на Windows XP, и название рассматриваемой нами службы изменилось. Теперь это удаленный доступ к рабочему столу. Но, в отличие от Windows XP, доступ возможен не только к активному сеансу — можно создавать новые сеансы работы с сервером, не нарушая работу текущего консольного сеанса. Без дополнительного лицензирования доступны лишь два удаленных сеанса работы, администратору их более чем достаточно. Для работы в режиме администрирования установки дополнительной роли сервера как сервера терминалов не требуется. Сеансы могут быть запущены как от имени одного пользователя, так и от разных. Для сеансов с определенными параметрами можно сохранять все параметры сеанса в файлах с расширением rdp. Учи-

тывая, что в вашей сети может быть не один сервер, эти файлы с понятными именами можно сохранять в специально отведенной для них папке. В одно и то же время вы можете воспользоваться двумя сеансами на каждом сервере в удаленном режиме.

Для подключения к удаленному рабочему столу или к серверу терминалов достаточно иметь компьютер с Windows XP, в которой встроена программа доступа к удаленному рабочему столу.

Вызвать эту программу можно через **Пуск | Выполнить | mstsc**. При этом откроется окно **Подключение к удаленному рабочему столу** (рис. 8.24).

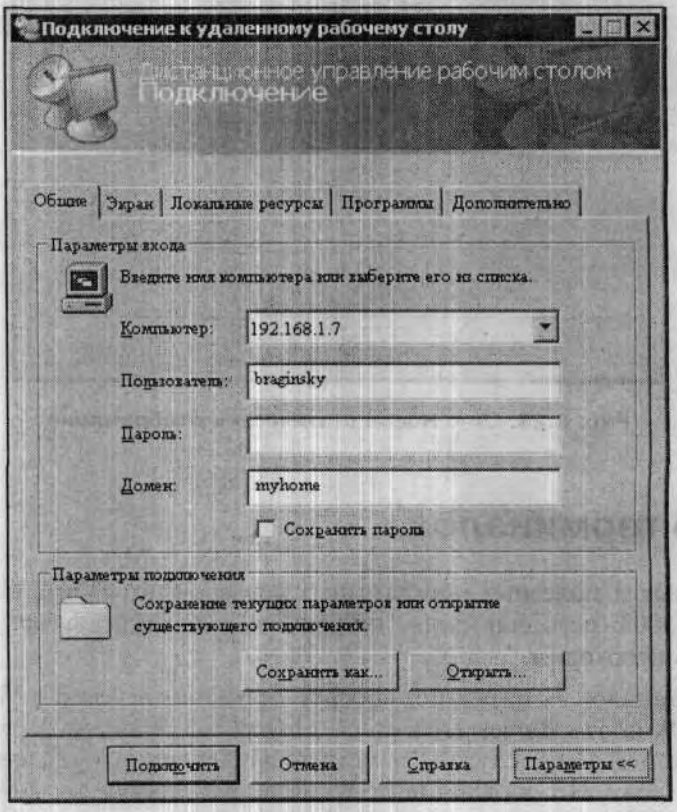


Рис. 8.24. Окно **Подключение к удаленному рабочему столу**

На нескольких вкладках этого окна вы можете установить любые желаемые настройки для отображения удаленного рабочего стола, а после завершения выбора этих настроек сохранить их в файл.

Если вы имеете права администратора на удаленном сервере, то никаких проблем с настройкой и входом в сеанс у вас не возникнет. Единственно,

что следует иметь в виду, это правила завершения сеанса. Как при обычном доступе к компьютеру, требуется выполнять определенные действия при выключении компьютера, например, при выходе из удаленного сеанса следует выполнять последовательность подобных действий. Само собой разумеется, что при удаленном доступе, выходя из сеанса, не следует выбирать **Завершение работы**. Мы управляем сервером, и после завершения удаленного сеанса сервер должен продолжать работу. Не следует и просто закрывать окно терминальной сессии. Сеанс останется активным на сервере, а вы имеете возможность открывать не более двух сеансов в один момент времени. Если вы оставите активными два сеанса, то больше не сможете подключиться к серверу, пока не закроете их, подойдя к самому серверу. Но, я думаю, если бы вы были рядом, то и удаленный доступ не очень был бы нужен. Особенно интересно оказаться в совершенно беспомощном состоянии из-за своей оплошности на расстоянии нескольких десятков или сотен километров от сервера. Мне как-то приходилось среди ночи вызывать такси и ехать к серверу, чтобы исправить свою ошибку.

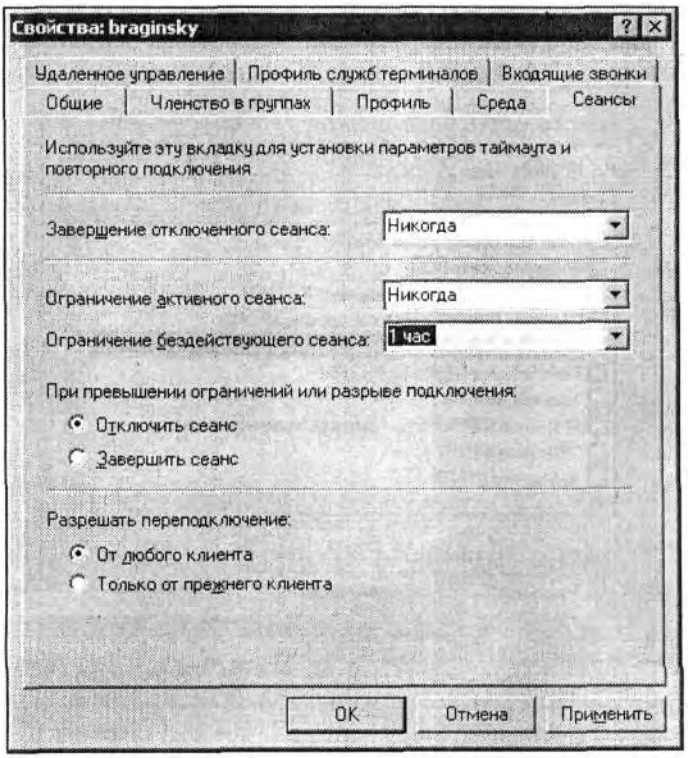


Рис. 8.25. Ограничение бездействующего сеанса

Но оплошность может заключаться не только в неправильном выходе из сеанса связи с сервером. Надо соблюдать особенную осторожность при внесении изменений в настройки сетевого подключения. При выходе из сеанса без его закрытия можно надеяться на автоматическое его закрытие, если заранее установить для учетных записей администраторов **Ограничение бездействующего сеанса** (рис. 8.25). Но при ошибке в настройках сетевого подключения вы рискуете потерять связь с сервером окончательно.

Прежде чем выполнять какие-либо действия на сервере в удаленном режиме, проанализируйте возможные варианты и последствия своих действий. Только при полной уверенности в положительном результате своей работы с сервером можно выполнять настройки сервера удаленно.

Работа через Интернет

Наибольшие удобства приносит применение программы **Удаленный доступ к рабочему столу**, когда этот доступ осуществляется через Интернет.

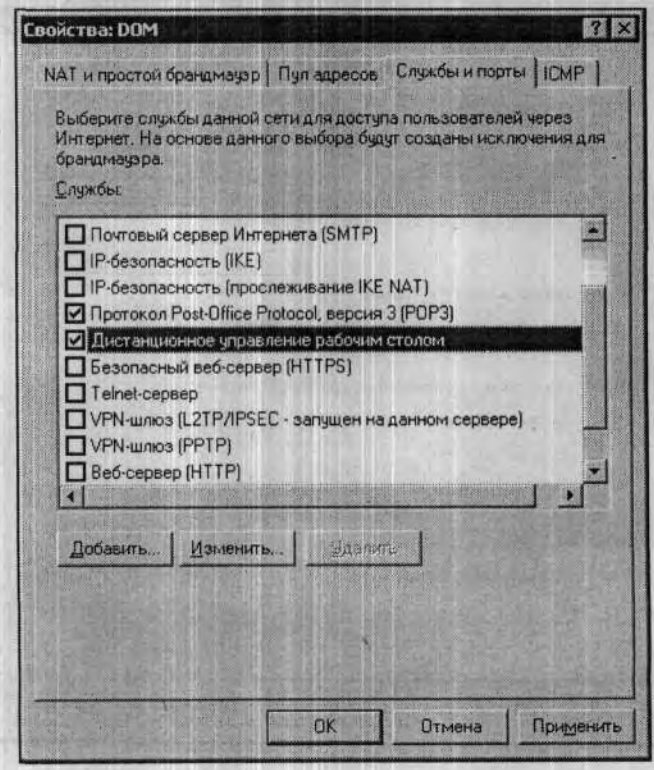


Рис. 8.26. Окно **Свойства: DOM**
(свойства интерфейса сервера, связанного с Интернетом)

Для того чтобы это было возможно, следует обеспечить доступ к удаленному рабочему столу на всех ступенях защиты сети от несанкционированного доступа из Интернета.

Если доступ сети к Интернету настроен через сервер, то следует обеспечить доступ из Интернета к рабочему столу сервера, отметив соответствующий пункт на вкладке **Службы и порты** окна свойств интерфейса сервера, на котором настроен NAT или который просто защищен брандмауэром (рис. 8.26).

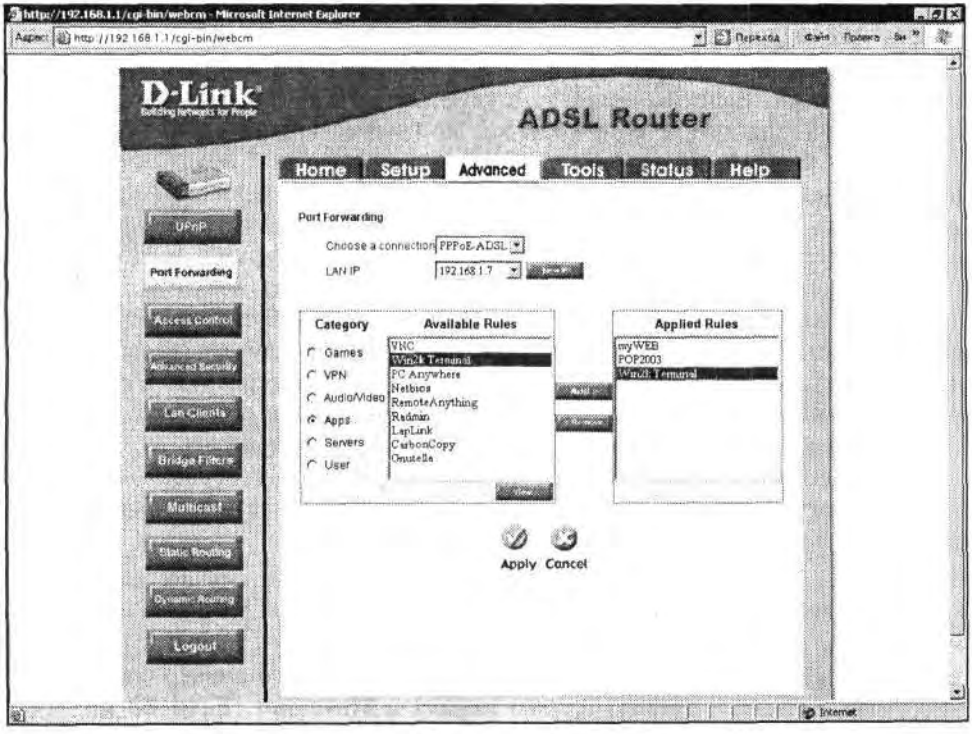


Рис. 8.27. Окно **Advansed Port Forvarding**
(расширенные настройки перенаправления портов)

Если доступ к Интернету организован через аппаратный маршрутизатор, то в его настройках следует обеспечить доступ к серверу. Некоторые модели маршрутизаторов имеют достаточно удобный Web-интерфейс управления и, к тому же, заготовленные шаблоны для самых распространенных настроек доступа к ресурсам сети из Интернета.

Так, ADSL-модем-маршрутизатор D-Link 500-T может быть настроен для доступа к удаленному рабочему столу конкретного компьютера простым выбором шаблонных настроек и адреса этого компьютера (рис. 8.27). Аналогичными возможностями обладают и другие типы маршрутизаторов. Если

ваш маршрутизатор не имеет Web-интерфейса, то придется изучить документацию к нему и выполнить настройку через Telnet или другие, предусмотренные для данной модели интерфейсы.

Возможные неисправности

Наиболее частая, пожалуй, ошибка при организации сети с маршрутизаторами и шлюзами — это установка лишнего DHCP-сервера. В современных аппаратных маршрутизаторах DHCP-сервер обычно встроен в устройство. Это позволяет создать сеть из небольшого числа компьютеров с минимальными затратами. Если вы оставите в сети два DHCP-сервера, которые работают в одной подсети, с одинаковыми или пересекающимися диапазонами адресов, то вполне возможно, что сеть будет работать медленно, выход в Интернет будет затруднен, возможны конфликты IP-адресов. Аналогичные проблемы возникнут и при установке второго сервера, если на нем устанавливается DHCP-сервер, дублирующий уже существующий в сети. Чтобы DHCP-серверы могли работать в одной сети, следует поделить диапазоны адресов, которые они будут выдавать. Но если в сети будут применяться зарезервированные адреса, которые клиенты должны получать постоянно, эти адреса должны быть зарезервированы на всех DHCP-серверах. В то же время нельзя забывать о параметрах сети, которые должны передавать клиентам DHCP-серверы. Если один из серверов не будет передавать компьютерам параметры сети, то в зависимости от того, какой DHCP-сервер выдал адрес клиенту, могут работать или не работать отдельные сетевые службы. Для небольшой сети лучше оставить один DHCP-сервер.

Неисправность DNS-сервера обнаруживается в нашем случае, когда нарушается доступ к ресурсам Интернета. Для того чтобы отличить проблемы, связанные с работой DNS-сервера, от других проблем связи с Интернетом, определите IP-адрес какого-либо узла и используйте его вместо символьного адреса для проверки работы самого канала в Интернет. Если по IP-адресу связь устанавливается, то проблемы с DNS-сервером, иначе надо искать другую причину.

Сервер терминалов позволяет клиентам обращаться к серверу как по IP-адресу, так и по имени компьютера в сети. Если говорить о применении удаленного доступа к рабочему столу для администрирования сервера, то лучше использовать IP-адрес. Это обеспечит сохранение связи между сервером и вами даже при проблемах с определением соответствия имени и IP-адреса.

Как и при работе с рабочей станцией, желательно периодически создавать резервные копии важных данных сервера. WINS- и DHCP-серверы имеют встроенную возможность архивирования и восстановления из архива своих баз данных. Эта функция доступна из контекстных меню консолей данных серверов.



Глава 9

Active Directory

Активный каталог — так обычно переводится словосочетание Active Directory. Ввиду того, что перевод не облегчает понимания назначения и функций Active Directory в сети, обычно это словосочетание приводится без перевода, а часто сокращается до AD. Таким сокращением мы и будем пользоваться в этой главе. Компьютер, содержащий AD, обычно называется контроллером домена.

Что же такое AD?

AD — целый комплекс средств Windows Server 2003. Это и сетевой каталог, содержащий сведения обо всех объектах сети, публикуемых в этом каталоге, и средство идентификации и распределения прав пользователей в сети. Учетные записи пользователей, групп пользователей, компьютеров, принтеров — все может храниться в AD. Рабочие станции, входящие в AD и соответственно в домен, опознаются сетью как свои, права на различные сетевые ресурсы может получить любая учетная запись (конечно, при содействии администратора). Централизованное хранение учетных записей позволяет идентифицировать пользователя при входе в сеть, обеспечив его всеми правами и средствами, предусмотренными для него в сети, включая профиль пользователя, который может тоже храниться на сервере.

В отличие от одноранговой сети, где сервер не выполняет функции контроля прав учетных записей пользователей, входящих в сеть, в доменной сети, содержащей AD, вы получаете централизованный контроль над всеми учетными записями в сети. Более того, подключив рабочую станцию к домену, вы автоматически становитесь администратором этой рабочей станции, как администратор домена.

Постепенно разбираясь с политиками домена, возможностями управления объектами AD, вы сможете очень гибко и эффективно управлять своей сетью, делая работу в ней удобной, а сеть защищенной от несанкционирован-

ных действий. Для системного администратора AD в сочетании со средствами удаленного администрирования становится незаменимым инструментом управления сетью.

Установка AD

Наш сервер уже выполняет несколько важных функций (во всяком случае, их настройка описана в книге). Теперь наступает момент, когда уже работающие в сети рабочие станции, вполне возможно, придется несколько перенастроить, а пользователям привыкнуть к новой процедуре аутентификации в сети. Но уже через пару дней работы с AD большинству активных пользователей сети станут понятны преимущества AD по сравнению со старой, одноранговой организацией сети.

Перед началом установки AD следует подумать о совместимости существующих настроек для работающих служб с теми преобразованиями, которые придется выполнить при установке AD. Например, почтовый сервер, который мы рассмотрели в *главе 8*, требует авторизации клиентов, как локальных пользователей компьютера.

Придется решить, по какому пути идти дальше. Либо менять способ идентификации пользователей на почтовом сервере, либо устанавливать AD и почтовый сервер на разные компьютеры. Какой из вариантов подходит вам, вы решите сами. В моей сети AD и почтовый сервер сейчас на разных серверах, но был момент их работы на одной машине. До тех пор, пока пользователей сети немного, не бойтесь переходить на оптимальную на данный момент организацию сети, даже если изменения коснутся средств, с которыми работают пользователи. Тем не менее, если позволяют средства, можно каждую из важных сетевых функций поручать не только отдельному программному серверу, но и отдельному компьютеру. В этом случае настройки, например, почтового сервера будут абсолютно независимы от других служб сети. Точнее, есть возможность оставить эти настройки независимыми. Но при необходимости можно каждую серверную функцию перенастраивать в соответствии с текущими потребностями.

Мы начнем установку AD на тот же компьютер, на который уже установлены рассмотренные ранее серверы.

Администрирование | Мастер настройки сервера — это традиционное для большинства системных администраторов начало установки новых ролей сервера. Роль, которую в данный момент следует выбрать, это контроллер домена (Active Directory). Контроллер домена — главный сервер домена, на котором обычно и располагается AD. Выбрав эту роль, разрешаем мастеру продолжить свою работу. Перед началом собственно установки AD мастер предупредит, что старые версии ОС Windows, а также клиенты

Samba и ОС Apple Mac OS X не смогут использовать преимущества AD ввиду отсутствия поддержки в них средств безопасного обмена данными, которые применяются в Windows Server 2003. Если вас это не пугает (большинство клиентов вашей сети используют Windows XP или Windows 2000), то продолжаем установку.

Следующие шаги будем рассматривать по порядку и более внимательно.

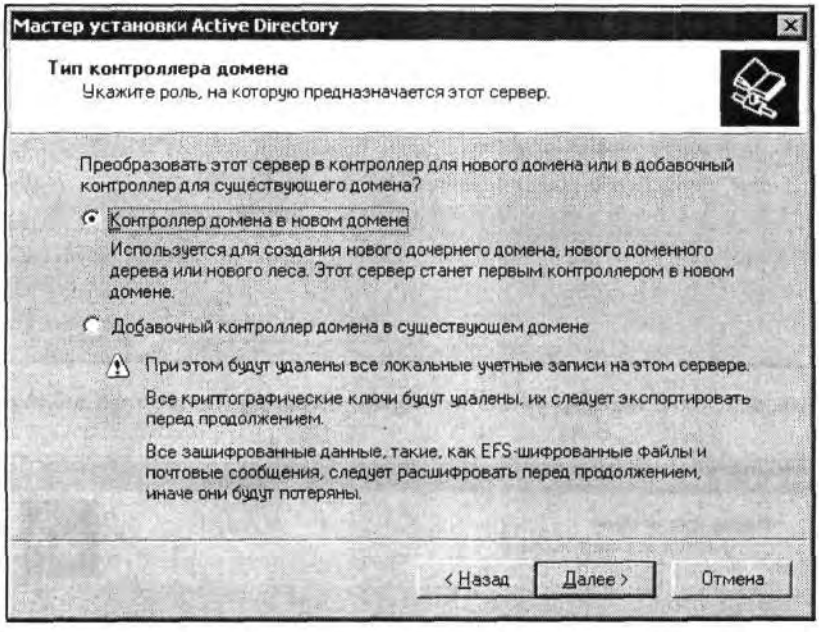


Рис. 9.1. Окно **Мастер установки Active Directory** (выбор роли сервера)

В процессе установки AD мастер предложит выбрать роль сервера, но уже на уровне работы в AD. Мы выбираем ситуацию, когда наш сервер становится первым контроллером домена (рис. 9.1).

Далее необходимо определить тип создаваемого домена (рис. 9.2). В нашем случае это совершенно новый домен, не зависящий ни от каких других доменов.

Примечание

Для выбора других вариантов требуется наличие уже работающей доменной сети.

На следующем этапе требуется указать имя домена (рис. 9.3). В *главе 8* мы уже рассматривали вопрос об имени домена в связи с установкой DNS-сервера.

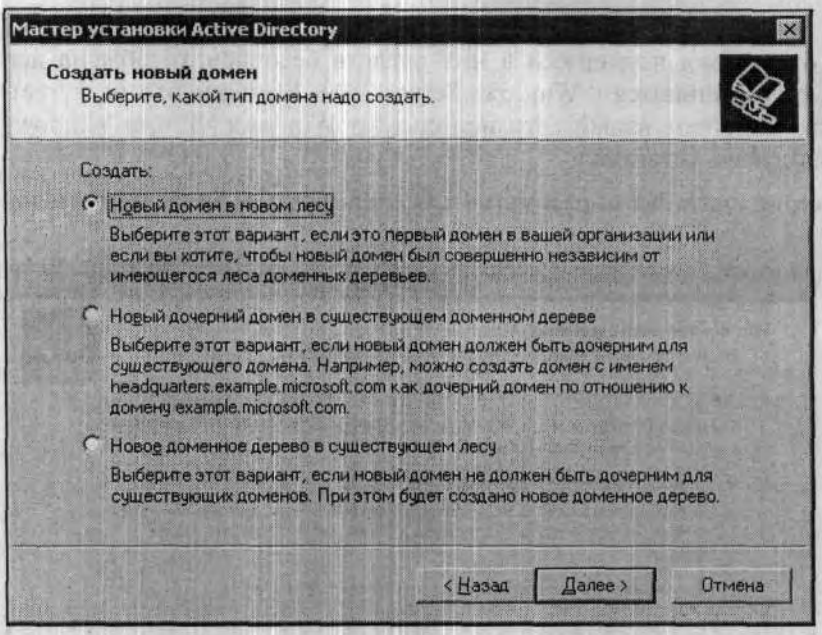


Рис. 9.2. Окно **Мастер установки Active Directory** (выбор типа домена)

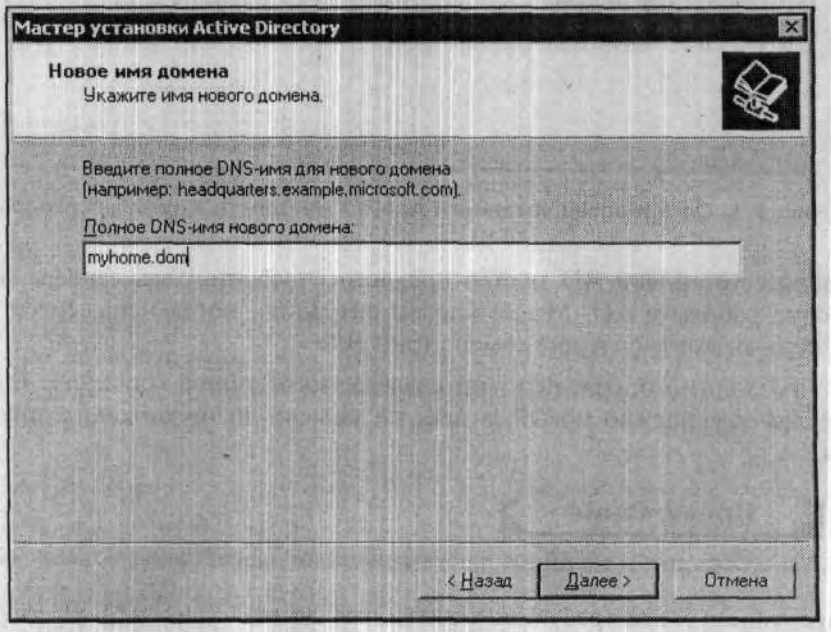


Рис. 9.3. Окно **Мастер установки Active Directory** (имя домена)

Тогда было решено, что имя будущего домена будет **myhome.dom**. Это имя домена и применим при установке AD. Конечно, если у вас есть другой вариант имени, который необходимо использовать, применяйте его.

Введя имя и нажав кнопку **Далее**, подтверждаем или изменяем NetBIOS-имя домена (рис. 9.4).

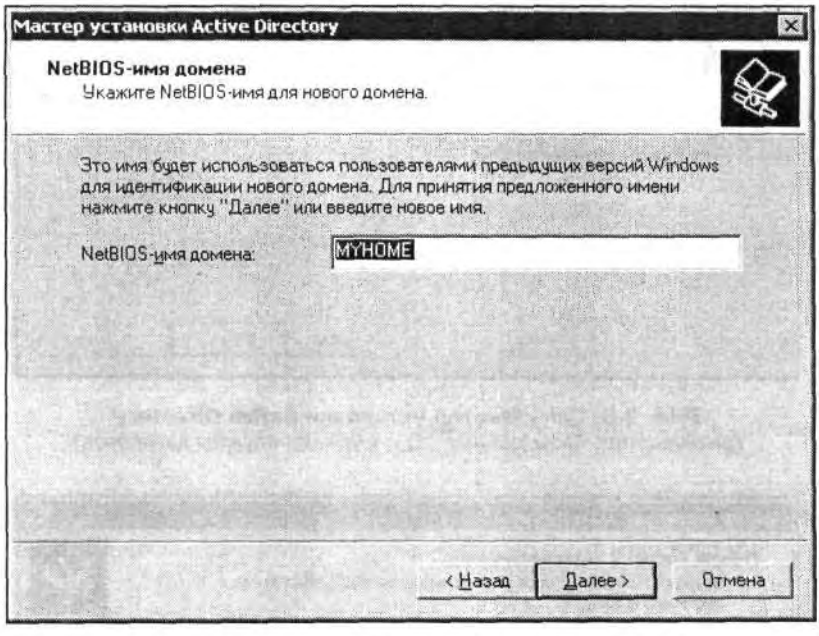


Рис. 9.4. Окно **Мастер установки Active Directory** (NetBIOS-имя домена)

Далее указываем место хранения данных AD (рис. 9.5). Имея эту информацию, вы можете делать резервные копии базы данных.

Указывая место размещения копии общих файлов домена (рис. 9.6), обратите внимание на то, что эта копия должна быть помещена на том NTFS. Для резервных копий файлов часто применяют отдельные диски FAT32, что позволяет обратиться к этим дискам даже из-под DOS в аварийной ситуации. Но в данном случае такое решение не применимо.

На следующем шаге мастер установки AD проведет диагностику DNS для службы каталогов. Скорее всего, тест, проведенный мастером, покажет, что сервер DNS настроен неправильно для обеспечения работы AD. Следует выбрать предложение мастера "Установить и настроить DNS-сервер на этом компьютере и выбрать этот DNS-сервер в качестве предпочитаемого DNS-сервера".

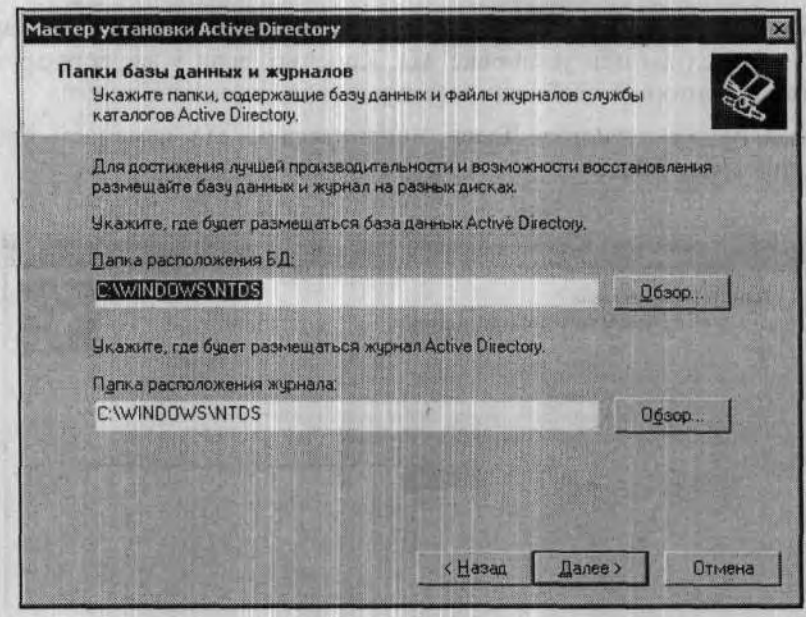


Рис. 9.5. Окно **Мастер установки Active Directory** (размещение базы данных AD и журнала службы каталогов)

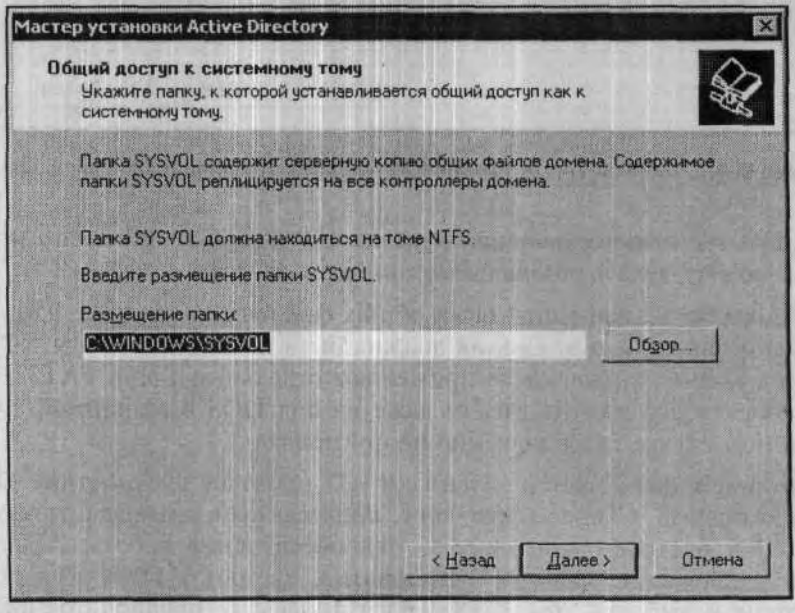


Рис. 9.6. Окно **Мастер установки Active Directory** (размещение копии общих файлов домена)

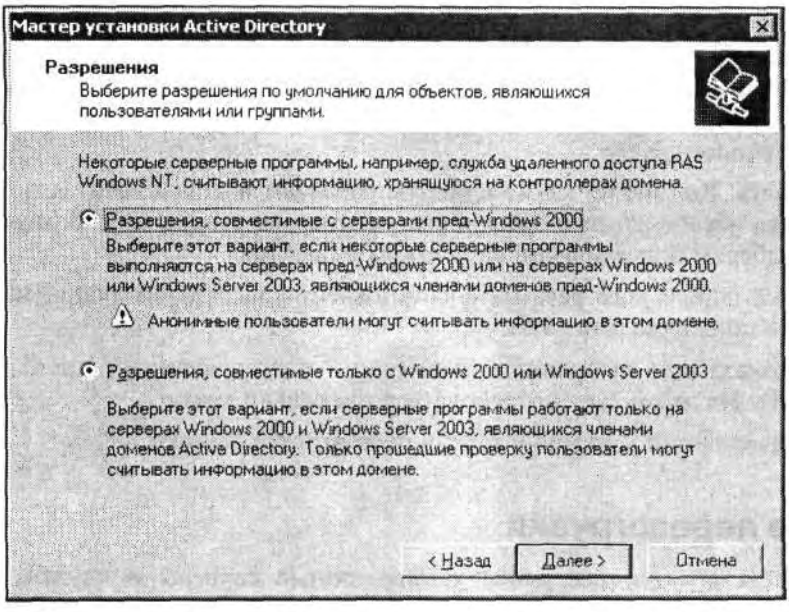


Рис. 9.7. Окно **Мастер установки Active Directory** (разрешения по умолчанию)

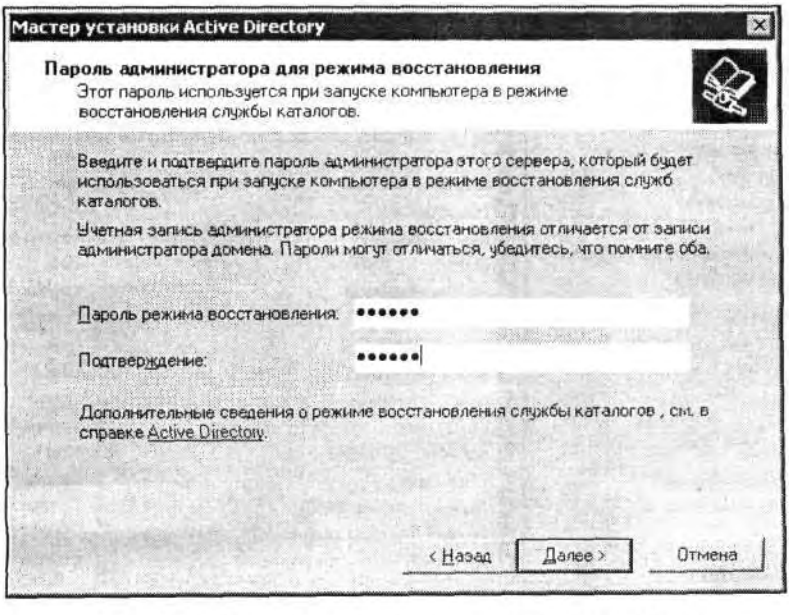


Рис. 9.8. Окно **Мастер установки Active Directory** (пароль режима восстановления)

Далее мастер предложит выбрать вариант разрешений по умолчанию, применяемых в нашем домене (рис. 9.7). Варианта два. Один менее строгий, но разрешающий работу со старыми операционными системами, другой более жесткий, предполагающий, что в сети работают ОС, версии которых не ниже, чем Windows 2000.

Вам решать. Вы знаете, какие клиенты работают в вашей сети, есть ли необходимость обеспечения возможности работы для старых ОС. В этом примере мы выберем более мягкий вариант разрешений.

Установка пароля для режима восстановления не требует пояснений ввиду простоты поцедуры (рис. 9.8).

После показа всех выбранных вами опций мастер начинает процедуру создания AD. На это может потребоваться несколько минут.

После завершения установки нужна перезагрузка сервера.

После перезагрузки

После перезагрузки все ранее установленные серверы и службы должны продолжать нормально работать, кроме почтового сервера.

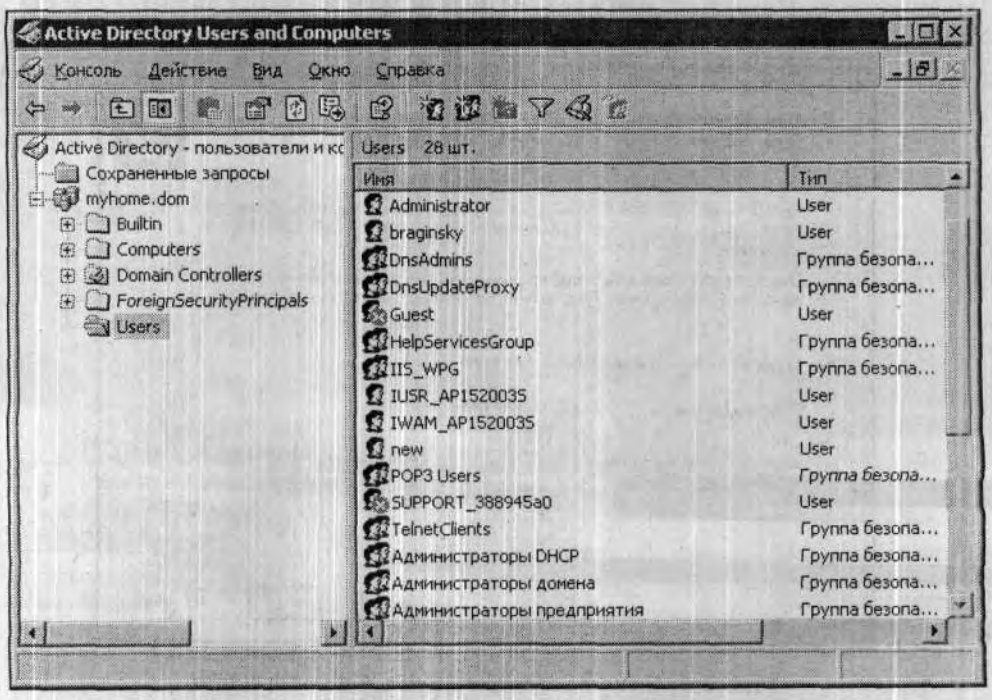


Рис. 9.9. Окно **Active Directory Users and Computers**

Методы проверки подлинности, которые были выбраны для учетных записей его пользователей, теперь не применимы. Больше нет локальных пользователей этого компьютера. В панели управления больше нет значков, которые позволили бы открыть средства управления пользователями. Теперь все ранее существовавшие учетные записи стали учетными записями домена. Проверка прав пользователей любых сервисов невозможна в обычном режиме.

Теперь доступ к управлению учетными записями находится по адресу **Администрирование | Active Directory Users and Computers** (рис. 9.9). Здесь теперь все — сами учетные записи, группы пользователей, которые заранее наделены определенными правами или учетные записи группы пользователей, созданные вами. Здесь можно встретить и компьютеры, если вы их зарегистрируете в домене, и принтеры... Словом, это мощнейший центр управления учетными записями и ресурсами сети.

Но почтовый сервер оказался не действующим.

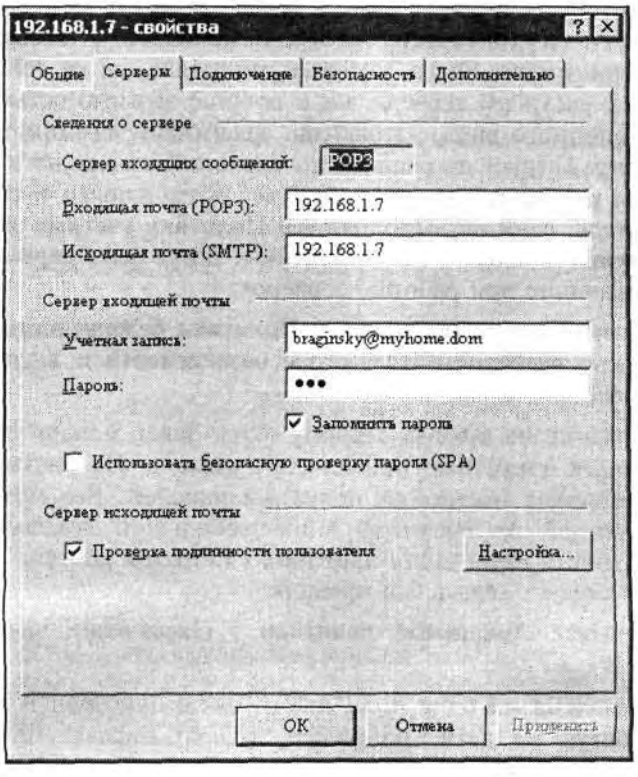


Рис. 9.10. Свойства учетной записи в Outlook Express

К сожалению, я не нашел способа, чтобы реанимировать службу POP3 после установки AD. Отправка писем по-прежнему работает, поскольку мы выбрали возможность анонимного использования нашего SMTP-сервера. Но POP3 теперь не позволяет выбрать вид аутентификации.

Единственный выход — переустановить эту службу. Причем переустановка требуется полная вместе с SMTP-сервером. После этого все работает в привычном для большинства пользователей варианте настроек (рис. 9.10).

Пользователи почтового сервера имеют возможность пересылать сообщения друг другу, но до регистрации доменного имени в Интернете они не смогут получать почту с внешних серверов. Тем не менее, отправлять почту на многие серверы, на которых не запрещено получение сообщений с незарегистрированных в Интернете серверов, возможность есть. Во всяком случае письма из моей домашней сети успешно принимаются почтовым сервером предприятия.

Политики

После установки AD на сервере многое изменилось. Учетные записи пользователей теперь имеют права, которые определяются не только возможностью доступа к ресурсам сервера, но и вообще возможностью использовать пароли определенного вида, условиями, заданными администратором домена. Зарегистрированный на сервере пользователь может не иметь доступа к тем или иным ресурсам, а иногда не будет возможности и самой регистрации пользователя, если не выполняются **Политики учетных записей** или **Локальные политики домена**. В этих политиках могут быть скрыты многие проблемы, возникающие при работе с сервером.

Давайте откроем **Администрирование | Политики безопасности домена**. В открывшемся окне развернем **Параметры безопасности** и выделим **Политика паролей** (рис. 9.11).

Обратите внимание на правую сторону окна. Здесь можно указать свойства паролей, которые допустимо применять в домене. На рисунке показан самый мягкий вариант настройки политики паролей. Его можно применять для изолированной от внешнего мира небольшой локальной сети. Чем больше вероятность несанкционированных попыток доступа к сети, тем более жесткими следует делать эти правила.

Теперь разверните **Локальные политики | Назначение прав пользователя** (рис. 9.12).

Здесь не определена ни одна политика. Можно определить эти политики и разрешить доступ из сети, например, только определенным категориям пользователей. А можно, наоборот, запретить локальный вход в систему всем кроме администратора. Для определения политики следует ее выделить и открыть (пункт **Свойства** в контекстном меню) (рис. 9.13).

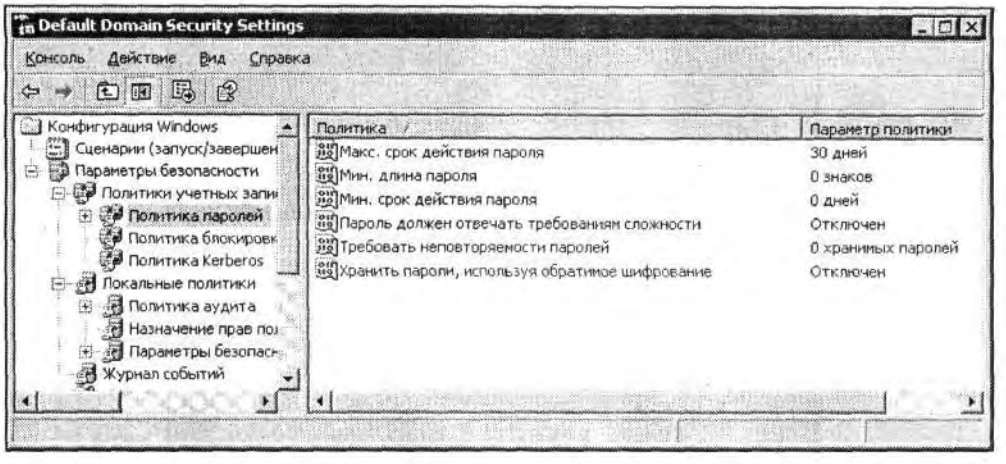


Рис. 9.11. Окно **Default Domain Security Setting** (параметры безопасности домена)

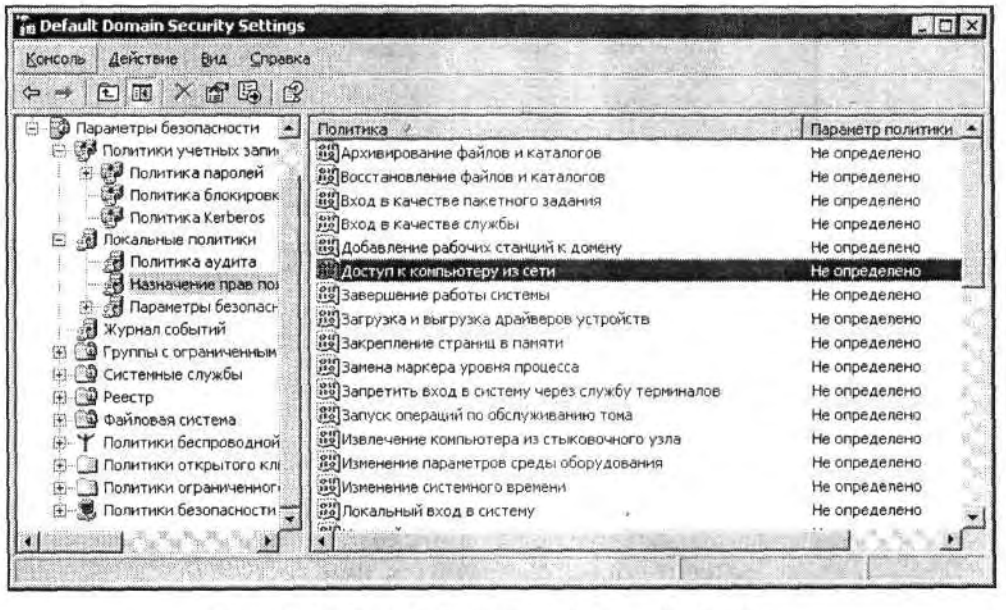


Рис. 9.12. Окно **Default Domain Security Setting** (назначение прав пользователей)

Нажав кнопку **Добавить пользователя или группу**, вы получите возможность выбрать из множества мест размещения учетных записей необходимую. Чаще всего такая учетная запись находится в контейнере **Users** (Пользователи) (см. рис. 9.9).

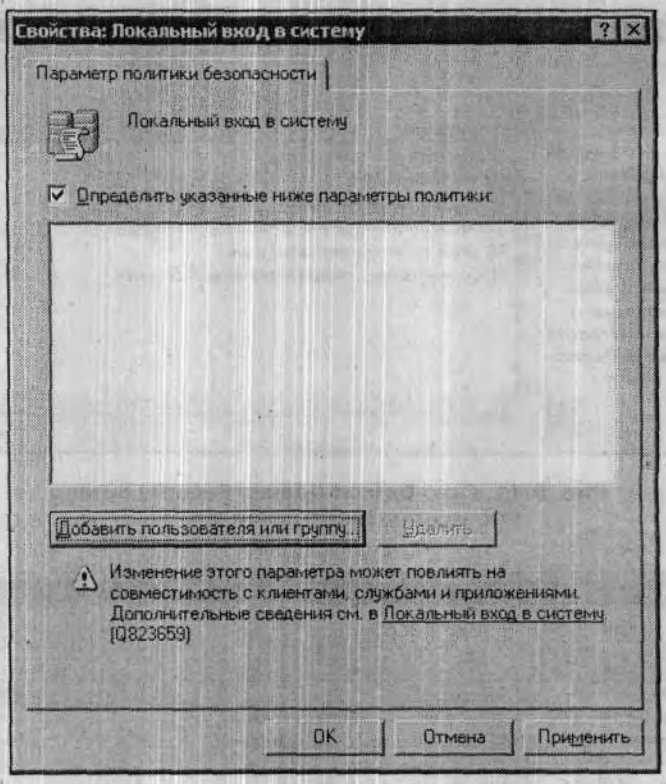


Рис. 9.13. Окно **Свойства: Локальный вход в систему**

Просматривая внимательно разнообразные политики домена, вы можете настроить сервер так, как это необходимо для вашей сети.

Добавление пользователей

Пользователи домена должны регистрироваться на сервере в AD. В отличие от одноранговых сетей, не обязательно создавать учетные записи пользователя на каждом компьютере сети, чтобы обеспечить к ним доступ. Достаточно дать учетной записи права на доступ к этому компьютеру. По умолчанию при регистрации компьютера в домене в числе его администраторов оказывается администратор домена. Администратор домена — это встроенная учетная запись. Большинство других учетных записей необходимо создавать, как и учетные записи почтовых пользователей. Создавая учетные записи, их можно систематизировать, помещая в контейнеры, которые могут иметь смысл подразделений или других организационных единиц. По умолчанию уже существуют контейнеры **Builtin** (Группы), **Computers** (Компьютеры), **Domain**

Controllers (Контроллеры домена), **ForeignSecurityPrincipal** (Объекты из других доменов), **Users** (Пользователи).

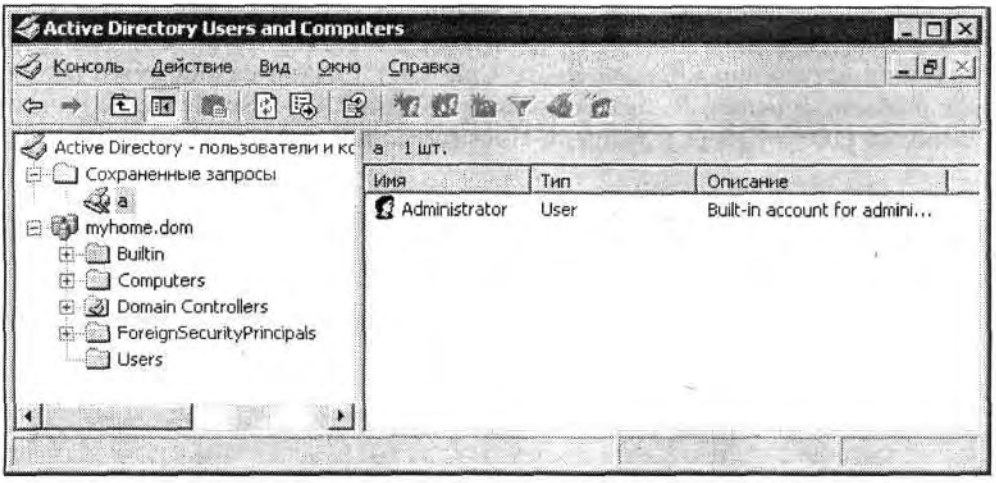


Рис. 9.14. Окно **Active Directory Users and Computers** (сохраненный запрос)

В дереве объектов AD есть еще одна интересная папка — **Сохраненные запросы**, которая может быть полезной при поиске учетных записей, когда их становится много (рис. 9.14). Администратору домена нередко приходится искать в AD учетные записи. Однажды выполненные условия поиска можно сохранить в папке **Сохраненные запросы**. При следующем аналогичном поиске не потребуется снова составлять условия запроса на поиск сведений. На рисунке показан сохраненный запрос для учетных записей, начинающихся на букву "A", имеющих тип **User**. Пока такая запись только одна. Интересно, что с помощью этого средства можно изменять свойства сразу многих объектов AD, найденных с помощью запроса. Мы рассмотрим эту процедуру несколько позднее.

Создание учетных записей пользователей почтового сервера происходит автоматически, когда вы создаете новый почтовый ящик. Другие учетные записи (или изменение существующих) приходится создавать вручную. Давайте создадим учетную запись рядового пользователя нашей сети. В отличие от учетных записей пользователей локальных компьютеров, в доменной учетной записи можно сохранять множество сведений различного характера. Иногда вместе с учетной записью пользователя приходится создавать и группу пользователей, члены которой должны обладать определенными правами. Но рассмотрим все по порядку.

Создадим учетную запись пользователя, который имеет постоянную обязанность — контролировать работу DHCP-сервера, корректировать настройки этого сервера при необходимости.

Открываем **Администрирование | Active Directory Users and Computers** (рис. 9.15). Для размещения всех созданных нами пользователей и групп создадим организационные единицы (Organizational Unit, OU). Создаются они точно так же, как и обычные папки. В данном примере создана OU — Family (семья) с вложенными OU — Groups (группы) и Users (пользователи).

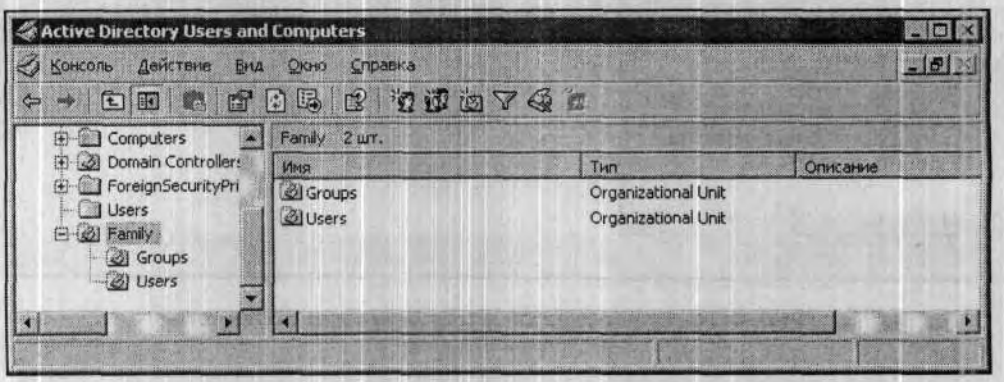


Рис. 9.15. Окно **Active Directory Users and Computers** (организационные единицы)

Новые организационные единицы позволят совершенно четко отделять созданные нами объекты от уже существующих в AD. Несмотря на то, что есть система поиска объектов по именам, нагляднее и удобнее работать с отдельными OU.

Перейдя в OU Users, вложенную в OU Family, создаем нового пользователя (User). При этом откроется окно, показанное на рис. 9.16.

Заполняем все поля формы. Некоторые поля заполняются автоматически, но вы можете изменить созданные автоматически записи. Нажав кнопку **Далее**, перейдем в следующее окно (рис. 9.17).

В этом окне создаем пароль пользователя. Обязательно обратите внимание на раскладку клавиатуры в этот момент — в поле ввода пароля символы не отображаются. Некоторые свойства пароля можно установить в этом же окне, отметив соответствующие опции. Можно также отключить учетную запись, если она создается заранее, например, и должна быть включена позднее.

Создан черновой вариант учетной записи. Теперь вызовите свойства новой учетной записи из контекстного меню ее значка.

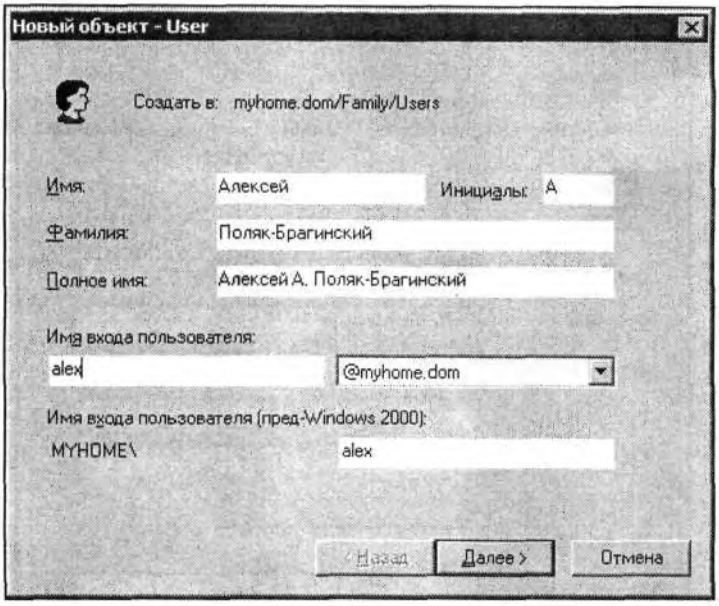


Рис. 9.16. Окно **Новый объект - User**

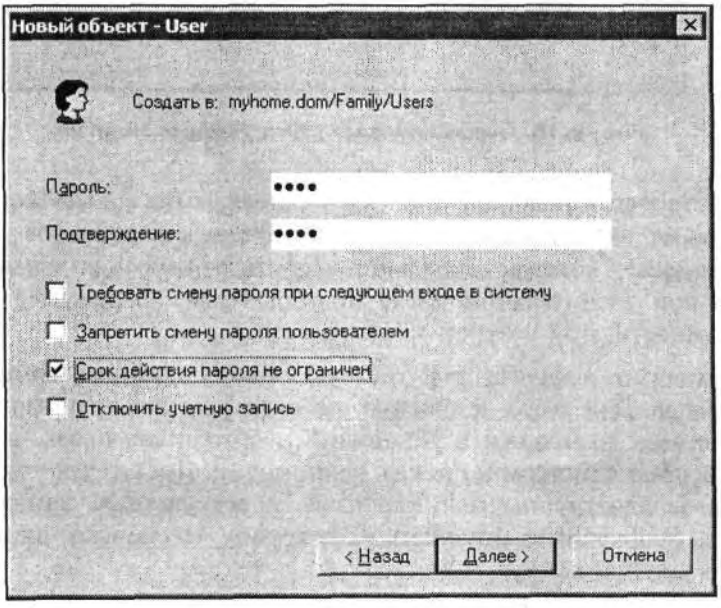


Рис. 9.17. Окно **Новый объект - User** (создание пароля)

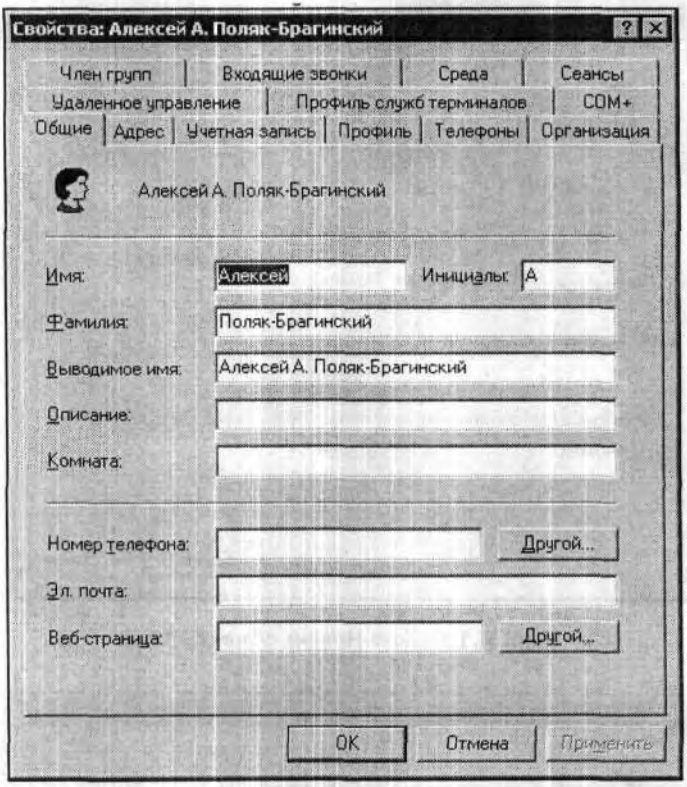


Рис. 9.18. Окно **Свойства: <Имя учетной записи>**

Окно свойств учетной записи (рис. 9.18) содержит несколько вкладок, которые позволяют внести в свойства много полезных параметров. Это и контактные данные, которые могут понадобиться вам, как администратору (особенно при значительном числе пользователей), и данные, определяющие возможности этой учетной записи в сети.

Нам необходимо наделить эту учетную запись правами администратора DHCP-сервера. Для этого, к счастью, не надо рассматривать политики сервера, выискивая возможности установить необходимые права, но не допустить присвоения слишком широких полномочий. Достаточно один раз установить права для группы пользователей, и все учетные записи, которым такие права необходимы, помещать в эту группу. Несколько таких групп уже создано по умолчанию.

Перейдите на вкладку **Член групп** (рис. 9.19). Нажмите кнопку **Добавить**. В открывшемся окне **Выбор: "Группы"** нажмите кнопку **Дополнительно**. В развернувшемся окне **Выбор: "Группы"** нажмите **Поиск** (рис. 9.20).

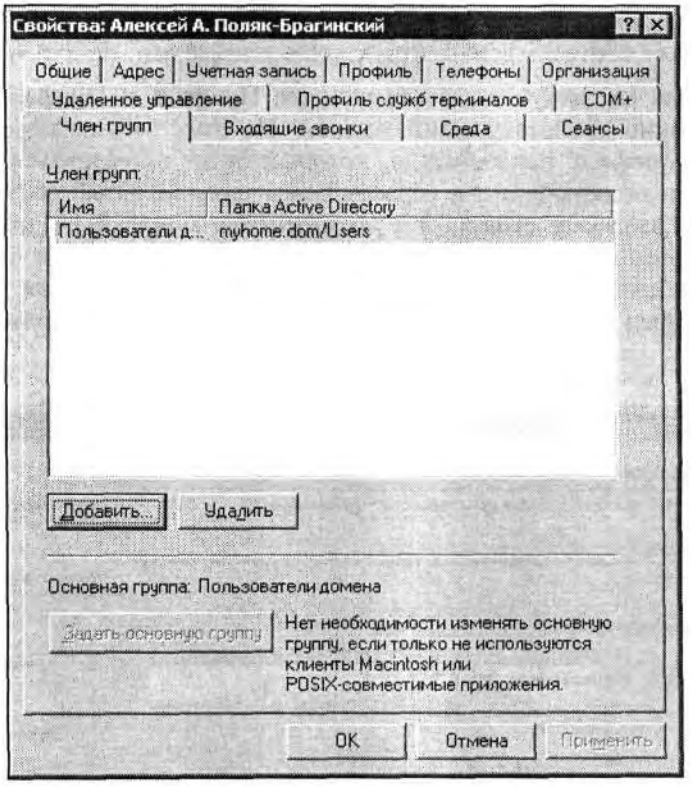


Рис. 9.19. Окно **Свойства: <Имя учетной записи>** (добавление в группу)

В появившемся списке уже существующих групп найдите **Администраторы DHCP**. Выделите ее мышью и нажмите **OK**.

В свернутом варианте этого окна появится имя выбранной группы в поле для ввода имен объектов (рис. 9.21). Нажав еще раз **OK**, мы добавим имя выбранной группы в окно свойств учетной записи. Теперь, нажав кнопку **Применить**, мы, наконец, добавим нашу учетную запись в выбранную группу.

Для наделения пользователя другими правами можно так же создать соответствующие группы и поместить в них его учетную запись.

Значительное число действий, которые требуются для изменения прав учетной записи, дают возможность администратору обнаружить свою ошибку на каком-либо этапе и отменить неверные действия.

Организационные единицы, которые мы создали перед учетной записью пользователя, не влияют на какие-либо свойства учетной записи. Они по-

зволяют организовать все объекты Active Directory в понятную структуру, которая может соответствовать структуре организации, использующей сеть.

Важными для вас могут оказаться вкладки **Профиль** и **Профиль служб терминалов** в окне свойств учетной записи. На этих вкладках можно указать сведения о профиле пользователя, который будет применяться при входе в сеть или при подключении к серверу через терминальный доступ (доступ к удаленному рабочему столу). Эта возможность может быть полезна, когда для определенной учетной записи необходимо установить не только права, но и вид рабочей среды — рабочий стол, программа, которая должна быть запущена перед началом работы, сетевые диски, которые должны подключаться.

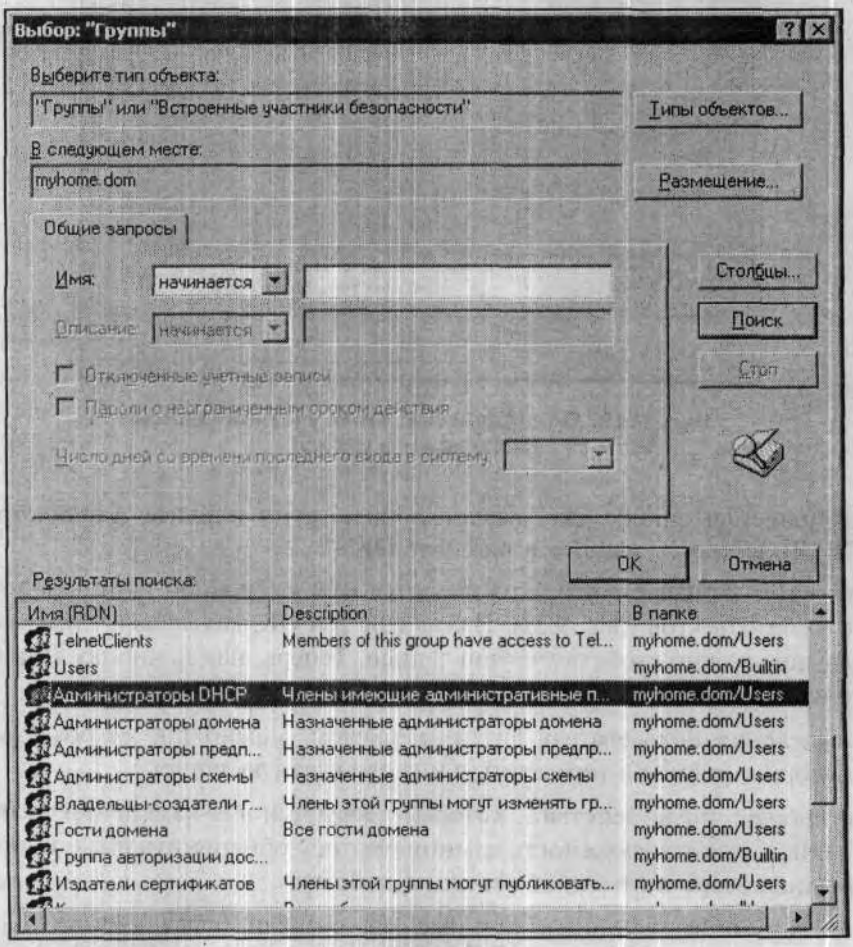


Рис. 9.20. Окно **Выбор: "Группы"**

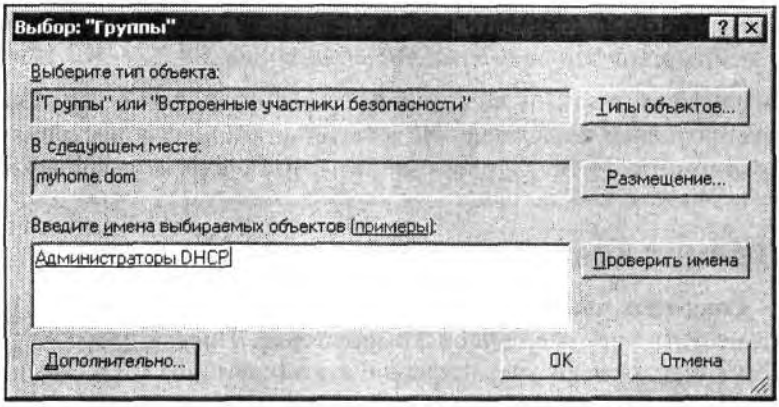


Рис. 9.21. Окно **Выбор: "Группы"** (свернутый вариант)

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 сохранить вид рабочего стола в неизменном виде при каждом входе пользователя в сеть. Добавление к профилю HTML-страницы позволит передавать пользователям необходимую информацию в текстовом и графическом виде и ссылки на файлы, расположенные в сети, для обеспечения их загрузки или выполнения. Конечно, "продвинутые" пользователи могут попытаться нарушить 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 не трудно. 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 мо-

мент могут закрыть лишние элементы рабочего стола, но при следующей загрузке компьютера эти элементы появятся вновь.

Профиль служб терминалов аналогичен сетевому профилю пользователя, но настраивается только на сервере. На рабочей станции для настройки профиля сервера терминалов не потребуется выполнять дополнительных действий.

Регистрация компьютеров

В папке **Computers** окна **Active Directory Users and Computers** (рис. 9.22) можно поместить учетные записи компьютеров. Правда, реально действующими могут быть только учетные записи компьютеров с ОС не ниже Windows 2000.

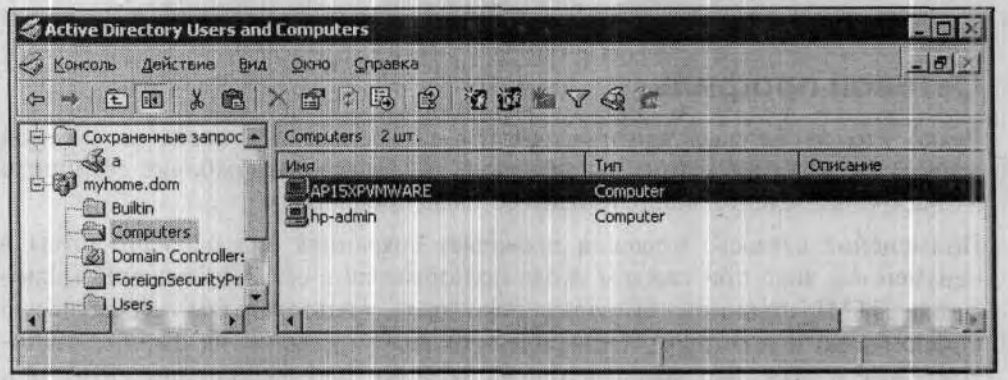


Рис. 9.22. Окно **Active Directory Users and Computers** (Computers)

Создаются учетные записи компьютеров обычно автоматически при подключении нового компьютера к домену. Как и учетные записи пользователей, учетные записи компьютеров имеют целый ряд свойств, среди которых нас может особенно заинтересовать **Член групп**. Это свойство устанавливается на соответствующей вкладке окна свойств. Примечательно оно тем, что мы можем не пользователя, а саму рабочую станцию наделить определенными правами.

Ни в какой одноранговой сети такое не возможно даже в принципе. А здесь — введите ваш компьютер в группу администраторов домена, и тот, кто работает в сети с этой рабочей станции, автоматически получает дополнительные права.

Кроме того, выбрав в контекстном меню значка компьютера пункт **Управление**, вы получаете возможность управления компьютером, поскольку при

регистрации рабочей станции в домене, администратор домена становится автоматически администратором рабочей станции.

Надо только иметь в виду, что все эти возможности доступны, когда рабочие станции имеют профессиональные версии операционной системы. Windows XP Home Edition, например, не позволяет включить рабочую станцию в домен.

Но и компьютеры с профессиональными версиями ОС не обязательно включать в состав домена. Например, мой ноутбук входит в домен сети предприятия. Приходя домой, мне нет необходимости регистрировать свой компьютер в домене домашней сети. Для получения доступа к большинству ресурсов достаточно указать учетные данные пользователя, которому разрешен к ним доступ. В отдельных случаях нужно войти в сеть, запустив сеанс сетевого пользователя. Если это сеанс администратора домена, то со своего компьютера можно получить доступ к управлению любым компьютером сети, подключенным к домену.

Регистрация других объектов

Одно из распространенных устройств, применяемых в сети, — принтер. Для сети не имеет значения, какого типа этот принтер, но важно, что он может быть доступен с любой рабочей станции. Сама процедура подключения принтера, находящегося в сети, к рабочей станции проблем не вызывает. Обычные пользователи сети имеют право выполнять печать на сетевых принтерах, а управлять принтером может администратор домена, администратор печати и администратор компьютера, к которому подключен принтер. Можно опубликовать принтер в Active Directory (рис. 9.23).

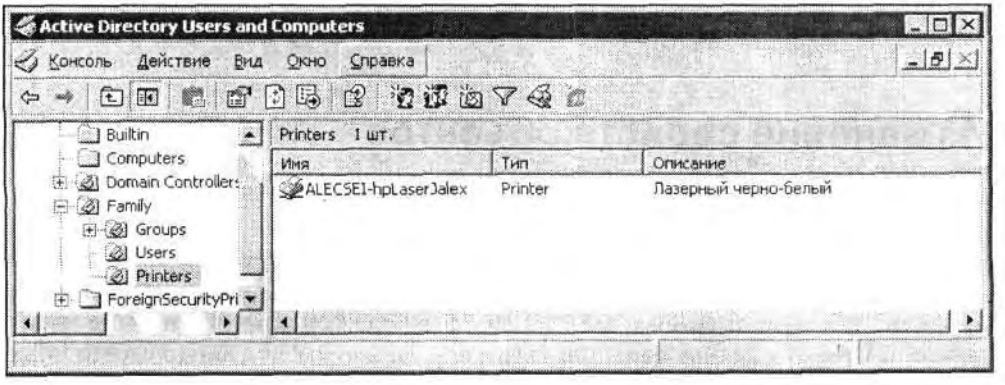


Рис. 9.23. Окно **Active Directory Users and Computers** (Printers)

Опубликовав принтер в Active Directory, вы сможете назначать права для управления данным принтером отдельным пользователям. Для этого достаточно открыть окно свойств объекта "принтер" и назначить управляющего (рис. 9.24).

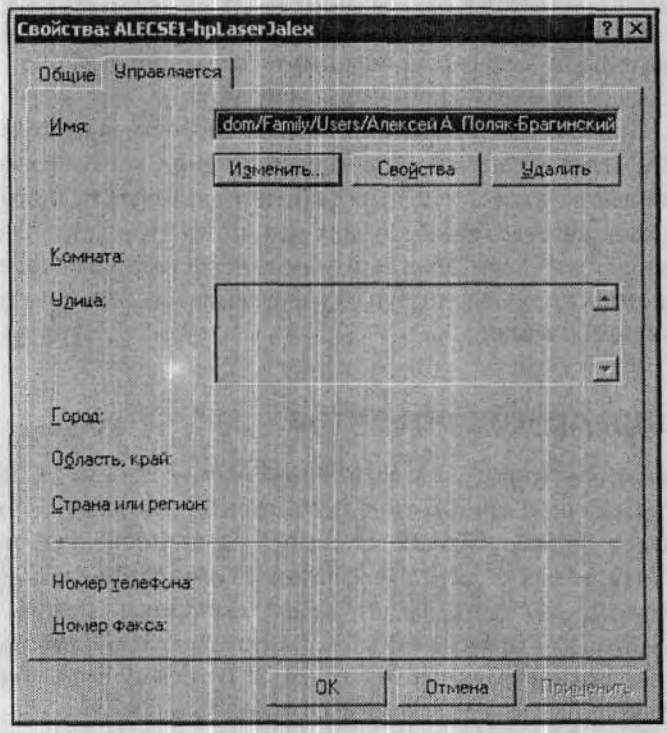


Рис. 9.24. Окно **Свойства: <Имя принтера>**, вкладка **Управляется**

Изменение свойств объектов

Ранее мы упоминали о том, что можно изменять свойства сразу нескольких объектов, входящих в Active Directory. Это можно делать с помощью сохраненных запросов. На рис. 9.25 показан сохраненный запрос **Пользователи**, в котором определяющим поиск полем стало поле **City** (Город) в адресе пользователя. Для всех пользователей из этого города (конкретное имя не имеет значения) было решено ограничить период возможной работы в сети. Выполнив созданный или измененный запрос, мы получили его результат в правой части окна.

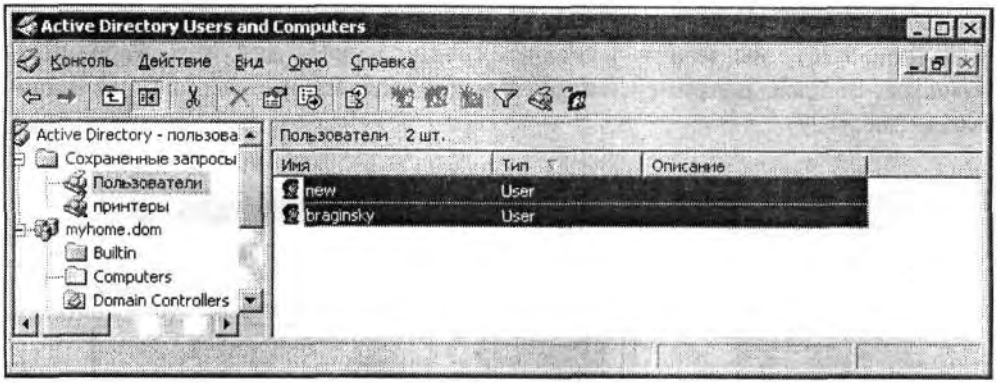


Рис. 9.25. Окно **Active Directory Users and Computers** (сохраненный запрос **Пользователи**)

Теперь, удерживая клавишу <Shift>, выделяем все найденные записи.

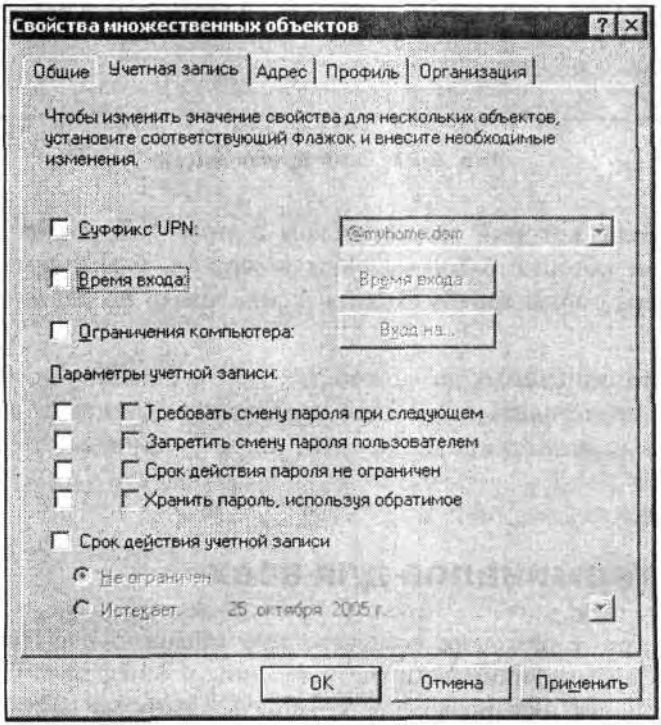


Рис. 9.26. Окно **Свойства множественных объектов**

Выбрав в контекстном меню всего выделенного блока записей пункт **Свойства** (рис. 9.26), мы можем изменять свойства сразу для всех выбранных объектов. Выбрав, например, опцию **Время входа**, мы попадем в окно **Время входа** (рис. 9.27).

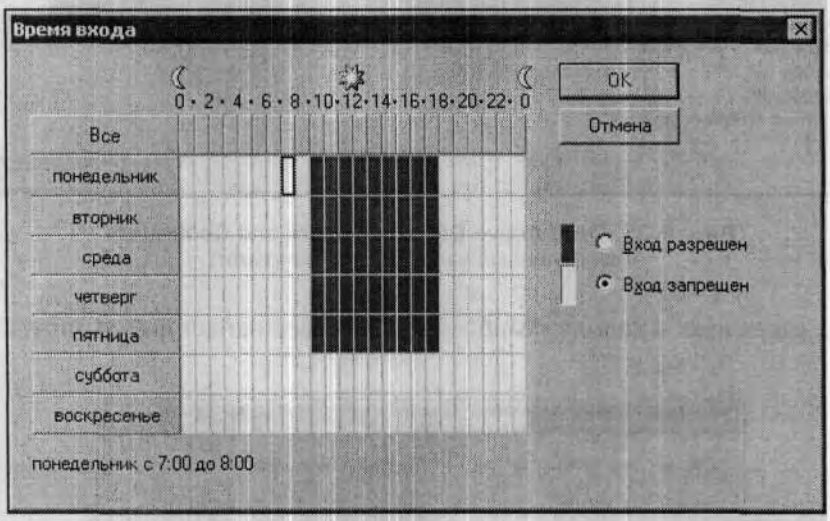


Рис. 9.27. Окно **Время входа**

Тот режим входа, который мы установим в этом окне, будет применен ко всем объектам, которые были выбраны в запросе. Обе учетные записи из нашего примера смогут теперь входить в сеть только по рабочим дням в рабочее время.

Я надеюсь, что описанных возможностей Active Directory достаточно, чтобы вы могли представить потенциал управления объектами в нем и осознать удобства администрирования сети, когда установлен этот компонент сервера.

Сервер терминалов для всех

Вернемся еще раз к разговору о сервере терминалов. Active Directory позволяет надежно идентифицировать учетные записи, определяя для них строго необходимые права. Это позволяет разрешить работу на одном компьютере нескольким пользователям. В прошлой главе мы уже говорили об этом сервере, рассматривали возможности подключения к нему. Но по умолчанию данный сервер позволяет подключаться не более двоим пользователям, да и

то отнесенным к группе администраторов сервера. Просто разрешить работать в удаленном режиме пользователю со слабым компьютером мы не можем. Но, приобретя дополнительные лицензии на сервер терминалов, вы получите возможность обеспечить пользователям, не входящим в группу администраторов, возможность работы на нем в удаленном режиме.

Для того чтобы обеспечить клиентов постоянными или временными лицензиями, необходимо установить компонент ОС Windows Server 2003 — сервер лицензирования. Microsoft рекомендует устанавливать сервер лицензирования на другой компьютер. Но в нашем случае, когда сервер у нас может быть единственным, сервер лицензирования следует устанавливать на тот же компьютер, на котором установлен и наш сервер. Установка сервера лицензирования производится точно так же, как и установка любого компонента Windows.

Процедура лицензирования сервера терминалов многократно описана в Интернете на различных форумах, но и самостоятельное ее проведение не вызывает никаких затруднений. Подобно активации Windows, активация и лицензирование сервера терминалов могут быть проведены в автоматическом режиме.

В режиме сервера терминалов, когда удаленно могут подключаться несколько пользователей, следует помнить о проблемах совместной работы с приложениями. Установку всех приложений необходимо выполнять с помощью средства **Установка и удаление программ**. Некоторые приложения и утилиты могут запускаться при загрузке Windows. Необходимо внимательно проверить возможность многократного запуска этих приложений. Еще лучше исключить возможность многократного запуска программ, что позволит и сэкономить ресурсы сервера, и избежать программных конфликтов.

Важно иметь в виду и вопрос лицензирования приложений, работающих на сервере терминалов. Скорее всего, потребуются дополнительные лицензии для многопользовательского режима работы Microsoft Office и других программ.

Если вопросы лицензирования вами уже решены, то можно начинать работу с сервером терминалов. Вполне возможно, что после его установки вам не удастся подключиться к нему удаленно, даже если вы раньше подключались в режиме администрирования. Теперь каждый пользователь, имеющий право работы с сервером терминалов, должен входить в группу его пользователей. И более того, для самой этой группы необходимо установить соответствующее разрешение. И это касается абсолютно всех пользователей сервера, включая администраторов. Для того чтобы особенности работы на сервере терминалов в удаленном режиме стали более осязаемыми, немного отвлечемся и понаблюдаем за работой системного администратора.

Перезагрузка

Некоторое время назад мне пришлось настраивать сервер в удаленном режиме. Наличие доступа к удаленному рабочему столу делает такую работу достаточно обычной. Но отсутствие возможности нажать на кнопку <Reset> заставляет в такой ситуации работать осторожно, чтобы своими действиями не вызвать зависания компьютера или потери связи с ним. Почти все процедуры настройки были мне известны. Для исключения необходимости вставлять в дисковод диски дистрибутивы были записаны заранее на жесткий диск. При необходимости можно было совершенно безбоязненно перезагружать этот сервер и снова выполнять подключение к нему от имени администратора. В числе последних процедур была запланирована установка сервера терминалов. Когда все необходимые компоненты были установлены, для проверки возможности работы обычных пользователей в удаленном режиме была создана тестовая учетная запись пользователя сервера терминалов. В какой-то момент сервер сообщил мне, что параметры учетной записи изменены, но будут применены после очередного входа в систему. Я не обратил на это предупреждение особенного внимания, поскольку действительно были изменены параметры учетной записи администратора. Правда, насколько они изменились, я понял несколько позднее, когда действительно потребовался повторный вход в систему.

После завершения всех настроек для контроля их правильности следовало перезагрузить север и снова подключиться к нему с учетной записью обычного пользователя. Эта процедура прошла гладко, никаких проблем ни при подключении, ни при тестовой работе почти не возникло. В одном из каталогов на сервере лежал документ, бывший для меня шпаргалкой, в которой было перечислено все, что необходимо было сделать. Я решил еще раз взглянуть в него, чтобы убедиться, что работа завершена, но наткнулся на отсутствие доступа к каталогу, где находился документ. Ну так что ж, ничего страшного, сейчас "перевойду" на сервер с учетной записью администратора и просмотрю этот документ. Но не тут-то было. Попытка подключиться к серверу от имени администратора потерпела провал.

Как же так, думал я. Обычным пользователем вхожу, а администратора не пускают. Может быть, неправильно ввел пароль? Может быть, ошибка в имени пользователя или в имени домена? Нет. Все перепроверено — все данные учетной записи верны. В чем же дело?

Снова вхожу на сервер с тестовой учетной записью.

Прав тестовой учетной записи было достаточно, чтобы просматривать состав групп пользователей. Добравшись до группы **Remote Desktop Users**, члены которой имеют доступ к серверу терминалов в удаленном режиме, я обнаружил, что администратора в этой группе нет. А ведь предстояло через какое-то время создавать новые учетные записи, да и вообще, доступ к этому

серверу требовался довольно часто. Ну, думаю, вот так перезагрузился. Что ж теперь, ехать за тридевять земель, чтобы администратора в группу **Remote Desktop Users** включить?

Размышляя, не спеша снова пробираюсь по пунктам меню до **Active Directory — Пользователи и компьютеры**. В очередной раз удивляюсь, почему в русифицированной операционной системе пункт меню пишется по-русски, а открывающееся за этим пунктом окно имеет англоязычный заголовок **Active Directory — Users and Computers**? Не торопясь открывать бесполезное при работе с тестовой учетной записью окно, кликаю по пункту меню правой кнопкой... Ура! Как я мог забыть об этой чудесной возможности, которая есть в современных ОС Windows? В контекстном меню по-русски написано **Запуск от имени**.

Ну вот. Теперь нам не страшна ситуация, когда администратору не удается подключиться к серверу терминалов со своими учетными данными. А если вдуматься, так уж ли часто есть необходимость подключаться к серверу от имени администратора? Даже на своей рабочей станции я регистрируюсь с локальной учетной записью, а большинство сетевых операций выполняю от имени соответствующего пользователя. Никто не застрахован от попыток "доброжелателей" перехватить ваши пароли, особенно в тот момент, когда вы подключаетесь к серверу через Интернет. Конечно, канал связи с сервером терминалов хорошо защищен, но средства нападения все же обычно опережают средства защиты. Если вы входите в систему на сервере с учетной записью, которая не имеет достаточных прав, чтобы выполнить какие-нибудь деструктивные действия, то, скорее всего, у вас будет время на обнаружение попыток входа на сервер, если имя и пароль учетной записи будут раскрыты. Для этого достаточно иногда просматривать журнал безопасности системы, в котором по умолчанию отличаются события успешной регистрации в системе.

Интернет-подключение к удаленному рабочему столу

Вариант подключения к серверу терминалов, который был рассмотрен ранее, позволяет получать доступ к серверу, когда сервер и ваш компьютер находятся в одной локальной сети. Вполне возможно, что эта сеть виртуальная и объединяет ваши компьютеры через Интернет. Но это локальная сеть. Существует и другой способ подключения к рабочему столу вашего сервера. Этот способ отличается тем, что на компьютерах, с которых производится подключение, не требуется клиент сервера терминалов (нужен для ОС младше Windows XP) или Remote Desktop Connections (Удаленное подклю-

чение к Рабочему столу). Даже операционная система может отличаться от Windows. Подключение в этом случае осуществляется с помощью интернет-браузера. Вы можете использовать такой вариант подключения, когда необходимо получить доступ к удаленному серверу с чужого компьютера, подключенного к Интернету.

Более того, вы имеете возможность предоставить доступ к приложениям, установленным на сервере любым доверенным пользователям Интернета. Единственное условие, которое необходимо выполнить в этом случае, это наличие доступа к серверу из Интернета. Это условие легко выполнить, если подключение к Интернету осуществлено через ADSL-модем или выделенную линию. Важно, чтобы компьютер имел реальный IP-адрес в Интернете, пусть даже динамический. Но и без Интернета в локальной сети можно использовать интернет-подключение к рабочему столу для обеспечения доступа к приложениям на сервере клиентам, работающим на компьютерах с устаревшими или отличными от Windows операционными системами.

Для осуществления такого варианта подключения необходимо подготовить сервер. Это совсем не сложно, потому что все необходимое уже есть в составе операционной системы. Достаточно открыть апплет **Установка и удаление программ** и перейти к **Установке компонентов Windows**.

Примечание

Такая возможность есть и в ОС Windows XP.

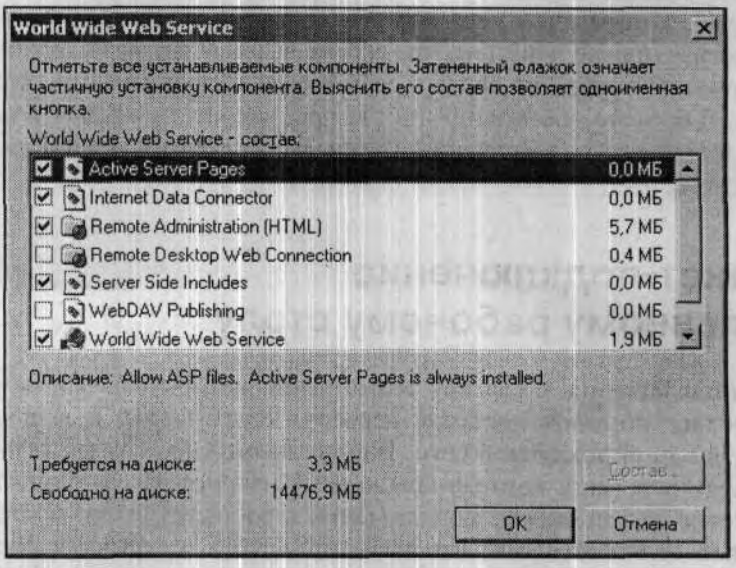


Рис. 9.28. Окно **World Wide Web Service**

Среди компонентов **Information Internet Services** (Информационные службы Интернета) есть **Remote Desktop Web Connection** (Инернет-подключение к удаленному рабочему столу). Установив этот компонент (рис. 9.28), вы обеспечите возможность подключения к серверу терминалов посредством браузера. При подключении, как положено, будет предложено авторизоваться в системе (рис. 9.29).

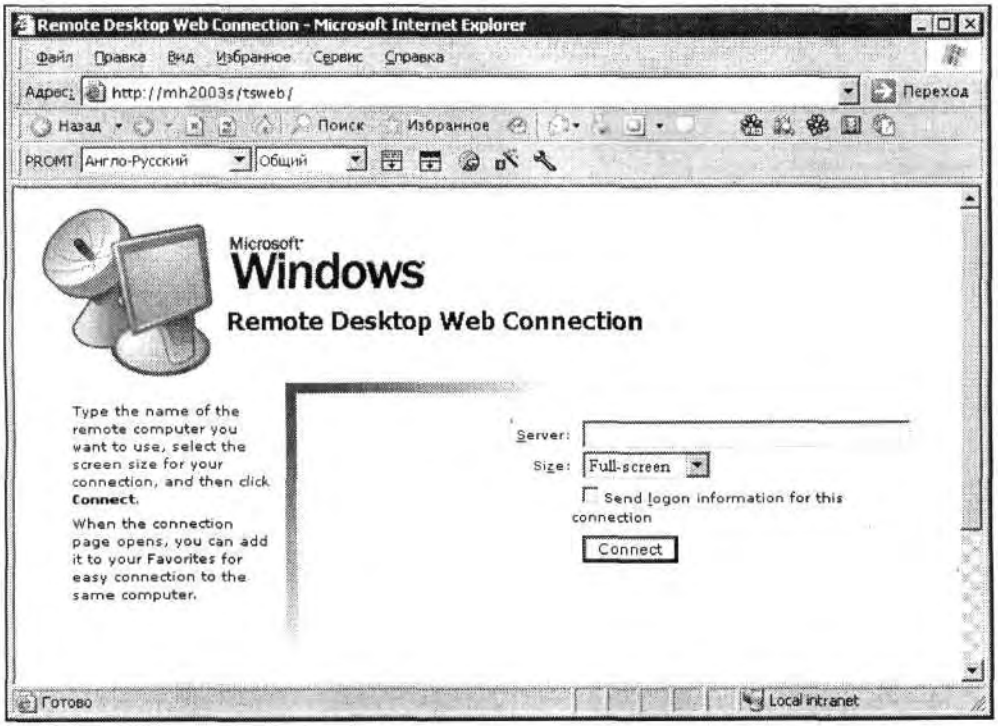


Рис. 9.29. Окно **Remote Desktop Web Connection** (авторизация)

А после установления соединения в окне браузера вы увидите рабочий стол сервера (рис. 9.30). При необходимости вы можете развернуть рабочий стол на полный экран.

Для подключения достаточно ввести в адресную строку браузера адрес вашего сервера, добавив к нему **/tsweb**. В отдельных случаях провайдеры доступа в Интернет закрывают наиболее используемые порты клиентов для доступа из Интернета. Применив маршрутизатор с настроенным перенаправлением портов или настроив это перенаправление на сервере, можно подключаться к серверу, используя другой порт, например, 9080. При этом

адрес для подключения будет выглядеть так: **http://<адрес сервера>:9080/tsweb/**. Но порт, используемый самой программой, должен быть стандартным (80).

По умолчанию файлы программы **Интернет-подключение к удаленному рабочему столу** находятся в каталоге %systemroot%\Web\Tsweb. В нем находятся и файлы default.htm и connect.asp, которые можно изменять по своему усмотрению, управляя дизайном страниц, сопровождающих процесс подключения (рис. 9.31).

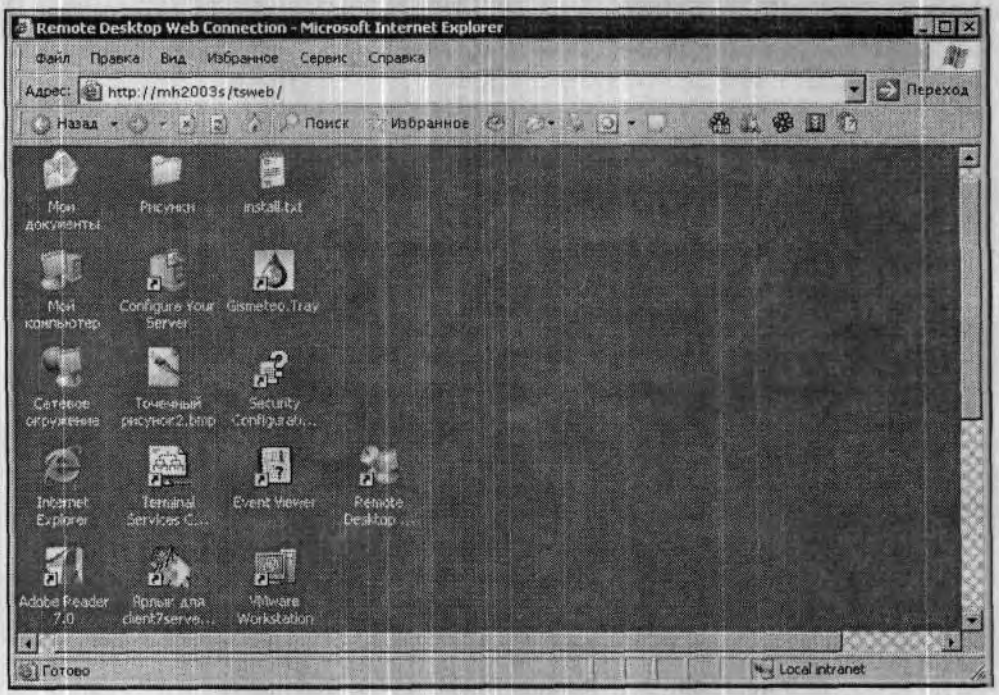


Рис. 9.30. Окно **Remote Desktop Web Connection** (соединение установлено)

Вы можете подключиться к этой странице, набрав в адресной строке браузера **http://okodox.webhop.net/tsweb**.

Примечание

Если подключение не удалось, попробуйте выполнить его позднее. При неудачном выходе из сеанса без его завершения он остается в неактивном состоянии на протяжении нескольких минут. В этот момент другое подключение может оказаться невозможным. В отличие от обычного подключения к серверу

терминалов, при интернет-подключении сервер не может отождествить последовательные попытки подключения одного клиента, считает их разными и не позволяет подключиться к неактивному сеансу.

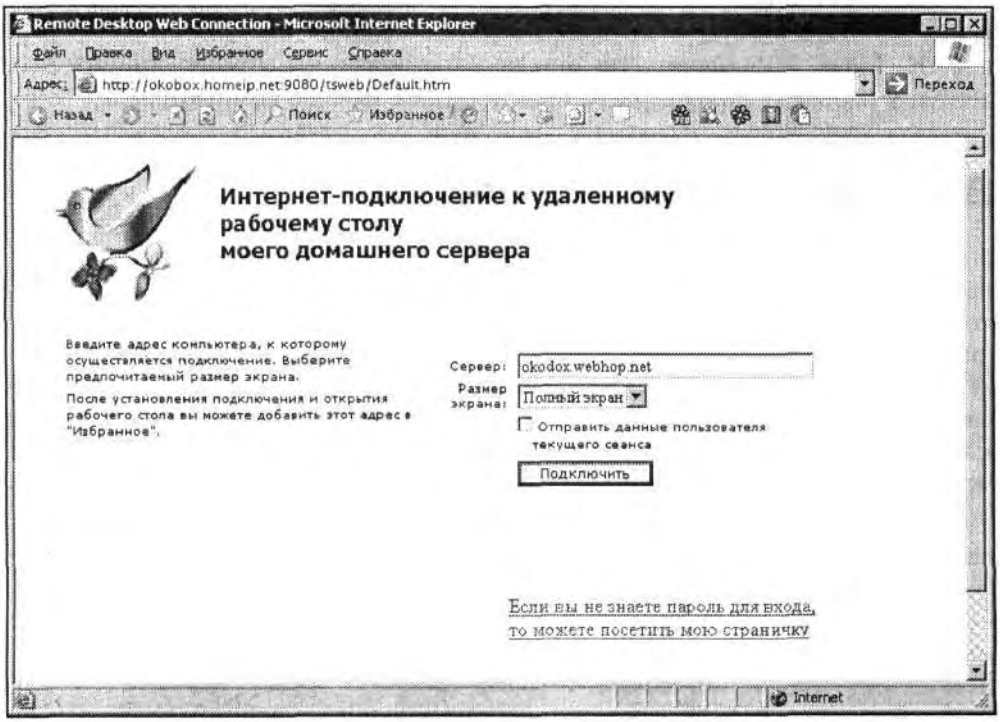


Рис. 9.31. Окно **Remote Desktop Web Connection** (отредактировано пользователем)

Чем этот способ лучше?

У вас может возникнуть вопрос — а почему нельзя просто подключиться к удаленному компьютеру, используя клиент терминального доступа?

У каждого решения всегда есть положительные и отрицательные стороны. Вот и у этого варианта подключения к удаленному рабочему столу есть преимущество в том, что клиент терминального доступа не нужен. Требуется только Internet Explorer, начиная с четвертой версии. Если вы уже попробовали подключиться к моему удаленному рабочему столу, то обратили, видимо, внимание на то, что имя сервера вводить не обязательно. При этом соединение все равно устанавливается. Все дело в том, что интернет-подключение к удаленному рабочему столу позволяет подключаться не только к

тому серверу, к которому есть доступ через Интернет. Другие рабочие столы могут быть подключены посредством сервера, с которым мы установили соединение через Интернет. Своего рода маршрутизация без маршрутизатора. К сожалению, с браузерами, отличными от Internet Explorer, такое подключение работать не будет. Но клиенты терминального доступа существуют и для ОС Linux. Это значит, что при необходимости вы можете организовать доступ к рабочему столу сервера практически с любого компьютера.

Возможные неисправности

Пожалуй, раз уж вы установили Active Directory, да настроили доступ к рабочему столу своего сервера, мы не будем рассматривать неисправности, которые для вас стали очевидными. Подсказки вроде "Убедитесь, что клиентский компьютер имеет активное подключение к сети и работает служба сервера WINS (или другой метод определения имен)" в изобилии встречаются в справочной системе. Но иногда появляются неисправности, причины которых не очень просто распознать. И они не связаны с банальным отключением патч-корда или программным отключением сетевого адаптера.

Тем не менее, прежде чем искать причины неполадок в AD или связанных с сервером терминалов, не забудьте проверить доступность серверов имен и "проходимость" коммутаторов и маршрутизаторов. Никто не застрахован от выхода из строя порта активного оборудования. При этом в системных сообщениях вы можете встретить очень грозные предупреждения, руководствуясь их описанием, можно, пытаясь настроить сервер, нарушить его работу окончательно, если устранять несуществующую причину проблемы. Во всяком случае перед решением проблемы, в причинах появления которой вы еще не разобрались, есть смысл использовать команду `ping` для того, чтобы убедиться в доступности серверов, отсутствие которых может повлиять на работу сети.

При недоступности DNS-сервера может не быть и терминального доступа, когда в параметрах подключения указывается имя сервера.

Вообще говоря, Windows Server 2003 — система очень устойчивая. В случае повреждения базы данных AD, сервер самостоятельно пытается восстановить ее, что в большинстве случаев заканчивается успешно. Но для того чтобы сервер имел возможность восстанавливаться, ему требуется дисковое пространство. Если вы пропустите момент переполнения диска, то неполадки в AD могут привести к полной неработоспособности сервера, и восстановление будет практически невозможно.

В небольшой сети нет необходимости создавать второй контроллер домена, особенно когда требования к отказоустойчивости сети не очень жесткие. В большинстве случаев восстановление сервера при серьезных сбоях может

быть выполнено из резервных копий. Создание резервных копий системы не рассматривается в этой книге, но Windows Server 2003, как и другие Windows, имеет в своем составе средства для создания таких копий в виде служебной программы *Архивация данных*.

Возможно применение программ сторонних разработчиков. Один из простых путей 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 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 копию 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.

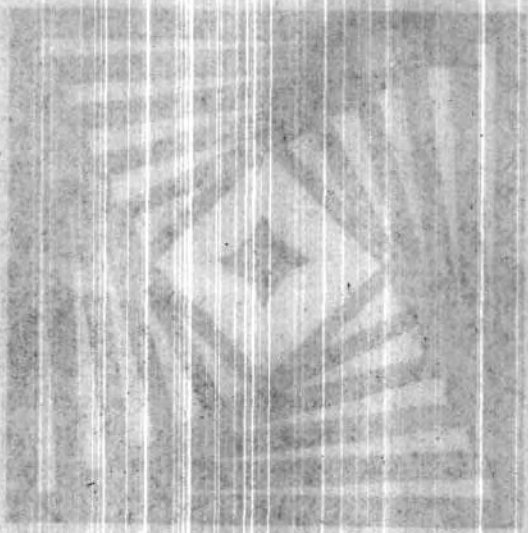
Применение этой программы позволяет оперативно восстановить работу сервера при выходе из строя винчестера.

Еще один способ обеспечить сохранность данных и быстрое восстановление сервера — это применение зеркальных томов. Для создания зеркальных томов необходимо иметь два одинаковых винчестера. Процедуры работы с зеркальными томами подробно описаны в справочной системе Windows.



ЧАСТЬ IV

РАСШИРЕНИЕ СЕТИ



Расширение сети — это не только добавление рабочих станций. Под расширением можно понимать и появление внешних связей. Например, связи с другими локальными сетями, с отдельными рабочими станциями в Интернете. Расширение сети может потребовать применения второго сервера. Чем следует руководствоваться при принятии решения о необходимости второго сервера? Необходимость во втором сервере может возникнуть при значительном расширении сети. Если сеть разрастается территориально, то возникают задачи репликации Active Directory на дополнительные контроллеры с целью ускорения доступа клиентов к ним. Крупные сети могут делиться на сайты, представляющие собой довольно условные структуры, связанные между собой относительно медленными каналами связи. Если не иметь доступную клиентам с учетными записями на каком-либо сайте копию базы данных Active Directory, то им придется обращаться к контроллеру, расположенному на другом сайте, через узкий канал связи, что серьезно замедлит работу сети.

Но нам пока такое расширение не грозит. И мотивы, которыми мы будем руководствоваться, будут иными.



Глава 10

Второй сервер

Каждый администратор стремится сделать свою сеть достаточно удобной для пользователей, простой в обслуживании и в то же время защищенной и безопасной. Особенно остро вопрос защищенности сети встает при подключении сети к Интернету и предоставлении пользователям возможности работать на компьютерах сети через Интернет.

Иногда в сети достаточно давно работает сервер Windows 2000 Server, на котором расположены Active Directory, сетевые приложения, файловые архивы. Подключать напрямую такой сервер к Интернету, с одной стороны, рискованно с точки зрения безопасности сети, а с другой — он может не справиться с дополнительными обязанностями ввиду недостатка производительности или объема памяти. Вероятно, вы захотите организовать дополнительно и контроль трафика Интернета для упорядочивания использования информации из глобальной сети пользователями. Такой контроль в удобном для администратора варианте может быть организован с применением дополнительного программного обеспечения, которое может создать весьма ощутимую дополнительную нагрузку на сервер.

Эти соображения и позволяют принять решение об установке второго сервера. Через него будет организовано подключение к Интернету, и на нем будут работать дополнительные сервисы, которые помогут организовать не только выход в Интернет для локальной сети, но и удобную связь с какой-либо другой сетью, а также возможность подключения к вашей сети из Интернета. Если пользователям сети это пока не требуется, то вы, как администратор, сможете быстро оценить те преимущества, которые вам даст организация двухсторонней связи между домашним компьютером, например, и вашей сетью.

Для того чтобы описанные возможности были доступны, необходимо организовать доступ в Интернет для сети через второй сервер. Пример, который будет рассматриваться далее в этой главе, ориентирован на подключение через ADSL-модем, но практически не будет отличий для подключения по

выделенной линии. Применять коммутируемый доступ в данном случае не рекомендуется. Если для организации общего доступа в Интернет коммутируемый доступ вполне применим (с учетом ограничений по скорости связи), то для двухсторонней связи проблем возникает больше, чем удобств, приносимых ею.

При подготовке этого примера я исходил из предположения, что у вас уже работает сервер на основе Windows 2000 Server. Таких сетей в настоящее время много, если не большинство. Это связано с тем, что при появлении Windows Server 2003 не многие администраторы решились переходить на новую операционную систему, не обнаружив в ней явных преимуществ для небольшой изолированной локальной сети. И при создании новых сетей администраторы, ориентируясь на имеющийся опыт, применяли Windows 2000 Server. Аналогичная ситуация была и после выхода Windows 2000 Server, когда администраторы старой закалки продолжали использовать Windows NT. Надо сказать, что и в сетях, где мне самому приходилось работать, Windows 2000 Server не спешат заменять на Windows Server 2003, но, решив устанавливать второй сервер, выбор делают в пользу новой операционной системы.

Для определенности далее в этой главе второй сервер будем называть *интернет-сервер*. Сразу отметим, что на интернет-сервере должно быть установлено два сетевых адаптера — один для подключения к локальной сети, другой для подключения к ADSL-модему. Операционная система сервера, используемого в примере, полностью локализована для России.

Для обеспечения подключения любого пользователя необходимо соблюсти некоторые условия.

1. Если вы хотите, чтобы пользователь имел доступ к сервисам, предлагаемым во всемирной сети, следует в свойствах IP-протокола рабочих станций указать адрес второго сервера в качестве шлюза, а на самом интернет-сервере настроить NAT.
2. Установить на интернет-сервере второй DNS-сервер.
3. Если вы не хотите, чтобы вирусы и хакеры проникали в вашу сеть извне, необходимо установить брандмауэр — защитный экран, не позволяющий проникать в вашу сеть IP-пакетам, которые не были запрошены самой сетью.
4. На интернет-сервере желательно установить антивирусное программное обеспечение.

Если четвертое условие для выполнения требует приобретения программ от разработчиков антивирусов, то первые три выполняются средствами самой операционной системы.

Примечание

Учитывая, что сервер не должен использоваться в качестве рабочей станции, мала вероятность проникновения вирусов в его систему, когда работает брандмауэр. На одном из серверов, известных мне, не установлено антивирусное программное обеспечение. Через этот сервер большинство IP-пакетов проходит транзитом. Обычные пользователи имеют доступ к некоторым архивам, расположенным на сервере, но только для чтения. Тем не менее, один раз в месяц проводится обновление, предлагаемое Microsoft. При этом загружается программа, проверяющая наличие и уничтожающая, если будут обнаружены, самые злобные вирусы.

Начинается все с запуска мастера настройки маршрутизации и удаленного доступа. Эта процедура вам уже знакома. 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 не сложно. Войдите в **Панель управления**, откройте **Сетевые подключения** и переименуйте имеющиеся адаптеры, например, как на рисунке (рис. 10.1).

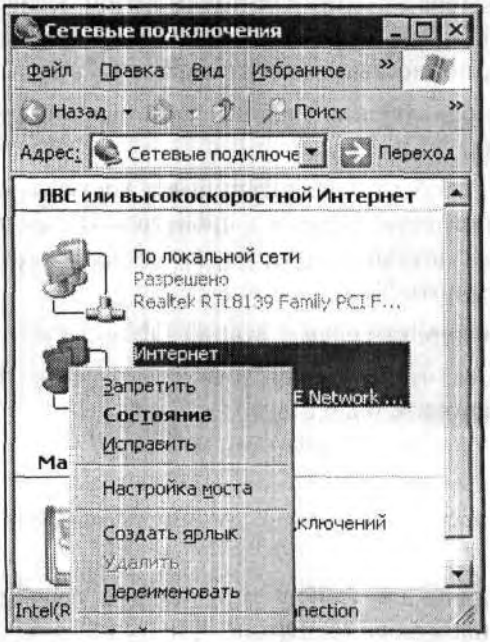


Рис. 10.1. Окно **Сетевые подключения** (переименование)

Один адаптер назовем "Интернет", а другой "По локальной сети". Посмотрите теперь в окно **Маршрутизация и удаленный доступ** (рис. 10.2). Перепутать интерфейсы сети при дальнейших манипуляциях будет невозможно.

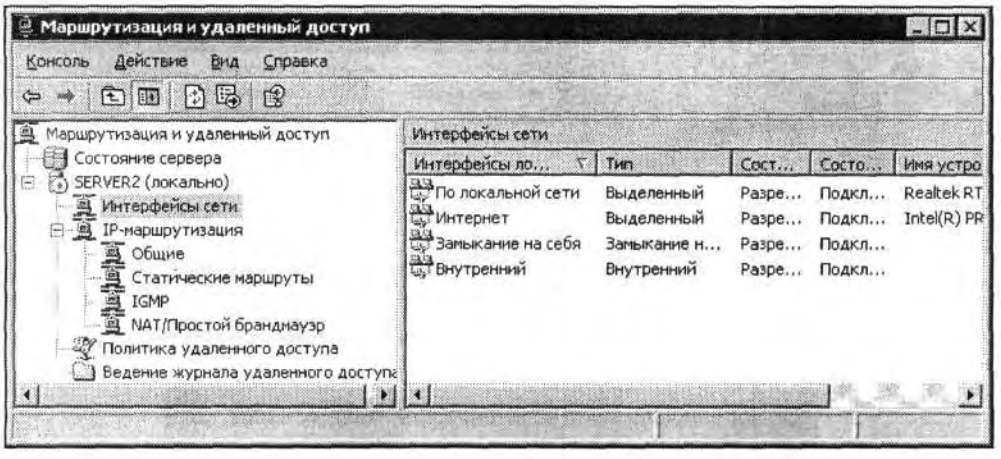


Рис. 10.2. Окно **Маршрутизация и удаленный доступ** (интерфейсы сети)

Вполне возможно, 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 окна **Маршрутизация и удаленный доступ** к **IP-маршрутизация | Общие** (рис. 10.3).

В свойствах интерфейсов, касающихся маршрутизации, видим IP-адреса, которые необходимо присвоить сетевым адаптерам. Провайдер при установке ADSL-модема выделяет вам не менее четырех IP-адресов. На самом деле из них можно реально использовать только один. Первый и последний адреса соответствуют адресам NNN.NNN.NNN.0 и NNN.NNN.NNN.255 при маске подсети 255.255.255.0. Но вам выделен диапазон адресов с маской NNN.NNN.NNN.252. В случае, показанном в примере, это сеть 81.195.117.136/30, в которую входят четыре адреса: 81.195.117.136, 81.195.117.137, 81.195.117.138, 81.195.117.139. Первый и последний для интерфейсов не применимы, второй используется для ADSL-модема, третий можно присвоить сетевому адаптеру, смотрящему в Интернет. Возможно, что вы закажете большее число адресов, тогда их диапазон будет шире, но первый и последний адреса диапазона применить все равно нельзя, а один адрес необходимо отдать ADSL-модему. Рассмотрим свойства интерфейсов последовательно.

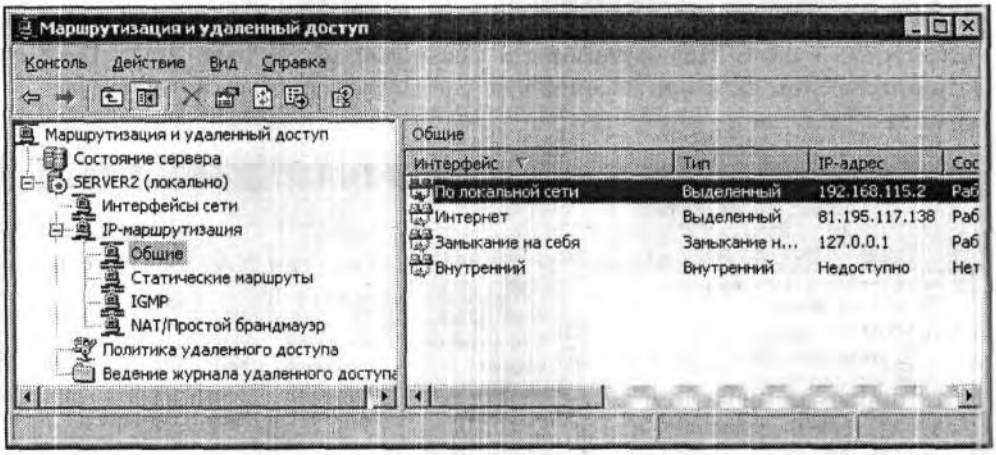


Рис. 10.3. Окно **Маршрутизация и удаленный доступ** (IP-маршрутизация, общие)

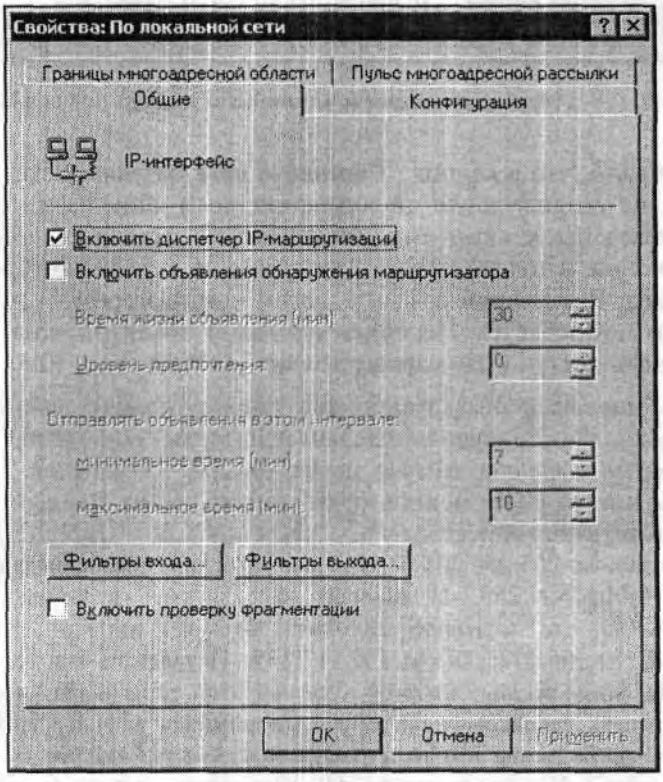


Рис. 10.4. Свойства интерфейса **По локальной сети**, вкладка **Общие**

В свойствах интерфейса **По локальной сети** на вкладке **Общие** (рис. 10.4) должен быть выбран флажок **Включить диспетчер IP-маршрутизации**. Тот же флажок должен быть выбран и в свойствах второго интерфейса.

Перейдем на вкладку **Конфигурация** (рис. 10.5). 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.

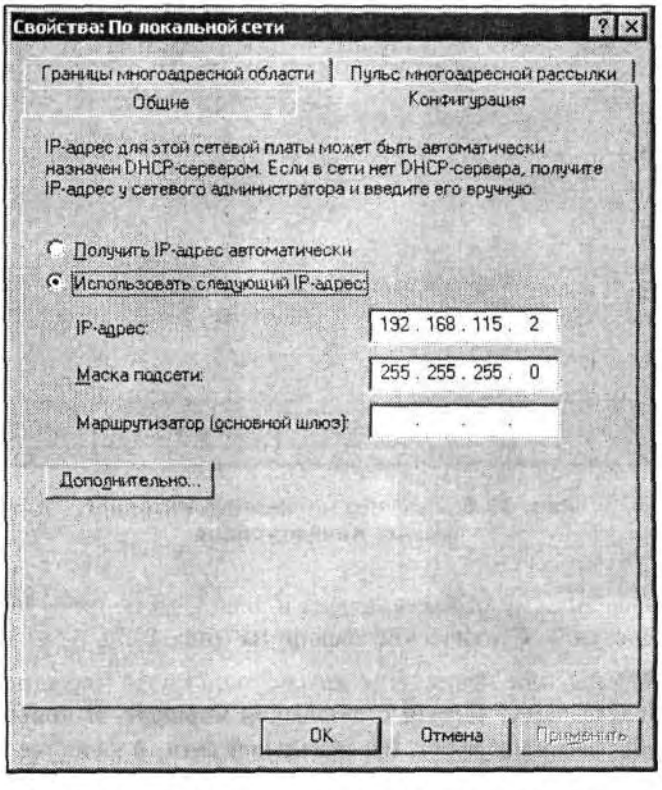


Рис. 10.5. Свойства интерфейса **По локальной сети**, вкладка **Конфигурация**

Для интерфейса **Интернет** (рис. 10.6) необходимо указать IP-адрес, который будет виден из Интернета. В данном случае это единственно возможный вариант — 81.195.117.138, маска подсети — 255.255.255.252. В качестве маршрутизатора (основного шлюза) указываем адрес ADSL-модема, поскольку именно через него будет осуществлен выход в Интернет.

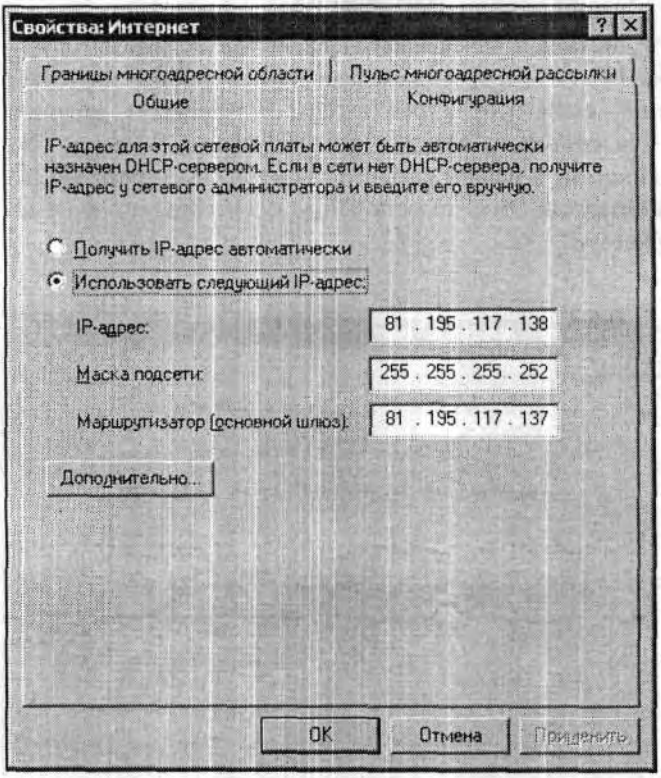


Рис. 10.6. Свойства интерфейса **Интернет**, вкладка **Конфигурация**

Перейдем к следующему объекту дерева в левой части окна **Маршрутизация и удаленный доступ — Статические маршруты** (рис. 10.7).

Если не назначены или назначены другие маршруты, находим в контекстном меню объекта пункт **Новый статический маршрут**. В появившемся окне (рис. 10.8) выбираем интерфейс **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, менять это значение не следует.

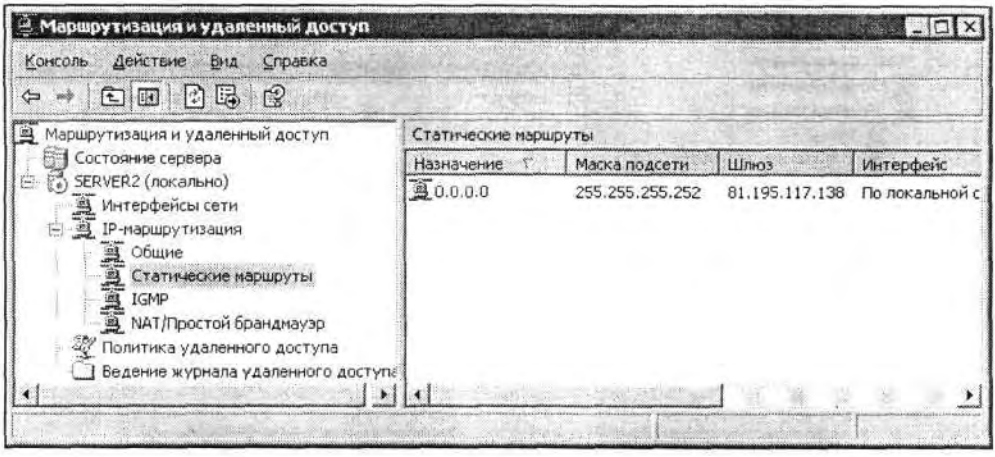


Рис. 10.7. Окно **Маршрутизация и удаленный доступ** (статические маршруты)

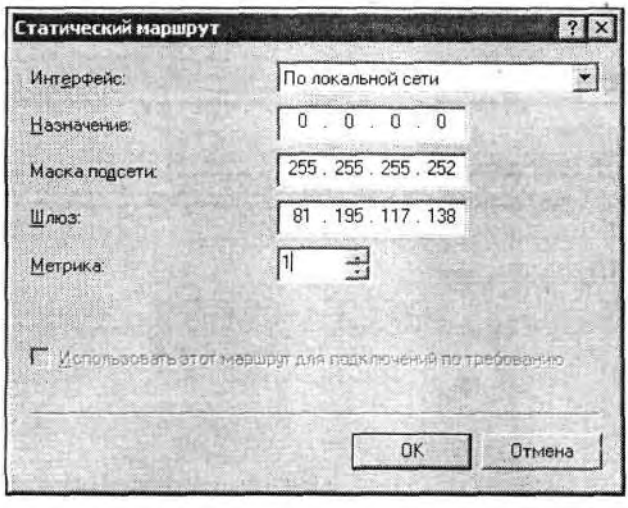


Рис. 10.8. Окно **Статический маршрут**

Следующий объект — IGMP (Internet Group Management Protocol, протокол управления группами Интернета). В этом объекте (рис. 10.9) должны быть указаны роли интерфейсов. Интерфейс **Интернет** находится в роли маршрутизатора, а **По локальной сети** — в роли доверенного интерфейса (прокси).

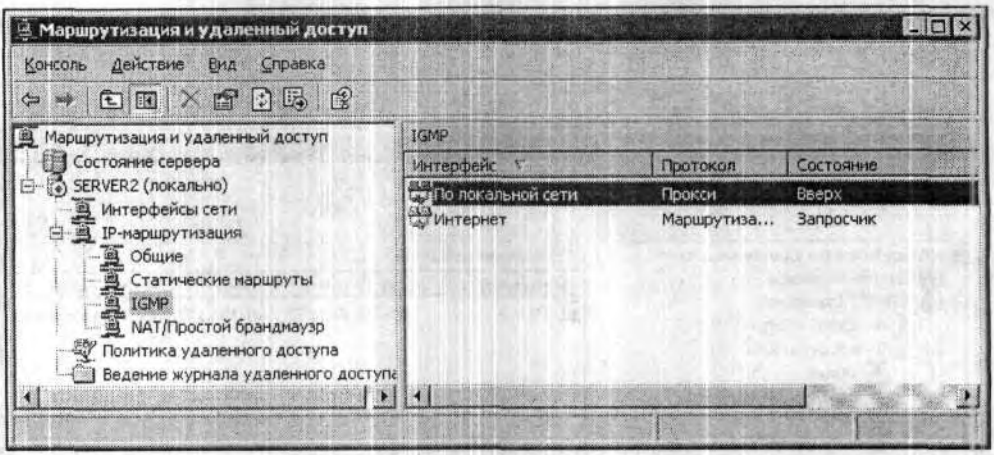


Рис. 10.9. Окно **Маршрутизация и удаленный доступ** (IGMP)

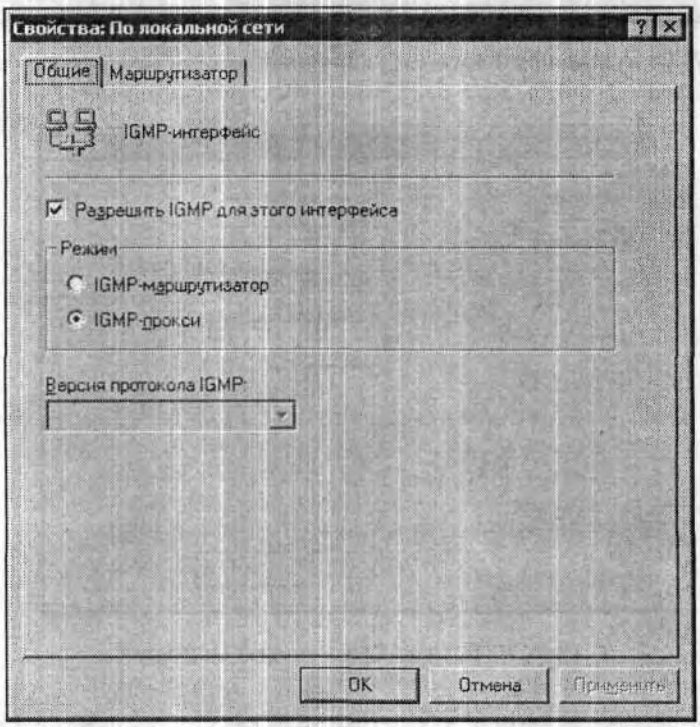


Рис. 10.10. Объект **IGMP**,
свойства интерфейса **По локальной сети**,
вкладка **Общие**

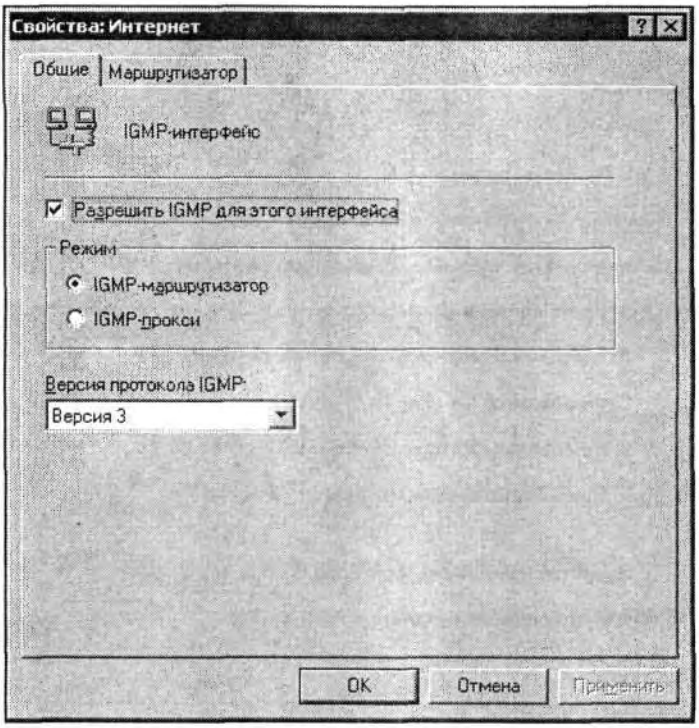


Рис. 10.11. Объект **IGMP**, свойства интерфейса **Интернет**, вкладка **Общие**

Если это не так, откройте свойства интерфейсов в этом объекте и установите необходимое (рис. 10.10 и 10.11).

Для обоих интерфейсов должен быть отмечен 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. 10.12) по умолчанию устанавливаются еще несколько параметров. Без необходимости их изменять не следует.

И, наконец, объект **NAT/Простой брандмауэр** (рис. 10.13). 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. 10.14).

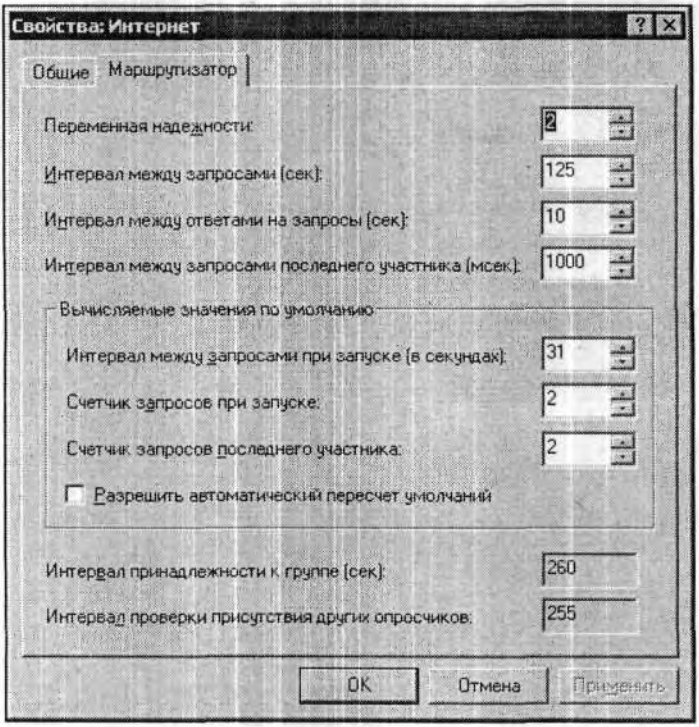


Рис. 10.12. Объект **IGMP**, свойства интерфейса **Интернет**, вкладка **Маршрутизатор**

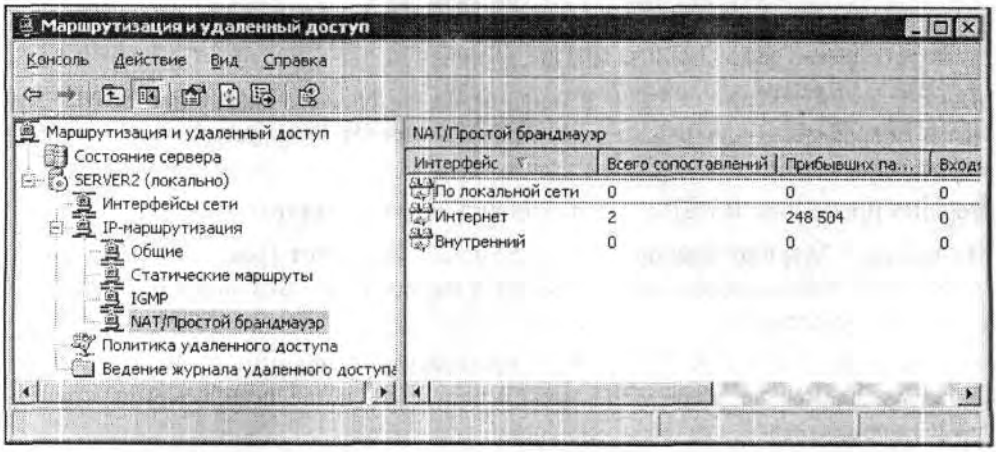


Рис. 10.13. Окно **Маршрутизация и удаленный доступ** (NAT/Простой брандмауэр)

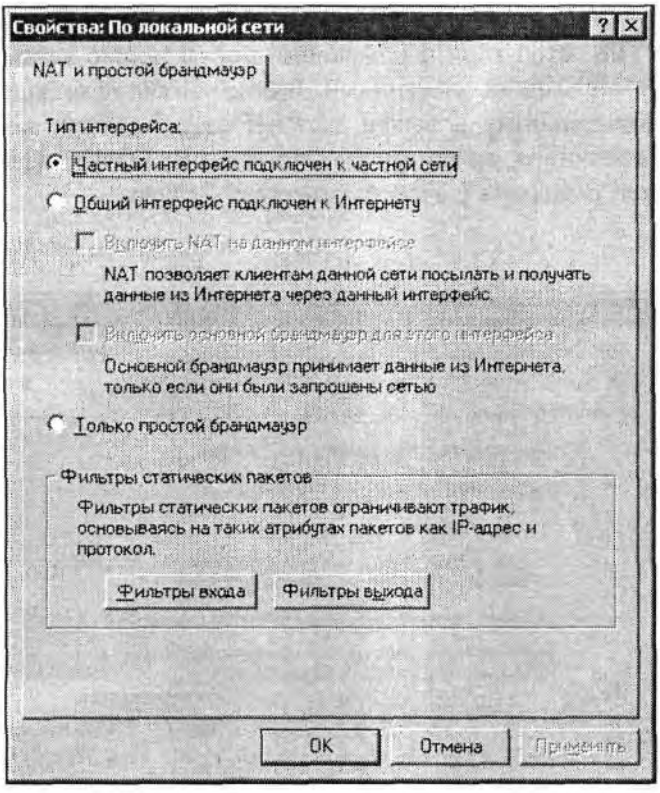


Рис. 10.14. Объект **NAT/Простой брандмауэр**, свойства интерфейса **По локальной сети**

Для интерфейса **Интернет** (рис. 10.15) должны быть отмечены — **Общий интерфейс подключен к Интернету**, **Включить NAT на данном интерфейсе**, **Включить основной брандмауэр для этого интерфейса**.

На вкладке **Службы и порты** (рис. 10.16) 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 — окно в вашу сеть. Через эти порты в сеть могут проходить пакеты, не запрошенные из нее.

Порты можно добавлять и изменять (рис. 10.17). Известное средство удаленного администрирования — RADMIN — можно применить для управления вашей сетью извне. При этом необходимо обеспечить достаточный уро-

вень защиты, установив труднораскрываемые пароли и аутентификацию средствами NTFS. Входящий и исходящий порты можно установить в соответствии с применяемыми значениями. Важно, чтобы исходящий порт соответствовал применяемому в вашей сети. IP-адрес должен соответствовать адресу того компьютера, на котором установлен RADMIN-сервер, и не обязательно должен совпадать с адресом интернет-сервера.

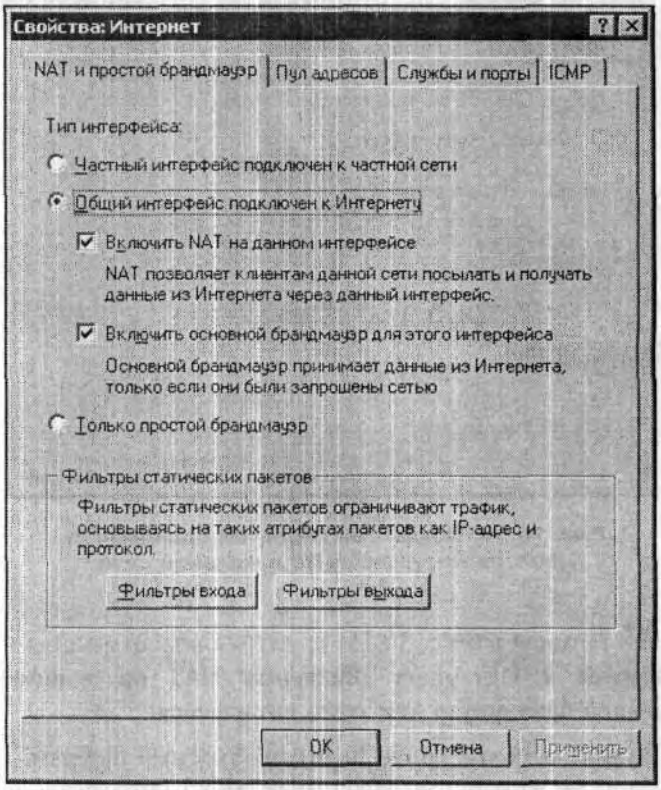


Рис. 10.15. Объект **NAT/Простой брандмауэр**, свойства интерфейса **Интернет**, вкладка **NAT и простой брандмауэр**

Внимание

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

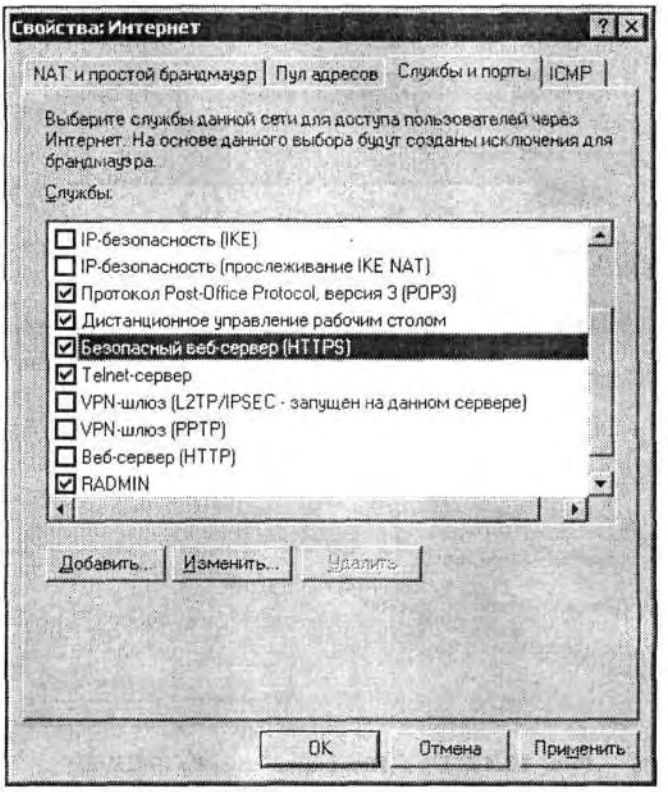


Рис. 10.16. Объект **NAT/Простой брандмауэр**, свойства интерфейса **Интернет**, вкладка **Службы и порты**

Некоторые службы заранее настроены и их необходимо только включить, указав конечный IP-адрес. На рис. 10.18 показано окно 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.

Аналогично можно установить доступ к почтовому серверу, Web-серверу и другим службам, которые вы используете в вашей сети. При этом для доступа к своему почтовому серверу вы сможете применять 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. Совсем не вредно открыть порт 123 по протоколу UDP для обеспечения синхронизации системного времени в вашей сети с каким-либо сервером точного времени.

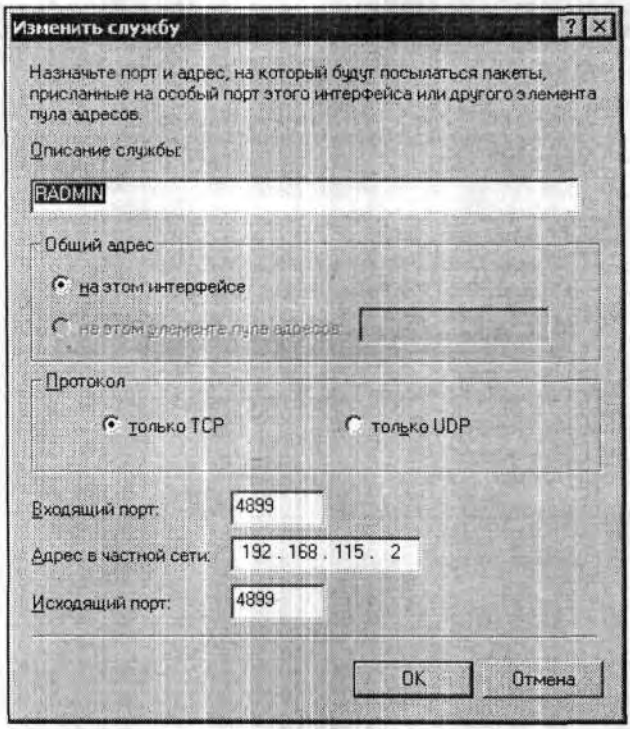


Рис. 10.17. Окно **Изменить службу** (RADMIN)

Несмотря на то, что мы настроили доступ извне и возможность подключения к Интернету из локальной сети, в свойствах сервера установлен только маршрутизатор и только локальной сети. Для контроля посмотрите на свойства интернет-сервера, вызвав соответствующее окно из контекстного меню объекта, соответствующего вашему серверу (рис. 10.19).

Если теперь вызвать мастер настройки сервера и посмотреть уже существующие его роли (рис. 10.20), то увидим, что сервер настроен в роли **Сервера удаленного доступа**. Собственно, с этого можно было начать, и мастер начальные настройки установил бы самостоятельно. Но уточнение настроек необходимо провести вручную.

С помощью этого же мастера можно дать еще одну роль серверу — **DNS-сервер**. 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. Настройки DNS-сервера нужно проводить через окно

dnsmgmt — DNS\<имя сервера> (рис. 10.21). Вызвать его не сложно: **Администрирование | DNS**.

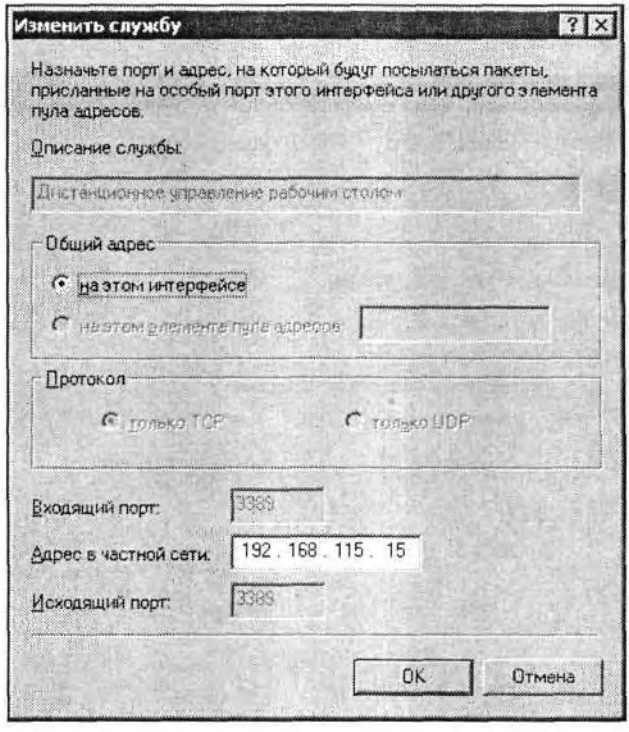


Рис. 10.18. Окно **Изменить службу** (дистанционное управление рабочим столом)

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. 10.22). 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 может привести к сообщению, что корневые ссылки не требуются (окно свойств сервера DNS, вкладка **Корневые ссылки**). Тем не менее, их все же добавить можно, удалив зону "." из списка зон прямого просмотра. Эта зона автоматически добавляется сервером, когда он получает 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 локальной сети, а как резервный — DNS-сервер интернет-сервера.

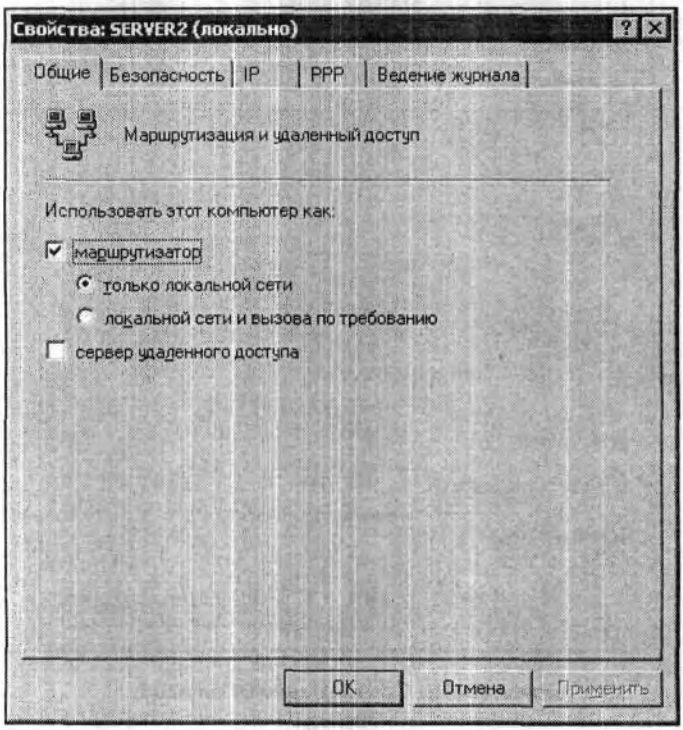


Рис. 10.19. Окно
Свойства: <имя сервера> (локально)

На компьютерах, подключающихся к Интернету, в качестве DNS-сервера можно указывать адреса ваших локальных DNS-серверов, которые теперь смогут разрешать не только внутренние имена, но и адреса Интернета в IP-адреса.

Более подробно о настройках службы DNS можно прочитать в статье "Система DNS (система имен доменов) — это основной компонент для разрешения имен в Интернете (разрешение имени узла в интернет-адрес)" в базе знаний Microsoft (**http://support.microsoft.com/default.aspx?scid=kb;ru;300202&FR=1&PA=1&SD=HSCH** на русском языке).

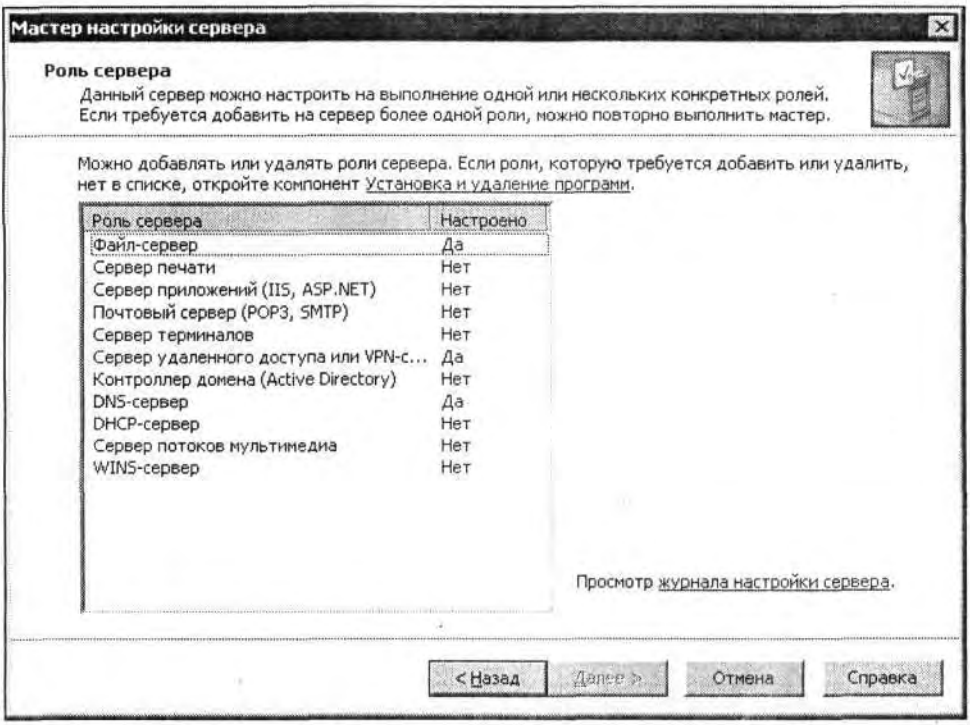


Рис. 10.20. Окно **Мастер настройки сервера** (роль сервера)

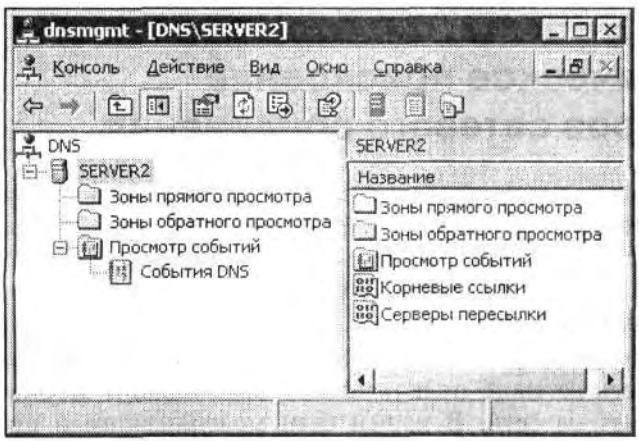


Рис. 10.21. Окно **dnsmgmt - DNS\<имя сервера>**

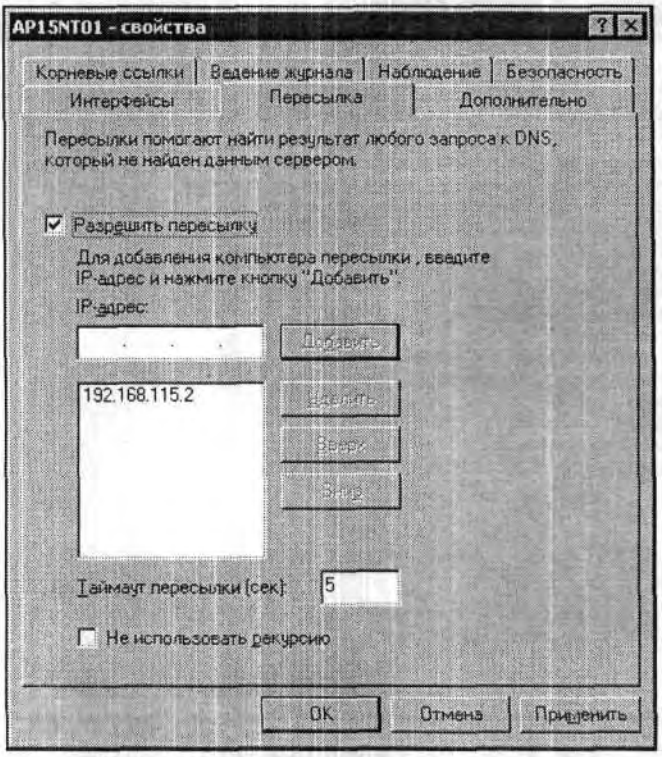


Рис. 10.22. Окно **<имя сервера> - свойства** (свойства основного DNS-сервера)

Автоматическое присвоение параметров сетевого соединения

Чем больше мы выполняем изменений в сети, тем сложнее могут оказаться настройки сетевых подключений у пользователей сети. Каждая модернизация сети может приводить к изменению этих настроек. Следует подумать и о пользователях, и о себе. Зачем утруждать пользователей необходимостью изменять параметры подключения или ждать вас, пока вы доберетесь до каждого рабочего места, чтобы выполнить эти изменения. Самый удобный вариант настроек сетевого подключения — это вариант автоматического получения параметров сети. В нашей сети модернизации и преобразования, необходимость которых была вызвана различными объективными обстоятельствами, привели к тому, что некоторым пользователям необходимо применять до трех шлюзов в разные сети. Оценив, какой из шлюзов приме-

няется наиболее часто, мы включили его в число автоматически назначаемых параметров. Другие параметры настраиваются пользователями самостоятельно, но с помощью выполнения пакетного файла, который содержит команды добавления дополнительных маршрутов.

Откуда же рабочая станция пользователя должна получить настройки сетевого подключения? Самый простой способ — передача рабочей станции параметров сетевого подключения DHCP-сервером. В отличие от других серверов, DHCP-сервер обнаруживается операционными системами Windows автоматически. По этой причине в подсети должен быть только один DHCP-сервер. Если вы помните, с самого начала книги, рассматривая примеры, мы старались избегать применения DHCP-сервера до тех пор, пока не стали применять сервер. Поскольку первый сервер сети в этом примере уже был настроен ранее, остается поправить настройки DHCP-сервера, который на нем работает. Вызываем окно настройки DHCP-сервера: **Администрирование | DHCP** (рис. 10.23).

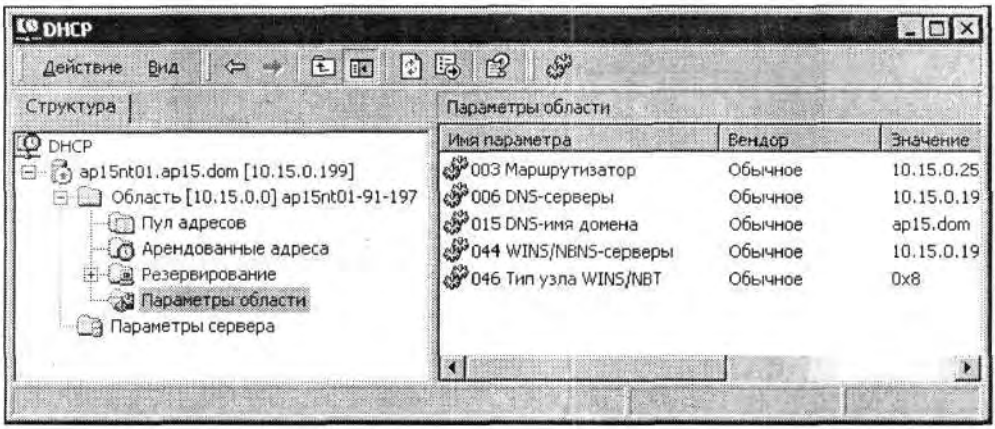


Рис. 10.23. Окно **DHCP**

DHCP-сервер может обслуживать несколько областей IP-адресов, но в нашем случае эта область одна. Параметры сетевого подключения, которые должны быть установлены для рабочих станций сети, можно указать в параметрах области. В контекстном меню узла **Параметры области** выберите пункт **Настроить параметры**. В окне **Область - параметры** (рис. 10.24) вы увидите довольно длинный перечень возможных параметров. Отметьте необходимые параметры, одновременно устанавливая их значения. На рисунке вы видите, что параметр **Маршрутизатор** (шлюз) получил определенное значение. Можно было бы указать и сразу массив адресов, но не всегда рабочая станция может сразу понять, когда какой шлюз использовать (требуются

дополнительные настройки маршрутизатора). Поэтому мы оставим одно значение шлюза, а маршрутизацию для другого шлюза настроим на тех рабочих станциях, где это необходимо.

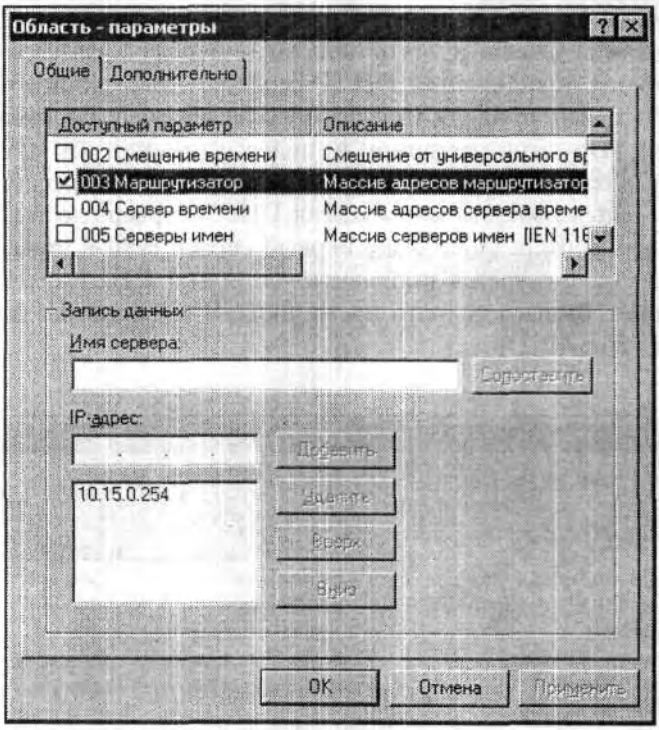


Рис. 10.24. Окно **Область - параметры**

DNS-серверы можно указать в любом количестве, добавив к локальным серверам серверы провайдера или другие, известные вам. Но обычно достаточно двух DNS-серверов, которые использует наша сеть.

После выбора всех необходимых параметров их значения будут видны в правой части окна **DHCP**. Теперь при каждой загрузке рабочие станции будут получать параметры для настройки своего сетевого подключения.

Для тех, кому мало одного шлюза

В отдельных случаях одного шлюза мало. Скажем, тот шлюз, что был указан в примере для передачи параметров подключения при загрузке рабочих станций, применяется для связи с удаленным сервером. Подключение к Интернету нужно не всем пользователям, но для его работы требуется указание

второго шлюза. В этом случае мы можем применить пакетный файл следующего содержания — листинг 10.1.

Листинг 10.1 Файл Internet.bat

```
netsh int ip reset "C:\resetip.txt"
netsh int ip add address "<Имя_интерфейса>" gateway=10.15.0.198 gwmet-
ric=2
route add 10.0.0.0 mask 255.0.0.0 10.15.0.254 metric 2
rem route add 192.168.0.1 mask 255.255.255.255 10.15.0.50 metric 2
pause
```

В файле всего пять строк. Последняя строка содержит команду, которая приостанавливает выполнение команд, а в данном случае позволяет сохранить окно командной строки открытым после выполнения всех команд, чтобы прочитать сообщения и убедиться, что все команды выполнены, либо увидеть проблемы и принять меры к их устранению.

Первая строка просто сбрасывает все полученные автоматически настройки. Вторая строка добавляет в качестве основного шлюза шлюз в Интернет. Третья строка добавляет маршрут в сеть 10.0.0.0 через шлюз 10.15.0.254. Это позволяет рабочей станции "понять", что все адреса сети 10.0.0.0 с маской 255.0.0.0 следует искать за шлюзом 10.15.0.254.

Четвертая строка в данном примере закомментирована. Но если комментарий убрать, то она позволит рабочей станции найти сервер 192.168.0.1 за шлюзом 10.15.0.50, если потребуется к нему обратиться.

Возможно, что вы сочтете более удобным сделать основным шлюз в Интернет, выдавая его адрес автоматически всем рабочим станциям сети. В таком случае вам потребуется организовать контроль работы пользователей в Интернете.

Трафик надо экономить

Как бы вы хорошо не администрировали свою сеть, может наступить момент, когда большая часть вашей планомерной работы может быть перечеркнута одним распоряжением руководства. Нет, совсем не со зла это было сделано, даже наоборот, — прогресс потребовал жертв. Нужно было включить нашу локальную сеть в растущую сеть корпорации. Само собой, пришлось изменять адрес сети, множество настроек, даже некоторые принципы администрирования, устоявшиеся уже в сети. Сроки, в которые предстояло выполнить модернизацию сети, были настолько сжаты, что эффективные средства наблюдения за трафиком Интернета и его учета пришлось времен-

но отключить. На несколько дней с экрана второго сервера пропали графики потребления трафика Интернета нашими пользователями. Через непродолжительное время основные проблемы нашей перестройки были решены. Пора было восстанавливать средства оперативного контроля над ходом сетевых процессов, включая и средства наблюдения за расходом трафика Интернета. Пользователей в нашей сети стало существенно больше, а в неразберихе скоротечных преобразований возможность пользования Интернетом была предоставлена большинству из них. Наши старожилы были "воспитаны" в достаточно строгих правилах, и Интернет использовался только по производственной необходимости. Конечно, исключения встречались, но именно как исключения. "Админ" строг, но ведь не зверь. Если кому-нибудь срочно требовалось найти в Интернете реферат для ребенка или информацию об автомобиле, который хотелось бы приобрести, — всегда пожалуйста на сэкономленном пользователем трафике можно бродить по Интернету сколько угодно, если не посещать сайтов, на которые обычно администраторы накладывают табу.

И вот, три или четыре дня в сети никакого контроля, а новые пользователи еще не освоились с нашими порядками, и кое-кто из них решил, что Интернет это не средство получения необходимой информации, а зона отдыха и развлечений. И это в рабочее время! И в то самое время, когда несколько новых пользователей настроились на радиостанции, ведущие вещание через Интернет, администратор начал восстановление средств наблюдения за трафиком. Он сидел у монитора второго сервера, создавая пока лишь самые грубые фильтры, позволяющие выделить группы пользователей и ощутить их активность в Интернете. Открыто очередное окно графического представления работы только что созданного фильтра, а там ярко-красный пожар графика входящего трафика. Тут же была включена детализация процесса и выявлены слушатели радио. По определенному адресу в Интернете настроен новый фильтр, который перекрыл дорогу трафику от радиостанции. Но через несколько секунд пожар графиков вспыхивает вновь! Находчивые радиослушатели моментально перешли на резервный адрес. Что ж, администратор наш тоже не лыком шит. Еще несколько минут, и в фильтры, перекрывающие поток трафика, добавлены все известные администратору адреса радиостанций. Да, у нашего администратора не забалуешь. Вы, наверное, решили, что при таких строгих порядках радиослушателей тут же уволили или, во всяком случае, лишили премии? Нет. Просто предупредили их руководителей о существующей системе ответственности за нерациональное расходование средств предприятия. Экраны графиков успокоились, как и потоки трафика, поглощаемого сетью из Интернета. Вместе с тем, несколько увеличилась производительность труда отдела, где трудились радиослушатели.

Организовать такой контроль можно, применяя разнообразные средства измерения сетевого трафика, а запретить отдельные адреса в Интернете

для пользователей сети можно средствами Windows. Когда мы в начале этой главы рассматривали подключение к Интернету через второй сервер, вы, возможно, обратили внимание, что в окнах свойств интерфейсов (рис. 10.25) есть две кнопки с интригующими надписями. **Фильтры входа** и **Фильтры выхода**. Именно за этими кнопками скрываются возможности ограничения входящего или исходящего трафика по отдельным адресам или их диапазонам.

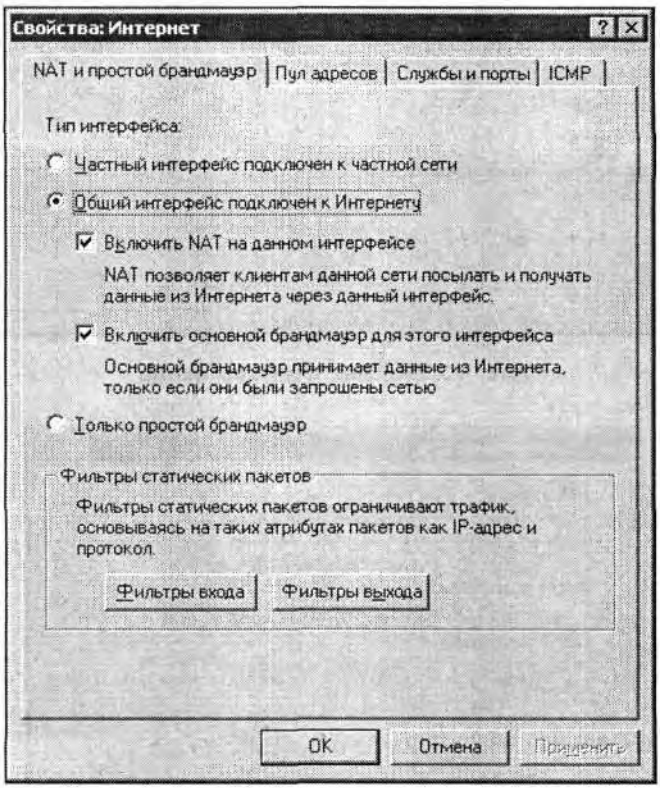


Рис. 10.25. Окно **Свойства: Интернет**, вкладка **NAT и простой брандмауэр**

Нажав на кнопку **Фильтры входа**, вы откроете одноименное окно (рис. 10.26), в котором перечислены уже существующие фильтры, и могут быть созданы новые.

Каждый фильтр после создания может быть изменен (рис. 10.27). Как при создании, так и при изменении необходимо указать параметры исходной сети и сети назначения, а также протокол, порт источника и порт назначения. Если параметр не указан, то воспринимается как любой.

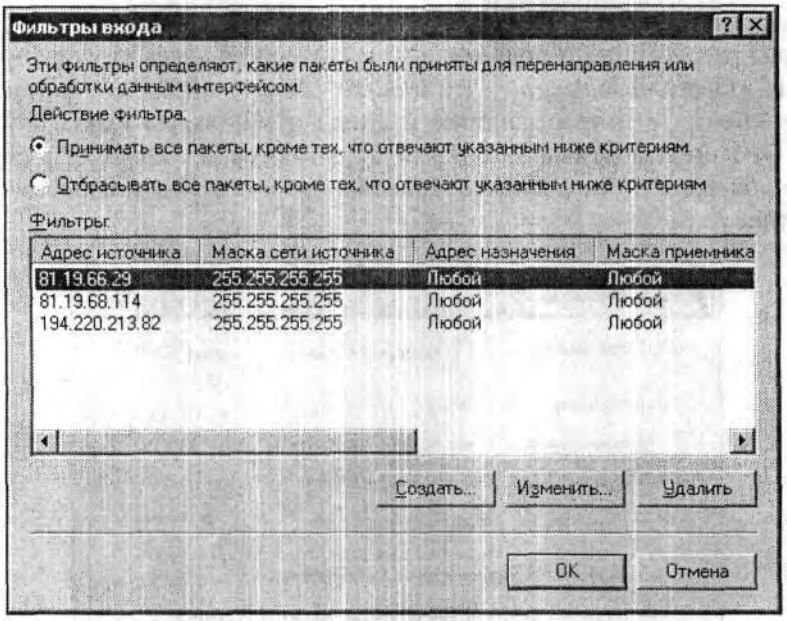


Рис. 10.26. Окно **Фильтры входа**

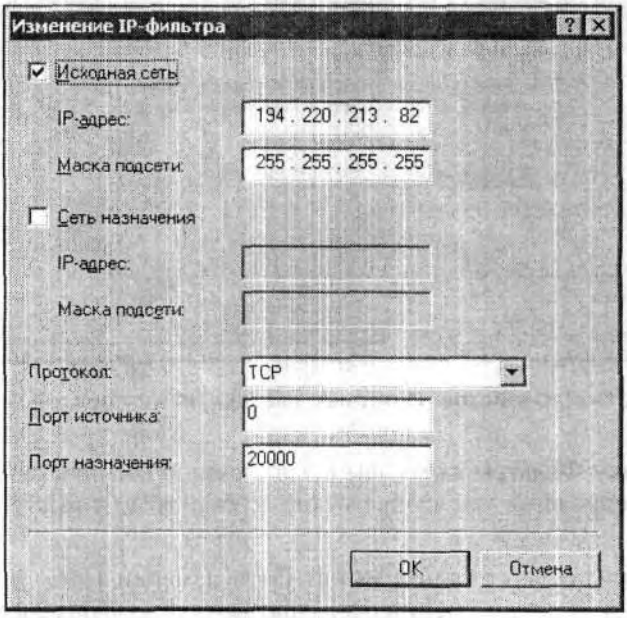


Рис. 10.27. Окно **Изменение IP-фильтра**

Показанный на рис. 10.27 фильтр запрещает связь внешнему серверу с адресом 194.220.213.82 по протоколу TCP с любого порта на любой адрес нашей сети и порт 20000.

Если в вашей сети есть лимит на расход трафика, то вы можете, не дожидаясь его перерасхода, установить фильтры входа для всех известных вам адресов Интернета, посещение которых можно запретить. Фильтры можно настраивать избирательно и к внутренним адресам сети. Независимо от того, какова реально маска подсети у вашей сети, вы можете, используя этот параметр, определять в фильтрах диапазоны исходящих или входящих адресов. Предположим, что из всего диапазона ваших внутренних адресов вам необходимо выделить несколько идущих последовательно друг за другом. Пусть это будут адреса 10.15.0.24—10.15.0.32. Рассчитаем параметры сети.

Учитывая, что наша сеть имеет маску 255.255.255.0, сразу заметим, что в двоичном представлении адресов сети первые 24 символа неизменны для любого из них. В выбранном примере 10.15.0.24 и 10.15.0.32 — начальный и конечный адреса. В двоичном представлении их последние октеты выглядят как 00011000 и 00011110. Ведущие нули необходимы, поскольку десятичными числами были обозначены двоичные октеты, длина которых восемь символов. В примере изменение адресов от минимального до максимального значения приводит к изменению трех из восьми двоичных символов. Пять символов неизменны. Добавим число неизменных символов к числу единиц в маске нашей сети (в двоичном значении маски неизменные разряды обозначаются единицами). Получим число 29. Значит, в фильтре можно указать сеть назначения 10.15.0.24/29, что соответствует записи адреса 10.15.0.24 с маской 255.255.255.248. При расчетах фильтров удобно пользоваться таблицей масок подсетей. Приведем ее фрагмент, который можно было применить при расчете примера (табл. 10.1).

Таблица 10.1. *Рсширение маски подсети 29*

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

Таблица 10.1 *(окончание)*

Маска подсети 255.255.255.248 /29 (11111111.11111111.11111111.11111000)			
32 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
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
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

Полностью таблица расширений масок дана в *Приложении*.

Для того чтобы обеспечить возможность гибкого управления потреблением трафика Интернета, есть смысл резервировать IP-адреса пользователей, которым необходим доступ в Интернет. Резервирование нужно выполнять в окне консоли DHCP-сервера.

Для того чтобы резервирование было выполнено корректно, необходимо знать MAC-адрес сетевого адаптера, IP-адрес которого резервируется. MAC-адрес рабочей станции можно узнать, выполнив команду `ipconfig /all` из командной строки. Фильтры входящего трафика нужны не только для ограничения возможностей пользователей в Интернете. Бывают ситуации, когда чей-нибудь сервер в Интернете работает некорректно. Например, один из них начал активно подключаться к нашему SMTP-серверу, создавая сеансы подключения, число которых у нас ограничено для экономии ресурсов сервера. В результате число сеансов работы достигало критического значения, и пользователи не могли отправить почту. Поскольку наш сервер должен отправлять почту только от пользователей нашей сети, возможность подключения к нему со стороны сервера нарушителя была пресечена.

Open VPN

Основное назначение второго сервера — это выполнение функций коммуникатора. Через него можно осуществлять связь как с сетью в целом, так и с отдельными компьютерами или серверами сети. Но следует учитывать, что каждый канал связи из внешнего мира в вашу сеть может потенциально использоваться злоумышленниками. Это значит, что всегда надо думать о защищенности каналов связи с сетью. Среди различных способов организации связи с сетью есть один, который становится все более известным и распространенным. Используя его, некоторые провайдеры предоставляют доступ в Интернет своим клиентам. Способов реализации VPN (Virtual Private Network, виртуальная частная сеть) существует на сегодняшний день великое множество. Но нас, с точки зрения самостоятельной модернизации сети, может интересовать не слишком сложный в настройках, но полезный для организации подключений точка-точка вариант. В нашей сети давно и успешно применяется средство под названием OpenVPN. Это открытая и бесплатная разработка, начавшая свое развитие в Linux, а теперь имеющая варианты и для Windows.

Организация доступа к локальной сети посредством OpenVPN 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 осуществлено подключение 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 время 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. При этом 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 и отдельным пользователям (возможно, руководителю организации). Доступ к файлам и принтерам через VPN не нарушает работы пользователя или 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, если доступ предоставляется 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 не обойтись, начнем с описания организации тестовой VPN между двумя машинами. Ваша сеть может существенно отличаться от той, что рассматривается в этой 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.

OpenVPN можно найти по адресу в Интернете **http://openvpn.sourceforge.net**. 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. 10.28).

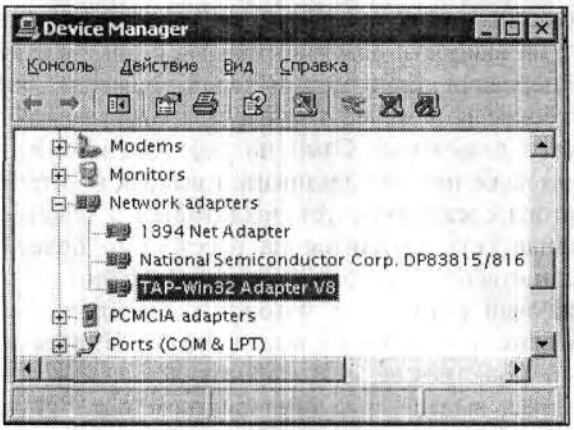


Рис. 10.28. Окно **Device Manager**
(новый адаптер в перечне оборудования компьютера)

Для нового адаптера автоматически создается и новое подключение (рис. 10.29), которое следует сразу переименовать в короткое и понятное имя, т. к. в файлах конфигурации программы OpenVPN нужно 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 10.2 и 10.3.

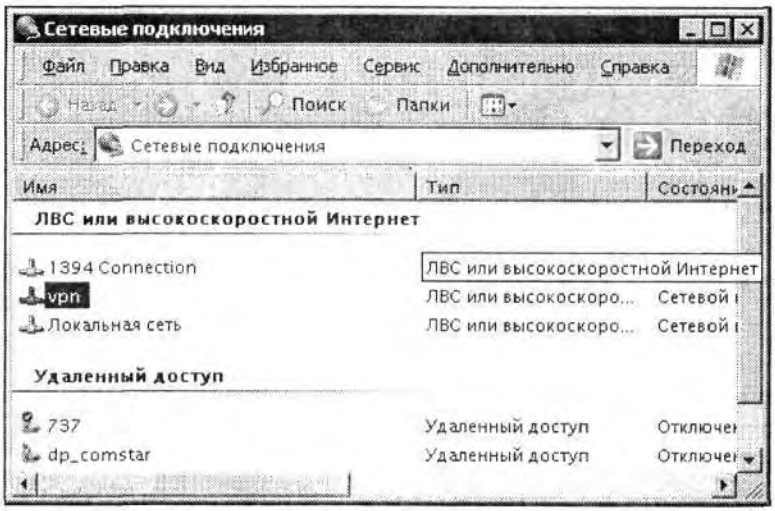


Рис. 10.29. Сетевые подключения (новое сетевое подключение)

Листинг 10.2. Local.ovpn — файл конфигурации для клиента OpenVPN

```
# 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 10.3. Server.ovpn — файл конфигурации для сервера OpenVPN

```
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
```

В обоих файлах `vpn` — это имя сетевого подключения (`dev-node`). 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` 192.168.116.3, а маску подсети — 255.255.255.0. Файлы должны иметь расширение ovpn. При этом в контекстном меню данных файлов появится пункт **Start OpenVPN on this config file** (Запустить OpenVPN с этим файлом конфигурации).

Для того чтобы организация виртуальной частной сети была возможной, необходимо, чтобы со стороны удаленного компьютера можно было выполнить `ping` по адресу сервера, к которому делается попытка подключения. В локальном файле конфигурации указывается имя сервера (параметр `remote`). Причем указывать можно только имя. Значит, связь имени и IP-адреса должна быть обеспечена одним из доступных способов. Это может быть указание DNS-сервера, который разрешит имя в адрес, а может быть и просто запись в файле C:\WINDOWS\system32\drivers\etc\hosts. Запись в этом файле — просто строка, содержащая IP-адрес и имя компьютера через пробел после адреса. 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. При удачной попытке 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. Для того чтобы сервер мог определить "своего" при подключении, применяется файл 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 и состоянии программы. Примеры окон клиентской и серверной частей программы с установленным соединением показаны на рис. 10.30 и 10.31. Признаком установившегося соединения в обоих частях программы является сообщение, содержащее строку **Initialization Sequence Completed** (Процедура инициализации завершена).

Сообщение клиентской программы `mute triggered` обозначает, 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.



Рис. 10.30. Окно OpenVPN на сервере



Рис. 10.31. Окно OpenVPN на локальной машине

При установившейся связи в сетевом окружении удаленного компьютера появится сервер. Для входа на него 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 сообщит 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 должен быть разрешен 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) **За-**

прос входящего эха для обеспечения возможности ответов компьютера на команду `ping` по его адресу. Настройки этого протокола доступны в дополнительных параметрах брандмауэра в ОС Windows XP и Windows Server 2003.

Поскольку в каждой сети, в том числе и в вашей, настройки доступа к ней могут иметь свои особенности, без экспериментов вам не обойтись и 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 дополнительного 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 dial-up. При этом для работы с документом Word его требовалось скопировать 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 был уже 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 ранее 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 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 OpenVPN. 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. 10.32 схематично показана организация подключения к локальной сети через Интернет с использованием виртуальной частной сети.

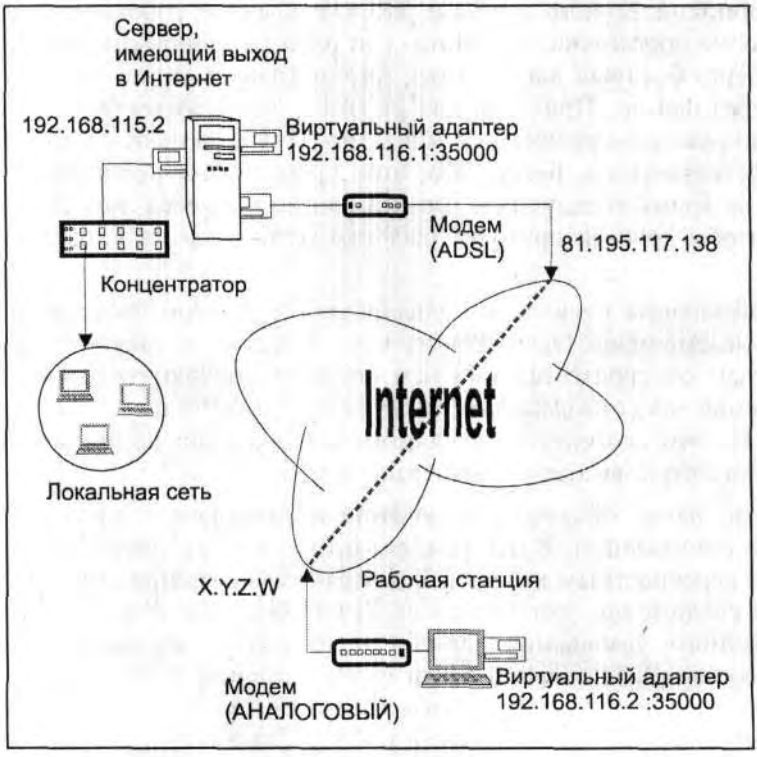


Рис. 10.32. Схема подключения к ЛВС через Интернет с применением VPN

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 обна-

ружения 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. 10.33).

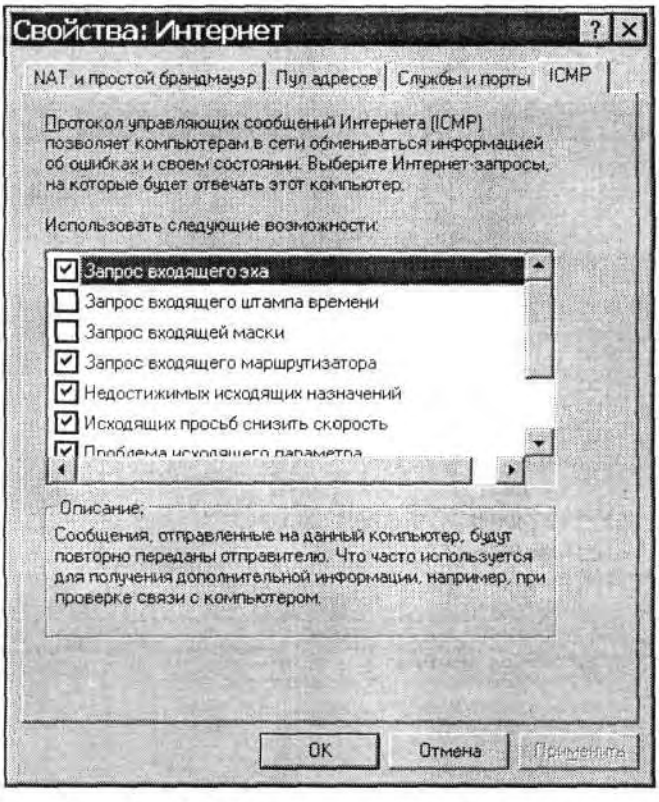


Рис. 10.33. Свойства интерфейса **Интернет**, настройка ICMP (запрос входящего эха)

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, устанавливая параметры сетевых подключений, будьте внимательны. Случайная ошибка при выборе параметров подключений к катастрофе не приведет, но заставит помучиться в поисках причин неудачи.

Когда вы убедились, что `ping` до сервера проходит нормально, время ответа не превышает 300 мс, а разброс значений этого времени невелик (не более

50%), то 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 `ping` будут нерегулярными. Если среди строчек ответов на экране появляется **Превышено время ожидания**, то следует искать причины нарушения качества связи или выбрать другое время для подключения.

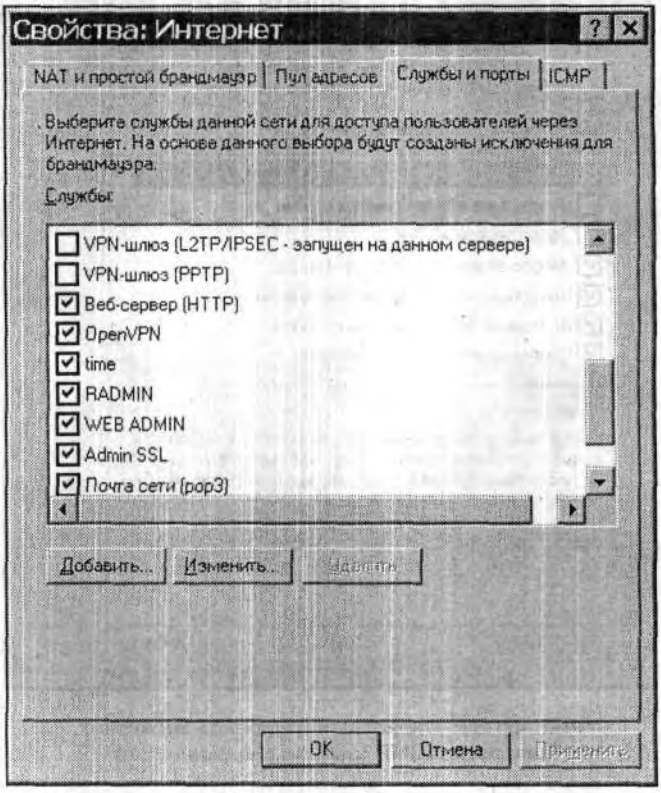


Рис. 10.34. Свойства интерфейса **Интернет**, открытые из оснастки **Маршрутизация и удаленный доступ**

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) этот порт должен быть открыт. В примере показано применение порта 35000, 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. 10.34 показано окно свойств интерфейса **Интернет** с перечнем служб, доступных из Интернета. На рис. 10.35 показано окно изменения свойств службы с указанием на номер входящего и исходящего порта. Можно выбрать эти значения отличающимися. 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).

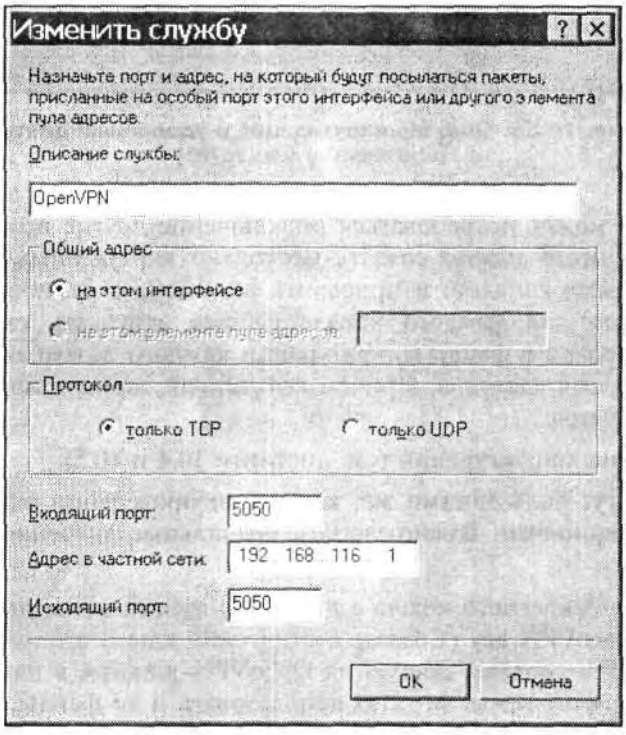


Рис. 10.35. Изменение службы для интерфейса **Интернет**, открытого из оснастки **Маршрутизация и удаленный доступ**

Открыв используемый порт, необходимо настроить маршрутизацию IP-пакетов, передаваемых через Интернет. Это также делается в оснастке **Маршрутизация и удаленный доступ** (рис. 10.36), где необходимо указать статиче-

ские маршруты. 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).

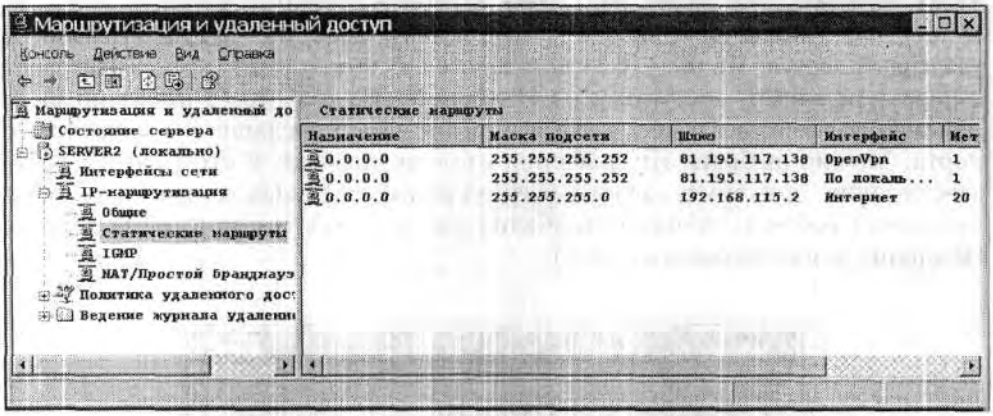


Рис. 10.36. Окно **Маршрутизация и удаленный доступ** (статические маршруты)

В дальнейшем может потребоваться подключение других пользователей через VPN. Для этого нужно создать несколько виртуальных адаптеров (по числу создаваемых каналов) и присвоить им имена с различными суффиксами. При этом для каждого канала следует запускать свой экземпляр OpenVPN-сервера, а в файле конфигурации каждого экземпляра указать соответствующее имя адаптера. Причем выбранный вариант маршрутов изменять не потребуется.

Создадим файлы конфигурации (см. листинги 10.4 и 10.5).

Эти файлы могут быть такими же, как и при проведении экспериментов с локальными машинами. Важно указать правильные значения IP-адресов и портов.

Создадим файл секретного ключа с помощью пункта меню программы **Generate a static OpenVPN key** (Создать статический ключ) и поместим одну копию на OpenVPN-сервере, другую на OpenVPN-клиенте в папку 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 подключение с рабочей станции, соединенной с Интернетом. Хорошо, если для проведения пробного подключения есть второй телефон. К сожалению, dial-up-подключение по той же линии, к которой подключен ADSL-модем, не всегда бывает достаточно хорошего качества, но, может быть, 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 проверяем 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 быть включена проверка подлинности по смарт-карте или сертификату, но при доступности сведений 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 (MD5-Chellenge).

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 компьютеру, имеющему непосредственное подключение к Интернету, то можно начинать настройку доступа к любой рабочей станции сети (рис. 10.37). Эта возможность позволяет любому пользователю (если вы настроили для него доступ) подключиться из дома к своему рабочему компьютеру. В нашей сети у второго сервера, имеющего непосредственное подключение к Интернету, есть 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, где работает OpenVPN-сервер, имеющий этот же номер порта, то связь OpenVPN-клиента осуществится именно с этой рабочей станцией. Если применяется брандмауэр, то необходимо разрешить связь из Интернета по этому номеру порта.

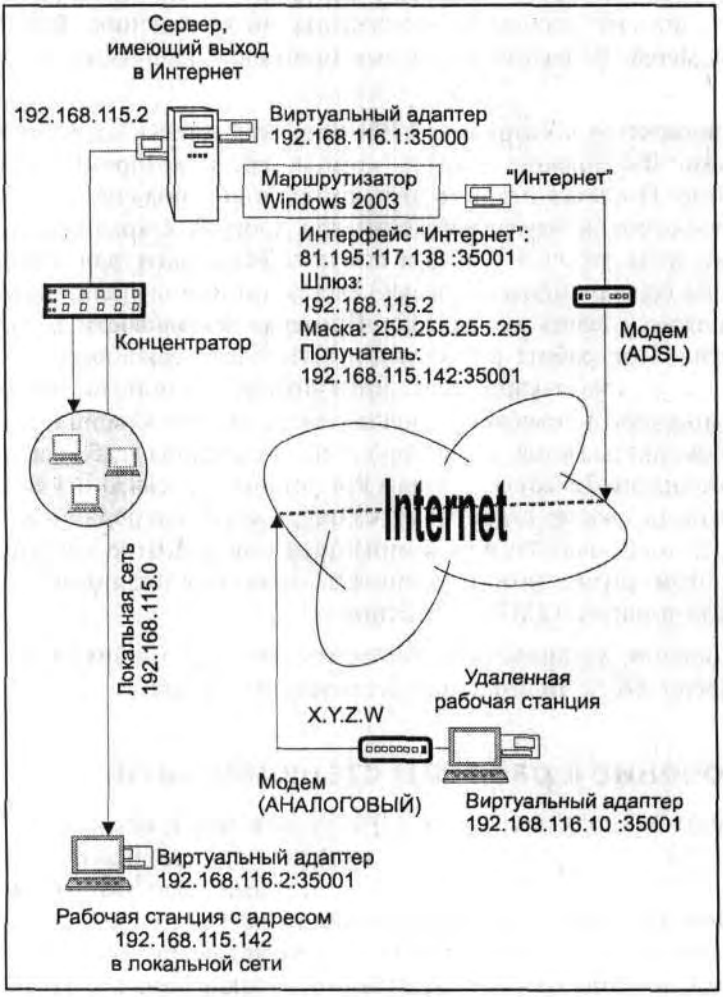


Рис. 10.37. Схема подключения к рабочей станции

Настройте доступ по выбранному порту к рабочей станции, создав еще одну службу, подобно тому, как показано на рис. 10.34 (OpenVPN), адресовав ее на соответствующий рабочей станции IP-адрес и указав выбранный для работы порт (см. рис. 10.35). Следует указать также статические маршруты (см. рис. 10.36) 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 для исключения 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. То есть 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 будет появляться **Initialization Sequence Completed with Errors**, когда установлено более одного виртуального адаптера, то 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 есть на сайте разработчиков OpenVPN, а здесь приведем еще раз содержимое файлов конфигурации сервера и клиента с некоторыми изменениями (листинги 10.4 и 10.5).

Листинг 10.4. Local.ovpn — файл конфигурации для клиента OpenVPN

```
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 10.5. Server.ovpn — файл конфигурации для сервера OpenVPN

```
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) 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 "подводных камней".

Интернет для первого сервера

Мы установили второй сервер и предоставили через него доступ в Интернет для пользователей сети. Но Интернет — это не только информация для пользователей сети. Это и обновления для программ и операционных систем, это и точное время в вашей сети. Интересно, что точное время зачастую не очень интересует администраторов сети. Какая разница, минута ту-

да — минута сюда. Что случится, если время в сети будет отличаться от действительного? До тех пор, пока сервер в вашей сети один, на самом деле нет большой беды, что время на нем не совсем соответствует вашему местному времени. Но когда серверов становится более одного, когда они имеют связь с другими сетями, возникают процессы, которые должны быть синхронизированы. Отсутствие информации о точном времени в течение продолжительного периода может привести к появлению если не фатальных, то все же неприятных ошибок, о которых вы будете читать в системных журналах. Отличие значений текущего времени на разных серверах может привести к невозможности синхронизации баз данных различных служб, включая DNS и Active Directory (при условии, что есть второй контроллер домена). Да и просто ощущение того, что время в вашей сети идет синхронно мировому времени, должно приносить удовлетворение вам, как администратору.

Все ранее сказанное наводит на мысль, что первый сервер должен быть обеспечен возможностью выхода в Интернет. Поскольку первый сервер является контроллером домена, он должен хранить время в сети, с ним должны синхронизировать свои часы рабочие станции. Если и он сам сможет синхронизировать свои часы с надежным источником, то мы будем уверены, что время в нашей сети так же верно, как сигналы точного времени по радио.

Если время не может быть синхронизировано сервером с эталонным источником в Интернете, то в системных сообщениях можно встретить такие:

```
Службе времени не удалось синхронизовать системное время в течение
86400 сек., поскольку ни один из поставщиков времени не смог предоста-
вить пригодный штамп времени. Служба времени не синхронизирована и
не может предоставить время другим клиентам или обновить системные
часы. Проследите за системными событиями во избежание появления бо-
лее серьезных проблем.
```

Как видим, сервер не сообщает о критической для системы ситуации, но предупреждает, что отсутствие синхронизации может привести к более серьезным проблемам. Поэтому следует настроить синхронизацию, чтобы избежать данных проблем.

По умолчанию Windows настроена на синхронизацию с сервером time.windows.com. Но нагрузка на этот сервер весьма высока и синхронизация с этим сервером не всегда возможна. Рабочие станции, включенные в домен, пытаются синхронизировать время с контроллером домена. Поскольку контроллер домна обычно доступен, время внутри сети синхронизируется регулярно.

Проверить возможность синхронизации можно, введя в командной строке команду `net time /set`. В ответ вы получите значение времени на сервере, значение времени на вашем компьютере и предложение синхронизировать часы компьютера с часами сервера, введя символ "Y" и нажав <Enter>.

Иногда контроллер домена не доступен. Наиболее часто это бывает, когда ноутбук, являющийся членом одного домена, подключается в сеть другого домена. Например, если вы используете один компьютер в домашней и рабочей сети, и одна из сетей "не родная" для него. В этом случае можно проводить синхронизацию времени вручную. Для этого следует в окне командной строки ввести команду `net time /set \\<имя_сервера>`. Ответ будет аналогичным тому, что был описан в предыдущем случае.

Но есть возможность заставить сервер и рабочие станции синхронизировать свои часы автоматически с одним из доступных серверов. Но при этом следует учесть, что порт 123 по протоколу UDP должен быть открыт для сервера. При этом другие компьютеры сети будут недоступны для внешних серверов времени. Они должны содержать список доступных локальных серверов времени и дополнительно, на случай работы вне сети, имена одного-двух внешних серверов. Сервер сети должен иметь список внешних серверов времени.

Если имена локальных серверов нам обычно известны, то имена внешних серверов, кроме time.windows.com, следует найти. Эти имена доступны в Интернете. Один из адресов, по которому можно найти действующие серверы времени, — **http://ntp.isc.org/bin/view/Servers/StratumTwoTimeServers**. По этому адресу доступна таблица с адресами серверов времени и указанием на его доступность. Таблица периодически обновляется.

На момент написания этих строк в зоне ru были доступны в числе других **ntp.psn.ru** и **ntp0.solarnet.ru**. Имена доступных в локальных сетях серверов-контроллеров доменов для моего компьютера **ap15nt01** и **mh2003s**.

Убедившись в доступности внешних серверов командой `ping` и проверив дополнительно, что удаленность этих серверов не превышает 10—12 "прыжков" по команде `tracert <имя_сервера>`, можно приступать к настройке компьютеров.

Начнем с сервера.

1. Установить службу SNTP server, если она пока не установлена (**Установка и удаление программ | Установка компонентов Windows | Прочие сетевые службы**).
2. Через оснастку **Службы** установить тип запуска службы **Авто** и запустить SNTP server. В случае фатального исхода попытки проверить функционирование службы DCOM (там же).
3. В окне командной строки подать команду `net time /setsntp:"ntp.psn.ru ntp0.solarnet.ru"`. (Список заключается в кавычки.) Это запустит службу w32time и автоматически занесет список адресов внешних серверов времени в ветку реестра (HKLM\SYSTEM\CurrentControlSet\ Services\ w32time\Parameters\ntpserver). Автоматически применятся и запишутся в реестр значения по умолчанию для политики синхронизации.

4. Открыть указанную ветку реестра в редакторе и изменить остальные значения параметров на желаемые.
5. Выполнить в командной строке `net stop w32time` и следом `net start w32time`. Это перезапустит службу времени, и изменения будут применены.
6. Проверить правильность настройки списка внешних серверов, записав в командной строке `net time /querysntp`. Вы должны увидеть правильно отображаемый список адресов.

Для проверки синхронизации времени на сервере:

1. Выполнить в командной строке `net stop w32time` и следом `net start w32time`. В системных событиях должно появиться сообщение, говорящее о получении правильного времени от внешнего сервера времени.
2. Измените вручную текущее время на несколько минут. Выполните команду `w32tm /resync`. Значение текущего времени должно восстановиться.

Следующие команды и действия необходимо выполнить на рабочей станции (ноутбуке):

1. Запустить команду `net time /setsntp:"ap15nt01 mh2003s"`.
2. Проверить командой `net time \\<имя_сервера_времени>` время на внешнем сервере и `time` — на этом компьютере.
3. Провести первую синхронизацию времени командой в окне командной строки `net time \\<имя_сервера_времени> /set`.

Возможные неисправности и их устранение

Практически все, о чем говорилось в этой главе, связано с маршрутизацией и подключением к различным внешним для локальной сети компьютерам. Неисправности, связанные с такими подключениями, обычно заключаются либо в отсутствии связи с удаленным компьютером, либо с качеством этой связи.

Отсутствие связи может быть вызвано как причинами физического характера, например, неработоспособностью удаленного компьютера, так и проблемами в работе серверов, обеспечивающих возможность связи.

Одной из распространенных проблем, приводящих к невозможности установления соединений в сетях, является недоступность DNS-сервера. DNS-сервер должен указать верный IP-адрес, когда известно символьное имя узла. Несмотря на весьма высокую надежность DNS-серверов в Интернете, они иногда отказывают, или их владельцы меняют принадлежащие им IP-адреса. Это случается не часто, и при обнаружении проблем со связью вы

скорее всего, не предположите, что проблема именно в этом. Возможна и такая ситуация, когда все серверы работают нормально, но вы сами изменили место или условия подключения рабочей станции, и использовавшийся ранее DNS-сервер стал недоступен.

На протяжении нескольких месяцев я использовал свой ноутбук и на работе, и дома. Причем дома на нем всегда был запущен клиент OpenVPN, позволявший получать доступ к рабочей сети. Со временем дома была создана небольшая сеть с выходом в Интернет. Я решил использовать возможность подключения ноутбука к домашней сети с помощью Wi-Fi. Для этого был установлен недорогой коммутатор, совмещенный с точкой доступа, а для ноутбука приобретен сетевой адаптер Wi-Fi. Тогда каждый компьютер в домашней сети имел собственные сетевые настройки, в которых были указаны и DNS-серверы. Собственные настройки имел и ноутбук. Когда все устройства были настроены и подключены, я обнаружил, что в отличие от других компьютеров домашней сети ноутбук не мог выйти в Интернет. Я проверял соединения, "пинговал" домашние компьютеры и даже некоторые известные мне адреса в Интернете. Все тесты проходили с положительным результатом, но страницы Интернета не загружались в браузере ноутбука.

Только прекратив суетливые поиски неисправности и задумавшись над возможными причинами происходящего, я понял, что же мешало моему ноутбуку.

Дело в том, что для своего же удобства я перенес клиента OpenVPN на сервер домашней сети. Это позволило поддерживать постоянное соединение между домашним и рабочим сервером. Благо, подключение к Интернету постоянное как с той, так и с другой стороны. Находясь в рабочей сети, ноутбук пользовался услугами DNS-серверов, имеющихся в локальной сети. Подключаясь к Интернету дома и запуская OpenVPN на ноутбуке, я снова имел возможность подключения к DNS-серверу рабочей сети. Теперь, когда клиент OpenVPN перестал запускаться на ноутбуке, DNS-сервер рабочей сети стал недоступен для него. Какой уж тут Интернет? Достаточно было в свойствах сетевого подключения ноутбука добавить адрес DNS-сервера провайдера, как доступ к Интернету полностью восстановился.

Позднее, чтобы не зависеть от места подключения, я настроил оба сервера на автоматическую выдачу параметров сетевых подключений клиентам сетей. Проблем с подключением к Интернету не стало.

Этот опыт показывает, что есть явный смысл в том, чтобы автоматизировать получение рабочими станциями параметров сетевых подключений. Это избавит вас от возможных ошибок в настройке рабочих станций, параметры подключения которых становятся стандартными и выполнимыми даже не очень опытным пользователем при консультации по телефону.

В сети возможны также проблемы при отсутствии синхронизации часов сервера с эталонными часами (сервером времени) в Интернете. Сама по себе эта проблема может возникнуть при отсутствии связи с DNS-сервером. Но возможно, что и сервер времени прекратил свою работу. Как и в случае с DNS-серверами, следует иметь несколько адресов серверов времени. Сервер сети будет продолжать разрешать символьные имена в адреса и синхронизировать свои часы, даже когда один из DNS-серверов или серверов времени в Интернете прекратит функционировать.

Практически каждое руководство для пользователей компьютеров рекомендует создавать резервные копии важных файлов. Рекомендации системным администраторам содержат сведения о создании отказоустойчивых дисковых систем, в которых информация сохраняется на двух или более носителях, чтобы выход из строя одного из них не привел к выходу из строя всей системы. Аналогичный подход следует использовать и во многих других ситуациях. DNS-серверы, серверы времени в Интернете имеются в достаточном количестве, чтобы можно было создать резервирование и с этой стороны.



Глава 11

Администрирование растущей сети и обеспечение ее бесперебойной работы

Сеть продолжает расти. Увеличивается число пользователей, появляются удаленные пользователи, крепнут связи с другими сетями. Повышаются требования к надежности сети. Доступ к рабочим станциям может быть обеспечен средствами Windows (**Управление компьютером**, **Удаленный доступ к рабочему столу**) или с помощью программ удаленного администрирования. Это позволяет избежать посещения пользователей сети при возникновении у них проблем. Помощь пользователям можно оказать дистанционно. Но помощь может потребоваться и самой сети, ее серверам, процессам, которые выполняются автоматически, но столкнулись с непредвиденной ситуацией. В отличие от пользователей, сервер не может пожаловаться на свои проблемы, позвонив вам по телефону. Это значит, что следует максимально защитить сервер (или серверы) от неприятностей. Мы уже можем обеспечить возможность периодического наблюдения за работой сервера, даже на значительном удалении от него. Удаленный доступ к рабочему столу позволяет нам это делать в любой момент времени. Но вот в очередной раз подключаясь к серверу, вы обнаружили, что сервер не отвечает. Что случилось в сети? Предположений может быть много, но уверенности нет ни в чем. Скорее всего, если сеть должна работать постоянно, вам придется идти, бежать, а может быть и ехать к ней. Настроение ваше во время поездки будет не на высоте — это ведь не поездка к подруге.

Чтобы избавить себя хотя бы от части переживаний во время аварийных ситуаций, следует свести к минимуму такие ситуации, а как дополнение, научить сервер сообщать о своих проблемах. Среди прочих проблем, которые мешают спокойно жить администратору сети, довольно часто встречающееся периодическое отключение электроснабжения. Как уменьшить неблагоприятные последствия этих событий?

Источник бесперебойного питания

В самом простом случае источник бесперебойного питания (ИБП) может быть просто подключен как переходник между питающей розеткой и компьютером. В этом варианте подключения вам не придется ничего настраивать. В случае отключения электроэнергии источник проработает так долго, насколько хватит запаса энергии аккумуляторов. В какой-то мере это даже хорошо.



Рис. 11.1. Организация бесперебойного питания серверов

Если длительные перерывы в электроснабжении встречаются не часто, то сервер будет достаточно хорошо защищен от неожиданных некорректных отключений. А если отключение продлится дольше, чем могут выдержать аккумуляторы?

К счастью, Windows содержит встроенные средства для взаимодействия с источниками бесперебойного питания. Рассматривая возможности программ сторонних разработчиков, сравнивая их со средствами Windows, мы пришли к выводу, что встроенных средств вполне достаточно, чтобы обеспечить надежную работу серверов. Все устройства серверной должны быть запитаны от источника бесперебойного питания. Один из серверов соединяется интерфейсным кабелем с источником бесперебойного питания. Схема соединений приведена на рис. 11.1.

Задача организации бесперебойного питания серверов включает в себя следующие подзадачи:

1. Подключение всего оборудования серверной к ИБП.
2. Установка связи ИБП с сервером и настройка их программного взаимодействия.
3. Обеспечение корректного выключения всех серверов при длительном отсутствии питания.
4. Организация передачи служебных сообщений администратору при длительных перебоях в электроснабжении.

Первая из этих подзадач решается наиболее просто и не требует пояснений. Другие задачи рассмотрим последовательно.

Программное взаимодействие

Программное взаимодействие ИБП и компьютера осуществляется через интерфейсный кабель, по которому ИБП может передавать компьютеру информацию о своем состоянии, а компьютер — команды управления источнику бесперебойного питания. Несмотря на разнообразие типов ИБП, разработчикам ОС Windows удалось создать стандартный интерфейс для настройки взаимодействия ИБП и компьютеров. Этот интерфейс объединен с апплетом панели управления **Электропитание**. Существуют и специализированные программы, поставляемые вместе с ИБП или приобретаемые отдельно. Они предоставляют дополнительные возможности для управления электропитанием и администрирования ИБП. Но в небольшой сети, когда число серверов не превышает двух или трех, а расположены они в непосредственной близости друг от друга, вполне достаточно тех средств, которые содержатся в Windows. В зависимости от вида информации, передаваемой от ИБП компьютеру, операционная система принимает решение о необходимых действиях. Для двух уровней разрядки аккумуляторов ИБП могут быть

отработаны три вида событий. Это может быть уведомление, какое-либо действие или запуск программы. Уровни разрядки устанавливаются пользователем. Для уверенной работы сервера в условиях нестабильности электропитания необходимо обеспечить достаточную емкость аккумуляторных батарей ИБП и возможность повторного перехода в режим работы от аккумуляторов, если после включения питания по электросети снова произошло отключение электроэнергии. Рекомендовать конкретные типы источников бесперебойного питания невозможно. Все зависит от конкретных условий работы и требований к сети. Если качество электроснабжения оставляет желать лучшего и периоды отсутствия напряжения в питающей сети достигают нескольких часов, но сервер должен продолжать работать, то целесообразнее использовать дизель-генератор. На аккумуляторах реально поддерживать работу сервера до одного часа. В моей сети продолжительность работы от аккумуляторов задана в 20 минут. Если после включения напряжения оно отключится снова, то заряда аккумуляторов хватит еще на 20 минут. В случае продолжительного отключения электроэнергии будет включен генератор, время запуска которого около 15 минут. Таким образом обеспечивается бесперебойность работы сети. При отказе генератора на время более 20 минут сервер должен корректно выключиться. С учетом необходимости именно такого режима работы и настроено управление электропитанием. Время максимальной работы от аккумуляторов определяется экспериментально. Причем для надежности следует использовать значение продолжительности работы до разряда на 80%. Это позволит иметь уверенность в сохранении возможностей ИБП на протяжении двух лет.

Время подачи первого предупреждающего сигнала для оповещения администратора о возможном отключении сервера должно оставлять возможность до окончательного отключения предпринять какие-либо действия, например, запустить генератор. Исходя из описанных условий работы, будем настраивать взаимодействие компьютера и ИБП.

После подключения интерфейсного кабеля от источника бесперебойного питания к серверу сервер обнаружит ИБП. В апплете **Электропитание** панели управления появится дополнительная вкладка **ИБП**, а в перечне схем управления питанием появится режим работы от источника бесперебойного питания (рис. 11.2).

Для корректной работы ИБП необходимо настроить параметры его взаимодействия с сервером. Для этого на вкладке **ИБП** (рис. 11.3) следует нажать кнопку **Настроить**. Откроется окно **Настройка ИБП** (рис. 11.4). В этом окне можно выбрать подходящий нам режим взаимодействия ИБП с сервером.

Рассмотрим режим, который применяется в моей сети. Отмечена опция **Включить все уведомления**. В следующих двух полях устанавливаем интервалы времени между неполадкой и первым уведомлением, и между уведомлениями, сбой питания продолжается достаточно долго. Эти уведомления вы-

водятся на консоль сервера. Включив монитор после сбоя, можно увидеть информацию о кратковременном сбое в виде единственного уведомления, или о достаточно продолжительном сбое в виде нескольких уведомлений. Посчитав их число и зная период между ними, можно определить продолжительность сбоя. В приведенном варианте первое уведомление появится уже через пять секунд после сбоя, а последующие будут выведены с периодичностью в две минуты. Если сбой прекратится до критического сигнала, то кроме уведомлений на экране монитора никаких его последствий не обнаружится.

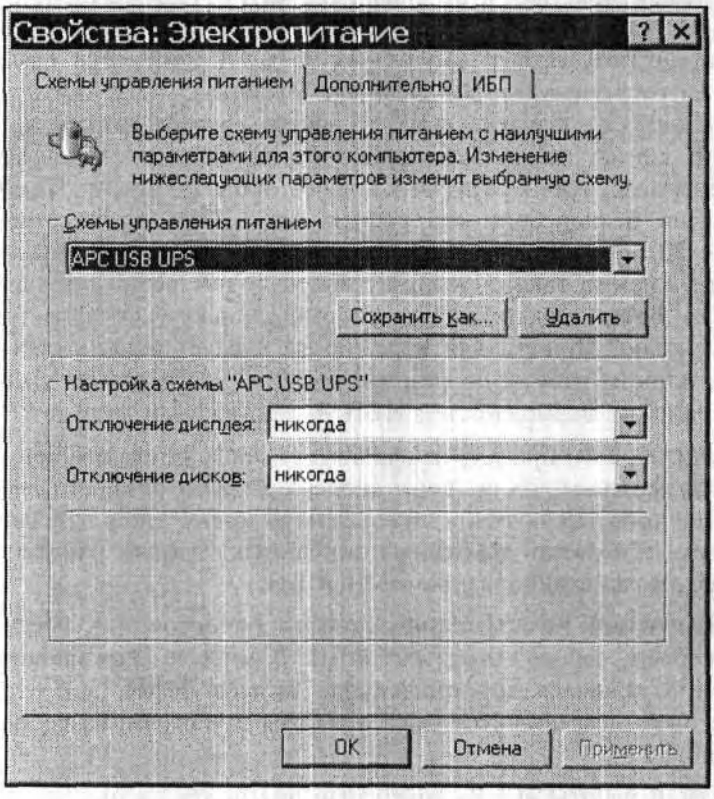


Рис. 11.2. Окно **Свойства: Электропитание**, вкладка **Схемы управления питанием**

Далее настраиваем режим работы после достижения критической величины разряда аккумуляторов. В этот момент должен быть подан **Критический сигнал**. Значение поля **Время работы от батареи до подачи сигнала (мин)** устанавливаем в зависимости от возможностей нашего ИБП. Следует экспери-

ментально определить время работы до остаточного заряда 10—20% и установить 50—70% от этого времени. В нашем случае это 30 минут. Следовательно, через 30 минут после начала сбоя будет подан критический сигнал. Нам в это время уже нет необходимости видеть этот сигнал или слышать его. Критический сигнал должен вызвать процессы, которые позволят корректно завершить работу сервера. В примере при подаче сигнала запускается программа (о ней поговорим далее) и выполняется завершение работы сервера и самого источника бесперебойного питания. Но в нашей сети есть еще один сервер, который запитан от того же ИБП, что и первый. Как же корректно выключить его? К счастью, существуют средства удаленного управления компьютерами и в том числе средство удаленного отключения компьютера. Такую программу можно запускать перед выключением первого сервера. Но в данном примере запускается командный файл, который вызывает несколько дополнительных программ, не только отключающих второй сервер, но и сообщающих администратору о выключении питания по электронной почте и на сотовый телефон в виде SMS-сообщения.

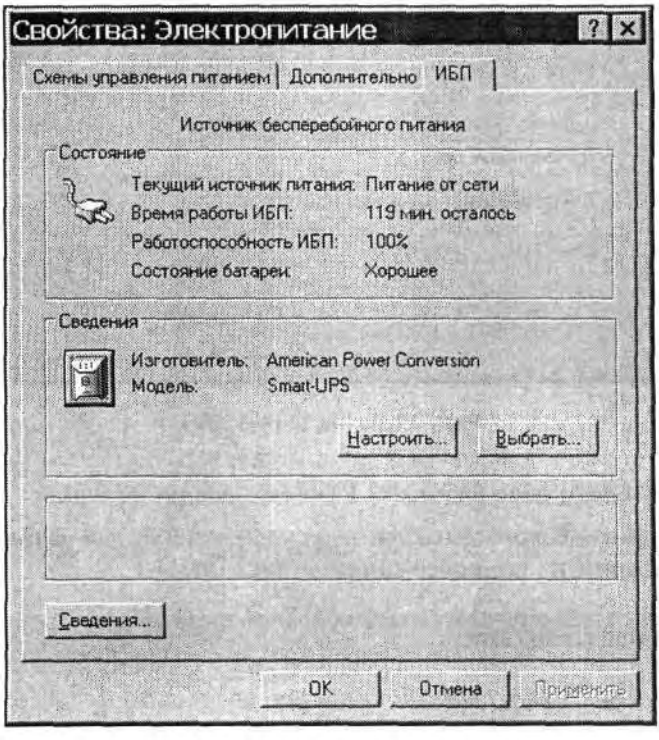


Рис. 11.3. Окно **Свойства: Электропитание**, вкладка **ИБП**

Сотрудникам, во время работы которых произошел сбой питания, да еще и не включился дизель-генератор, что привело к выключению серверов, не придется искать вас. Вы уже все будете знать сами. Мне, например, в этом случае остается позвонить ответственному лицу и попросить его после включения напряжения нажать кнопку, расположенную на ИБП. При этом серверы включатся и все программы начнут работать.

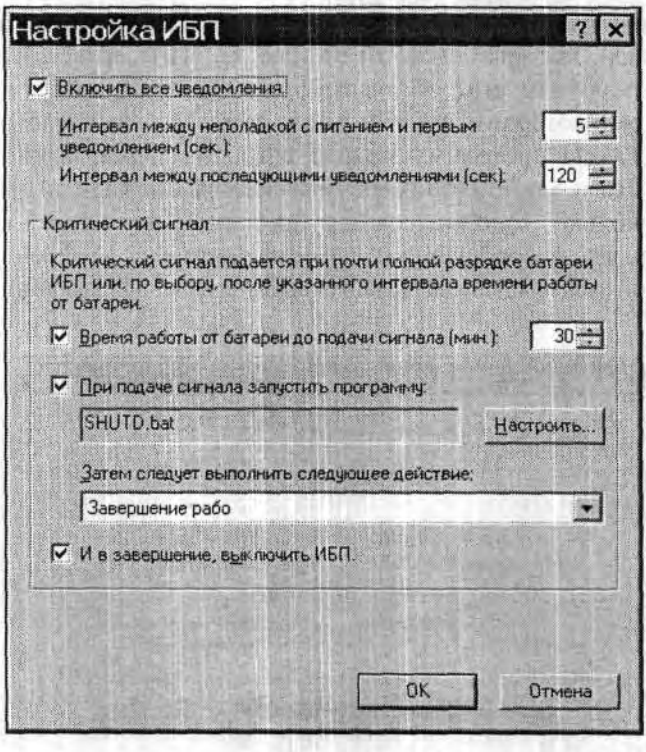


Рис. 11.4. Настройка ИБП

Как же это на самом деле работает? Разберем все по порядку.

При подаче критического сигнала запускается пакетный файл SHUT.BAT. Давайте посмотрим на его содержание — листинг 11.1.

Листинг 11.1. Файл SHUT.BAT

```
Net send ap15.dom /users SHUTDOWN SERVER!!!!!!
msg * "SHUTDOWN SERVER!!!!!!"
call SDS1.cmd
cd\
```

```
cd zerat
ups.bat
pause
```

Первые строки файла — это команды для отсылки сообщений пользователям домена (`net send`) и пользователю, открывшему сеанс на сервере (`msg`), поскольку доступ к удаленному рабочему столу открыт через Интернет. Пользователи успеют сохранить свою работу до выключения сервера.

Следующая команда (`call`) позволяет выполнить еще один командный файл (SDS1.CMD) и вернуться к выполнению пакетного файла.

Файл SDS1.CMD содержит всего одну строку (листинг 11.2).

Листинг 11.2. Файл SDS1.CMD

```
lanshutdownc -a 10.15.0.199 -u <Имя_пользователя> -p
<Пароль_пользователя> -d ap15 -m "Otkluchenie cherez 30 s" -t  30  -f
```

Это команда запуска бесплатной консольной программы LanShutDownC.exe (**http://www.lantricks.com/lanshutdown/index.php**), которая при наличии необходимых параметров позволяет корректно выключить удаленный компьютер, отправив сообщение пользователям домена. Имя пользователя и пароль должны соответствовать учетной записи, имеющей права на указанные действия. В составе Windows XP и Windows Server 2003 есть и штатная команда — `shutdown`, которую тоже можно применить в данном случае. Но автору больше понравилась lanshutdownc.exe.

После отправки сообщений и команды на выключение второго сервера продолжается выполнение SHUT.BAT. Осуществляется переход в каталог, содержащий файлы консольного почтового клиента. В данном случае применяется бесплатный почтовый клиент ZeRAT (**http://adom.nm.ru/zeratrus.htm**).

Вызывается на выполнение пакетный файл UPS.BAT, содержащий команду управления почтовым клиентом `zerat.exe UPS.txt`.

Информация об адресе назначения и содержание сообщений находятся в текстовом файле UPS.TXT (листинг 11.3).

Листинг 11.3. Файл UPS.TXT

```
Host:81.195.117.138

SMTPAuth:login                  ; smtp authorization NONE or LOGIN
SMTPUSER:<имя_учетной_записи_почты>  ; username. Leave it blank if
SMTPAUTH=NONE
```

```
SMTPPASS:<пароль>              ; password. Leave it blank if SMTPAUTH=NONE
From:Server2 <адрес_отправителя>
X-Priority: 1
X-MSMail-Priority: High
Importance: High
To:user@smsmail.ru
CC<2-й_адрес получателя>
Type:multipart/mixed
Subject: server shutdown !!!!!!
charset:Windows-1251
$boun
Content-type: text/plain
Сервер упал!!!
```

Текст сообщений короткий. Копия сообщения отправляется на реальный почтовый адрес, а само сообщение на почтовый адрес сервиса SMSMAIL (**http://www.smsmail.ru/**). Этот сервис платный, но платить придется лишь 4 цента за сообщение сервера об аварии.

Теперь, когда все задачи выполнены, сервер может выключаться в соответствии с условиями, указанными в настройках электропитания.

Таким образом, перебои электропитания не приведут к некорректному выключению сервера и связанному с этим риску потери данных. Более того, применение дополнительного источника электроэнергии может сохранить работоспособное состояние сервера на продолжительное время. В наши дни, с учетом угрозы террористических акций, применение средств резервного питания может быть весьма актуальным для многих сетей. Но бесперебойность работы сети связана не только с бесперебойным питанием сервера. Даже когда большинство процессов в сети автоматизировано, необходимость вмешательства администратора может быть не таким уж редким явлением.

Удаленное администрирование

Чтобы можно было вмешиваться в работу сети или оказывать помощь пользователям сети, необходимо обеспечить возможность доступа к серверу и компьютерам сети. Само собой разумеется, что, находясь около сервера, вы этот доступ имеете. Но пользователи могут работать в любое время суток, а ваш рабочий день ограничен несколькими часами. Что же делать, когда проблемы, возникшие в сети, случаются вечером или в выходной день, когда вы не обязаны находиться на рабочем месте? Все решается достаточно

просто, если обеспечить доступ к сети через Интернет. При определенном опыте вы сможете не только избавить себя от поездок на работу в неурочное время, если ваша сеть — ваша работа, но и получите возможность одновременно администрировать две и более сети, находясь дома.

В *главе 4* мы рассматривали доступ к рабочей станции из Интернета. Для администрирования сети необходим доступ к серверу. В большинстве случаев этот доступ требуется только администратору и позволяет оперативно решить проблемы пользователей, находясь даже на значительном расстоянии от сервера. Для доступа к серверу можно использовать сразу несколько предназначенных для этого средств. Их можно применять как альтернативно, так и комплексно. Например, доступ к удаленному рабочему столу или Radmin *(см. главу 6)* можно применять как самостоятельно, так и совместно с OpenVPN *(см. главу 10)*, что позволит уменьшить число открытых портов и снизить риск несанкционированного доступа к серверу. Ведь для того чтобы воспользоваться удаленным доступом к рабочему столу или программой Radmin, достаточно знания имени пользователя и пароля. Эти данные при определенных неблагоприятных обстоятельствах могут быть похищены. Применение OpenVPN требует дополнительно применения файла ключа. Если имя пользователя можно увидеть на экране компьютера, когда происходит авторизация пользователя, а пароль можно подсмотреть во время его набора с клавиатуры или подобрать с помощью специальных программ, то файл ключа для OpenVPN можно получить, только имея уже доступ к серверу. Если доступ к файлу ключа есть только у администратора, а из Интернета нет прямого доступа к серверу, то вероятность взлома такой защиты резко снижается. Причем комплексное применение описанных средств практически не усложняет процедуру доступа к серверу. Включая дома компьютер, я запускаю клиентскую часть OpenVPN. На сервере сети всегда запущен сервер OpenVPN, что позволяет подключиться к нему в любой момент. Образовавшийся защищенный канал доступен только мне. При этом есть возможность как "обычного" сетевого доступа к серверу, так и возможность работы с ним через удаленный доступ к рабочему столу или через программу Radmin. Более того, Radmin позволяет в этом случае получить доступ к любой рабочей станции сети, на которой установлена эта программа. Для чего используется штатная возможность программы устанавливать подключение через другой компьютер, в данном случае через сервер сети.

Если еще принять во внимание возможность управления сервером через Web-интерфейс *(см. главу 7)* и Telnet, то вы можете получить набор средств для администрирования сети, который позволит в безопасном режиме выполнять любые операции в удаленном режиме.

Приведу несколько примеров, когда возможность такого режима работы позволяла экономить время как мне, так и пользователям сети.

Дежурный администратор

Ввиду того, что наша сеть работает круглосуточно, как и многие ее пользователи, есть необходимость оперативного вмешательства в ее работу при возникновении нештатных ситуаций. А ситуации такие возникают, как оказалось, не так уж и редко. Хорошо, когда есть определенный штат работников группы поддержки. Но это могут себе позволить только крупные сети. В сетях, подобных той, где мне приходится работать, группа поддержки нередко состоит из самого администратора сети. И так получается, что этот администратор всегда дежурный администратор. К кому можно обратиться в два часа ночи, если через час должна начаться важная работа, но в сети возникла проблема, которая не даст выполнить эту работу? Конечно, к дежурному администратору. Я не помню, сколько раз мне приходилось рассказывать ночным пользователям по телефону, как выйти из сложившейся ситуации, сколько раз приходилось прерывать свой отдых и выезжать им на помощь, когда им не удавалось выполнить все, что я пытался им объяснить. Так уж случилось, что иначе поступать было нельзя — слишком высокая ответственность лежала на сети, в которой мне пришлось быть администратором. Я стал уставать от этих проблем. Выход был найден, он состоял в организации удаленного доступа к сети с соблюдением мер безопасности, которые можно считать достаточными для нашей сети. Когда все настройки и испытания были завершены, некоторое время проблем в сети не возникало. Но сеть растет, в ней появляются новые устройства, новые пользователи, новые проблемы.

И вот, в один из приятных субботних вечеров раздается телефонный звонок.

— Александр Владимирович, у нас проблема. Перестала работать программа N! Что нам делать?

Про себя думаю: "Что делать, что делать — маршрутизатор перезагрузить надо". Если бы это случилось еще месяц назад, пришлось бы ехать на работу. Голосу же на другом конце телефонной линии сообщаю, что волноваться не надо, прошу подождать минут пять, и если программа N не заработает, то позвонить снова.

Далее подключаюсь к серверу, запускаю сеанс Telnet и перезагружаю маршрутизатор. Проверяю режим его работы в том же сеансе. Убедившись, что все работает нормально, иду пить чай... Через пять минут звонка не последовало.

Вскоре в сети появился свой почтовый сервер. Пользователи получили возможность обмениваться внутренней и внешней почтой. Настройку почтовых клиентов у пользователей выполнял мой помощник, и пользователи часто не знали даже своего почтового пароля, который был сохранен на их рабочей станции. И вот, в радостный воскресный день очередной телефонный

звонок. На этот раз совсем не из моего предприятия, а из квартиры, где проживало важное должностное лицо. Оно (лицо) вспомнило, что не проверило почту в пятницу, а там должно быть сообщение чрезвычайной важности. Необходимо помочь получить почту на домашний компьютер. Что ж. Продиктовать настройки почтового клиента не сложно. А вот вспомнить пароль, которого я и не знал, как и сам пользователь, мне не удалось. Ну, так что ж, подключаемся через Web-интерфейс к почтовому серверу и меняем пароль пользователя. Процедура заняла три минуты. Из телефонной трубки сыплются благодарности, а я радуюсь, что и в этот раз не пришлось выезжать на работу в выходной день ни мне, ни должностному лицу.

Очередной телефонный звонок. На этот раз я только что приехал с работы. Этот пользователь не отличался знанием ПК, выполняя работу автоматически. До тех пор, пока компьютер не проявлял своей индивидуальности и работал "как все", все шло гладко. Но теперь окно программы застыло и не позволяло выполнить обычные для пользователя действия. Я порекомендовал перезагрузить компьютер, на что последовал неожиданный для меня вопрос — а как? В некотором замешательстве я стал объяснять про то, что на системном блоке есть такая кнопочка...

— А какого она цвета? — спросил пользователь.

— Кажется, зеленого.

— Нажал.

— Что видите на экране?

— Ничего, экран черный.

— ???, попробуйте еще раз нажать.

— Нажал, на экране все то же самое, что было до перезагрузки.

— Ничего не делайте, подождите. Вы увидите, когда можно будет продолжать работу.

С этими словами я положил трубку, поняв, что пользователь вместо кнопки <Reset> нажимал на кнопку выключения питания монитора. Объяснять еще что-либо было бесполезно.

Снова подключаемся к серверу по каналу OpenVPN. На компьютере пользователя установлена программа Radmin, но в обычном состоянии она не запущена. Вхожу в терминальную сессию на сервере с правами администратора домена. Подключаюсь к компьютеру пользователя в режиме управления компьютером, запускаю службу Remote Administrator. Через Radmin перезагружаю компьютер пользователя. Есть, как вам известно, и другие средства дистанционной перезагрузки рабочей станции, но в этот раз просто не пришло в голову, что можно воспользоваться `shutdown` из командной стро-

ки. Это не сложнее, чем с использованием Radmin, и выглядит примерно так:

```
shutdown -r -f -m \\имя_компьютера -t 30 -c "Подождите, идет перезагрузка" -d up:125:1
```

Правда, для ОС младше, чем Windows 2000 команду применить не удастся.

Возможно, что проблему можно было решить более мягкими средствами, но перезагрузка для Windows — универсальное лекарство, когда нет времени разбираться в тонкостях ситуации.

Резервирование и архивирование данных

Бесперебойность работы сети обеспечивается множеством средств. Одно из них, это резервирование данных. Говорят, что береженого Бог бережет, даже когда вы уверены, что ваш сервер защищен от неприятностей, и данные пропасть не могут, скорее всего, вы не учли еще какую-нибудь мелочь. Недавно меня вызвал директор предприятия и спросил: "А что будет, если в серверной произойдет пожар, и не сработают средства пожаротушения? Можно ли в этом случае спасти данные, а позднее восстановить работу системы?"

Первое, что вам, вероятно, пришло в голову, это спасение сервера, вынос его из огня. Но наш сервер закреплен в стойке, и снять его с нее быстро не получится. Но и в этом случае можно найти выход. Существуют съемные винчестеры. Если установить такой винчестер на компьютер, выполняющий функцию хранителя архива, то в случае необходимости его можно просто вынуть и вынести из опасной зоны. Конечно, если пожар уничтожит оборудование, его придется восстанавливать, но продуманно организованный архив данных позволит восстановить работоспособность системы почти без потери данных и функциональности. Как же организовать архивирование данных, чтобы обеспечить их восстановление в различных неблагоприятных ситуациях?

В зависимости от вида данных и их количества могут быть применены различные способы их архивирования. Для резервного копирования данных можно применять как специализированные устройства, например, стримеры, так и обычные магнитные носители или компакт-диски. На CD-R удобно хранить дистрибутивы и данные, которые не будут изменены в обозримом будущем. Данные, которые могут меняться относительно часто, можно сохранять на CD-RW, заменяя устаревшую версию данных новой.

Но сохранение данных на CD сложно автоматизировать, для записи на компакт-диск необходима предварительная подготовка, систематизация и отбор данных. Применение дополнительного съемного винчестера позволяет полностью автоматизировать сохранение оперативно изменяющихся дан-

ных. С него же, при необходимости, можно копировать данные на компакт-диски.

Какие данные необходимо сохранять? Если есть такая возможность, то абсолютно все. Если вам приходилось переустанавливать ОС на своем компьютере, возможно, вы обнаруживали, что не все данные после переустановки системы оказывались на месте. Что-то было забыто при предварительном сохранении. Если бы сохранилась копия всей системы, то пропавшие при переустановке ОС данные можно было бы восстановить. Данные на сервере требуют еще более ответственного отношения к себе.

По нашему опыту удобно процедуры архивирования и резервирования данных разбить на три группы.

- Резервное копирование текущих данных.
- Резервное копирование системы.
- Архивирование исторических данных.

Архивирование исторических данных — это их запись на внешние носители с целью освобождения места на винчестере, и обеспечение доступа к данным при необходимости. Эта работа проводится вручную перед очисткой дисков сервера. Вид данных, подлежащих архивному хранению, определяется требованиями к вашей сети.

Резервное копирование — это копирование с целью оперативного восстановления данных на винчестерах серверов в случае фатального сбоя. Для оптимизации процессов резервного копирования полную копию системы можно делать через относительно большие интервалы времени, например, один раз в три месяца, копии изменившихся данных следует делать сразу после изменения. Лучше всего ежедневно отслеживать изменившиеся или добавленные файлы и копировать их.

Дело системного администратора, какие средства он выберет для копирования данных. Здесь мы рассмотрим применение программы Acronis для резервного копирования и восстановления системы в целом, а также команду `Xcopy` для копирования изменившихся данных.

Acronis True Image Server — резервное копирование всей системы

Эта программа позволяет сделать резервную копию всей системы, давая возможность администратору проводить быстрое восстановление ее после серьезных сбоев, связанных с потерей всей информации, включая настройки самого сервера. Программа имеет несколько версий, предназначенных для работы на разных уровнях системы от рабочей станции до сети в целом.

По ссылке **http://www.acronis.ru/enterprise/products/ATISWin/** можно найти всю информацию об этом продукте.

В качестве примера рассмотрим работу с одной из серверных версий, позволяющей делать резервные копии сервера (рис. 11.5).

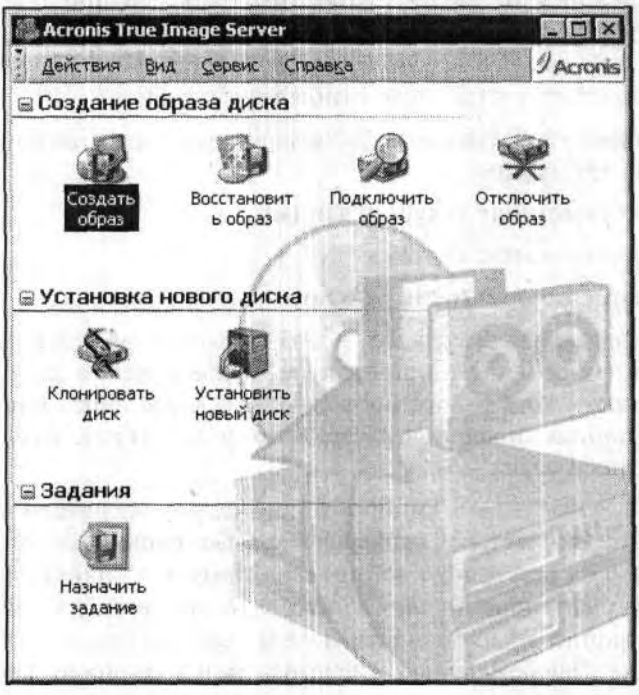


Рис. 11.5. Окно программы Acronis True Image Server

Можно создавать образ системы по команде администратора, но можно и запланировать создание образа с помощью планировщика заданий, встроенного в программу. Важно, что для восстановления системы из образа не требуется установленная ОС на сервере или другом компьютере. Загрузка может быть выполнена с компакт-диска, который поставляется с дистрибутивом или записывается пользователем (администратором). Интерфейс программы практически не меняется в зависимости от вида запуска.

Для каждого выбранного действия запускается мастер, в частности, при создании образа диска запускается мастер создания образов. С помощью мастера можно выбрать диск или отдельный раздел, образ которого необходимо создать (рис. 11.6).

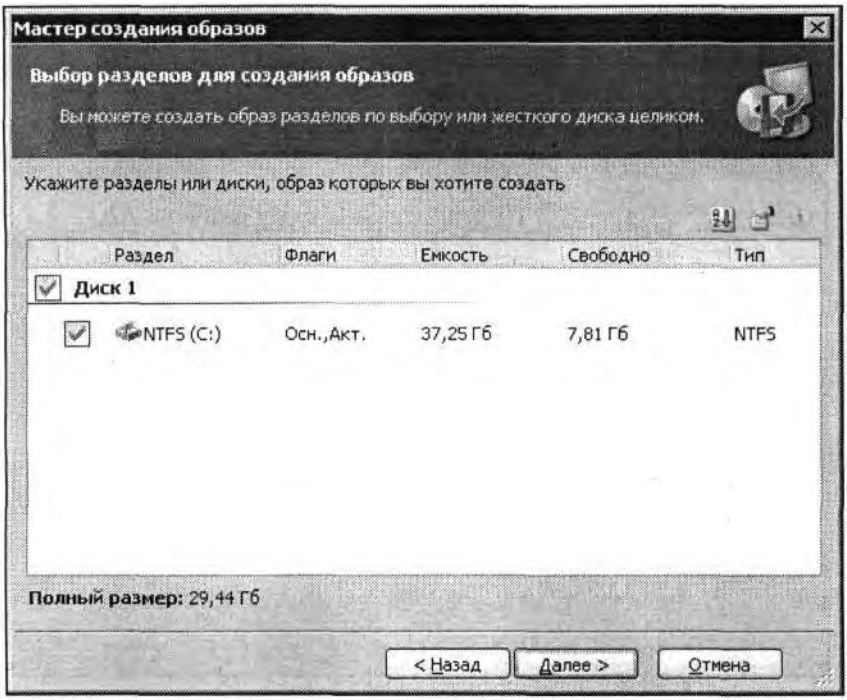


Рис. 11.6. Окно **Мастер создания образов** программы Acronis True Image Server (выбор разделов)

Выбрав диск и/или раздел и нажав кнопку **Далее**, мы можем выбрать место сохранения архива (рис. 11.7). Причем это может быть любой сетевой каталог на любом компьютере или сервере. Естественно, что программа потребует указания пароля и имени пользователя для подключения к каталогу. Далее будет предложено выбрать вид копии — полная или инкрементная. Инкрементная копия (копируются только изменившиеся части системы) создается в случае, если полная уже была создана ранее. Если при существующем уже архиве выбрать создание полной копии, то архив полностью заменяется.

Создав образ диска, вы можете быть уверены, что даже катастрофический сбой на сервере не приведет к полной потере данных. Образ можно восстановить даже на новый сервер аналогичной конфигурации.

Кроме восстановления диска или раздела, созданный образ можно использовать для поиска и восстановления данных, которые случайно были удалены после создания образа. Для этого достаточно подключить образ в качестве сетевого диска (рис. 11.8).

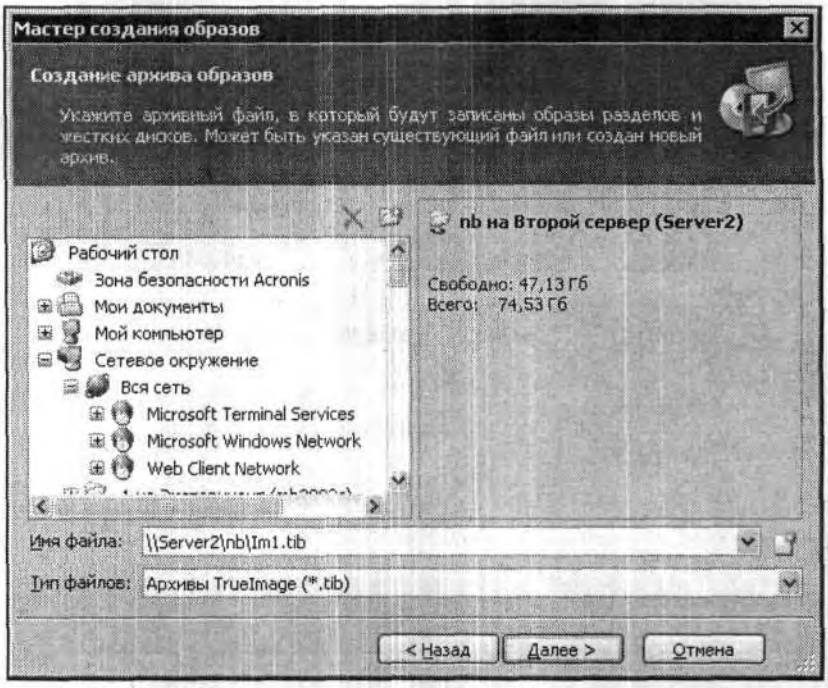


Рис. 11.7. Окно **Мастер создания образов** программы Acronis True Image Server (создание архива образов)

Подключение к образу может занять довольно продолжительное время, поскольку проводник программы должен осмотреть сеть и дать возможность подключения к любому доступному каталогу. Открыв необходимый каталог и указав на последний файл архива, можно подключить весь архив в качестве сетевого диска. Число файлов в архиве зависит от вашего выбора при его создании. Для того чтобы иметь возможность переписать архив на CD-R, размер файлов можно установить в соответствии с емкостью дисков.

Подключив образ, вы можете копировать файлы, как с обычного сетевого диска (рис. 11.9).

Чтобы отключить образ, следует также воспользоваться средствами программы.

Создание образа диска может занимать значительное время (несколько часов). При этом останавливать работу сервера нет необходимости, но следует учитывать, что дополнительная нагрузка на дисковую систему может затруднить выполнение отдельных операций сервером. Поэтому время создания образа лучше планировать на время, когда к серверу происходит минимальное число обращений пользователей.



Рис. 11.8. Окно **Мастер создания образов** программы Acronis True Image Server (просмотр архива образов)

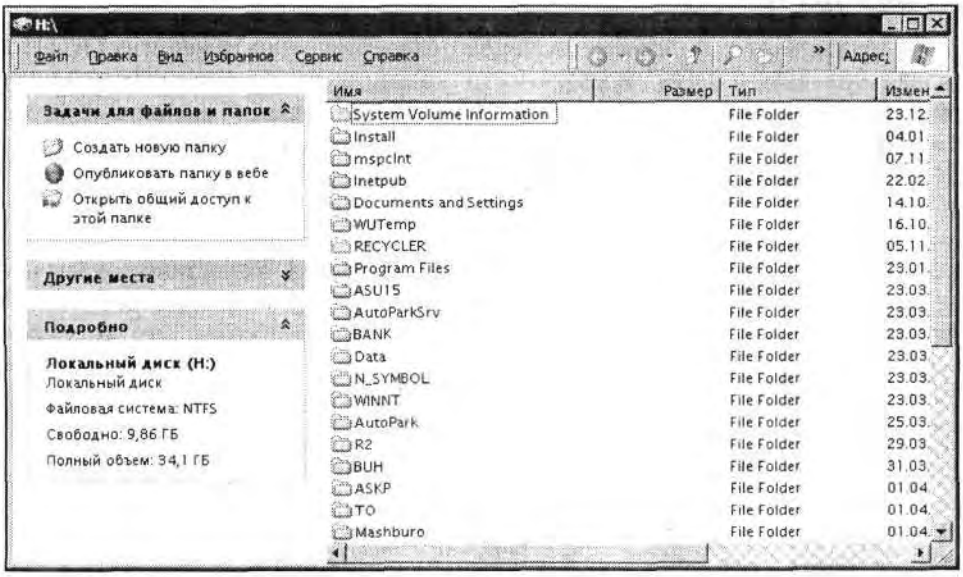


Рис. 11.9. Образ сервера, подключенный как сетевой диск

Как часто необходимо делать резервные образы? Если регулярно делаются копии данных, с которыми работают пользователи, то можно ограничиться архивами образа после существенных обновлений в системе. Важно иметь возможность восстановить работоспособность сервера, а данные можно восстановить из ежедневных архивов. К существенным обновлениям следует относить не только обновления системы через Windows Update, но и любые изменения, которые нельзя сохранить в виде файла. Например, в нашей сети пришлось сменить сетку адресов. Это потребовало изменения довольно большого числа настроек, повторять которые еще раз не хотелось бы. Следовательно, необходима новая, возможно, инкрементная копия образа системы. Такие копии можно делать как для серверов, так и для ответственных рабочих станций, настройка которых с нуля достаточно трудоемка.

Архивы желательно сохранять на съемном винчестере, что позволит спасти данные даже в очень сложной обстановке (пожар, стихийное бедствие и др.), восстановив их даже на другом сервере.

> ***Важное замечание***
>
> Создавая образ сервера на сетевом диске, например, на съемном диске другого сервера, не забудьте дать полные права на файлы в созданном каталоге учетной записи, от имени которой будет создаваться образ. Иначе программа сообщит о неправильном имени или формате файла. Для восстановления информации необходимы права на чтение каталога для всех.

Команда *Xcopy*

`Xcopy` существует в Windows с момента появления этого семейства ОС. Появилась она еще в DOS. Возможности команды `Xcopy` существенно шире, чем просто команды копирования файлов. Во время выполнения этой команды может проводиться анализ копируемых файлов, анализ уже существующего архива, а в зависимости от результатов анализа могут выполняться те или иные действия. `Xcopy`, несмотря на свою кажущуюся простоту, команда интеллектуальная, что позволяет ее использовать при автоматизации копирования данных в целях их резервирования. Успешным оказывается применение этой команды и для отбора каких-либо файлов с целью передачи кому-либо или куда-либо для дальнейшей обработки. Это могут быть ежедневно формируемые файлы с информацией о постоянно идущих процессах, например, которые требуются для отчетов или для участия в других процессах.

Если вам не приходилось использовать программу `XCopy` в целях создания резервного архива данных, посмотрите листинг 11.4, в котором приведены команды, необходимые для этой процедуры. Это реальный пакетный файл, работающий в реальной сети. Вам потребуется только изменить пути к файлам, чтобы заставить его работать в вашей сети.

Листинг 11.4. Файл CopyData.bat

```
@ echo off
xcopy /c /y /z /i /e /d C:\AutoPark \\Server2\Archive\Autopark\AutoPark\
    >C:\ASU15\ArchAutoPark.txt
if errorlevel 4 goto lowmemory
if errorlevel 2 goto abort
xcopy /c /y /z /i /e /d /exclude:C:\ASU15\exclude.txt C:\AutoParkSrv
    \\Server2\AutoParkSrv\ >C:\ASU15\ArchAutoParkSrv.txt
if errorlevel 4 goto lowmemory
if errorlevel 2 goto abort

goto exit

:lowmemory
echo Недостаточно памяти
echo или неверный путь.
goto exit

:abort
echo Нажата Ctrl + C .
goto exit

:exit
```

Что же делает этот файл? Рассмотрим его работу подробнее.

Прежде всего, отметим, что в процессе выполнения команды производится анализ возможных проблем и при их возникновении выполнение останавливается. Это возможно благодаря тому, что `XCopy` генерирует значение переменной `errorlevel` в зависимости от ситуации, и выполнение файла продолжается со строки, следующей за меткой, на которую ссылается команда `goto` (перейти). Вся информация о работе программы записывается в текстовые файлы, которые можно просмотреть в любое время после завершения копирования.

Но самые важные инструкции команды находятся в параметрах, указанных через слеш ("/") после самой команды.

Приведем описания параметров, которые использованы в этом файле.

- `/c` — игнорирует ошибки. Если в процессе копирования встретится нечитаемый файл и копирование его невозможно, то процесс копирования перейдет к следующему файлу.

- `/y` — устраняет выдачу запроса на подтверждение перезаписи существующего конечного файла. (При автоматическом копировании нет оператора, который сможет подтвердить необходимость действия.)
- `/z` — копирует по сети в режиме перезапуска. Если возникают проблемы в сети и копирование в сетевой каталог временно становится невозможным, процесс возобновляется до успешного завершения.
- `/i` — если источником является каталог, или источник содержит подстановочные знаки, и результат не существует, то команда `Xcopy` считает, что результат — это имя каталога, и создает новый каталог. Затем `Xcopy` копирует все указанные файлы в новый каталог. По умолчанию команда `Xcopy` запрашивает подтверждение, является ли параметр-результат каталогом или файлом.
- `/e` — копирует все подкаталоги, включая пустые.
- `/d[:мм-дд-гггг]` — копирует только файлы, измененные не ранее заданной даты. Если не включить значение `мм-дд-гггг`, команда `Xcopy` копирует все файлы-источники, которые новее существующих файлов-результатов. Эта возможность позволяет обновлять только измененные файлы, что, в свою очередь, снижает нагрузку на сеть.
- `/exclude:файл1[+[файл2]][+[файл3]]` — определяет список файлов, содержащих строки с именами файлов, которые копировать не следует.

Другие параметры команды `Xcopy` вы сможете посмотреть в справке. Но уже тех, что приведены в этом файле, достаточно для выполнения множества задач копирования данных.

Задание на копирование помещается в планировщик Windows, и его расписание настраивается на удобное для копирования время (например, ночное).

По завершении процесса копирования создается файл с отчетом о скопированных файлах. Приведем содержание одного из двух файлов, создаваемых после копирования (листинг 11.5).

Листинг 11.5. Файл ArchAutoPark.txt

```
C:\AutoPark\EXPORT\KADR.TXT
C:\AutoPark\EXPORT\OutMat.TXT
C:\AutoPark\EXPORT\PARK.TXT
C:\AutoPark\EXPORT\PROBEG.TXT
C:\AutoPark\EXPORT\README.TXT
C:\AutoPark\EXPORT\SKLAD.TXT
C:\AutoPark\REP\$$\FsMv1_02.rep
C:\AutoPark\REP\$$\FUELC_02.REP
```

```
C:\AutoPark\REP\$$\Ms071_02.rep
C:\AutoPark\TJR\15.ecn
C:\AutoPark\TJR\rmtagent.erh
Скопировано файлов: 11.
```

Когда процесс копирования отлажен, заглядывать в эти файлы приходится не часто. Но при возникновении проблем они могут помочь разобраться в причинах.

Нестандартные инструменты администратора

В значительной степени бесперебойность работы сети зависит от наличия удобных инструментов администрирования. Значительная часть таких средств может быть создана самим администратором или найдена у других "админов", уже создавших себе комплект удобных инструментов. Каждая сеть имеет свои особенности, и инструменты придется "затачивать" именно под вашу сеть. Тем не менее, иметь в качестве исходного материала готовый набор инструментов полезно. Не придется, по крайней мере, изобретать велосипед. Если создание командных или пакетных файлов — достаточно распространенная задача для многих пользователей, то создание сценариев может вызывать затруднения даже у опытных администраторов. В то же время современные операционные системы позволяют использовать сценарии с ощутимой пользой для администратора. Сценарии (распространено еще название "скрипты") позволяют выполнять множество задач простыми средствами, настраивая эти средства под определенные задачи. Это позволяет отказаться в ряде случаев от поиска специализированных программ, но требует знакомства с языками сценариев. Для упрощения работы по созданию своего набора инструментов для администрирования растущей сети приведем несколько сценариев, которые можно использовать при создании своих. Кроме сценариев можно применять и другие средства, которые, несмотря на свою простоту, почему-то не используются многими администраторами, даже когда эти средства могут снизить трудоемкость их работы.

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, находящийся на одном из компьютеров сети, может потребоваться очень продолжительное время. Проводя поиск со своего рабочего места, администратор может сократить это время и 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 из сети. 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 апплет **Управление компьютером**.
2. В появившемся окне **Computer Management** (Управление компьютером) 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 **ОК** в этом и следующем окне.
5. В окне **Выбор компьютера** после поиска компьютера появится его полное имя, нажмите **ОК**, если выбор верен.
6. Теперь в окне **Commuter Management** вы увидите консоль управления удаленным компьютером, имя которого указано рядом со значком компьютера в правой части окна (рис. 11.10).
7. Кликните на папке **Общие ресурсы** в правой части окна, в левой части вы увидите список общих ресурсов.
8. Кликните правой кнопкой мыши на папке **Общие ресурсы** в правой части окна. Выберите **Новый общий ресурс**. В открывшемся окне мастера создания общей папки введите имя папки, в которой вы намерены осуществить поиск (рис. 11.11). Если вы не помните имя, то с помощью кнопки **Обзор** выберите в дереве папок необходимое и нажмите **ОК**.
9. Введите имя общего ресурса и его описание, нажмите **Далее**.
10. В следующем окне выберите необходимый тип доступа и нажмите **Далее**.
11. Если не требуется еще один общий ресурс, откажитесь от его создания.

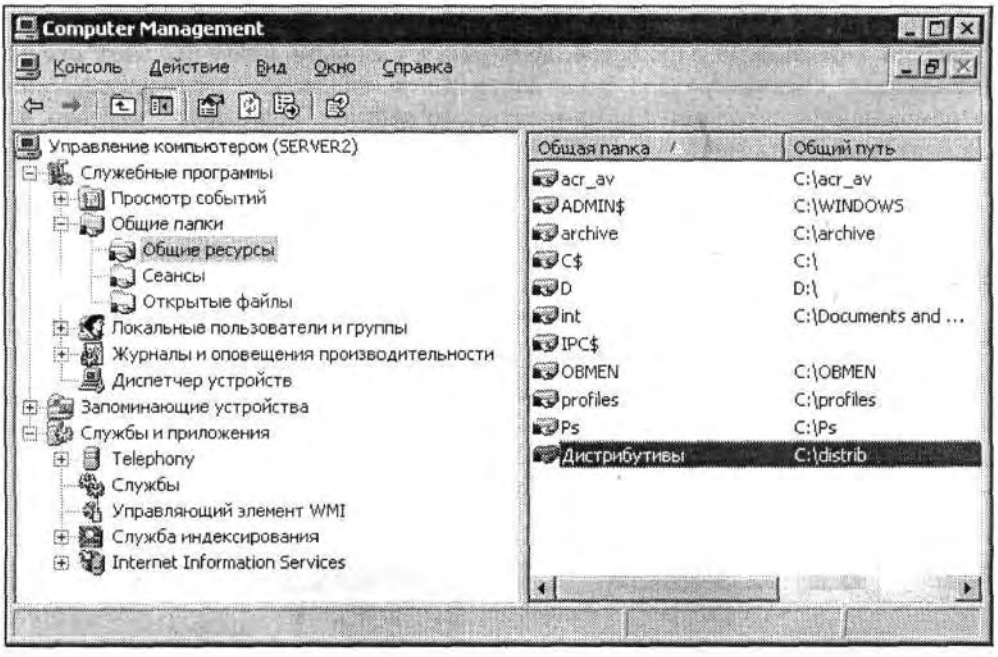


Рис. 11.10. Окно **Commuter Management**

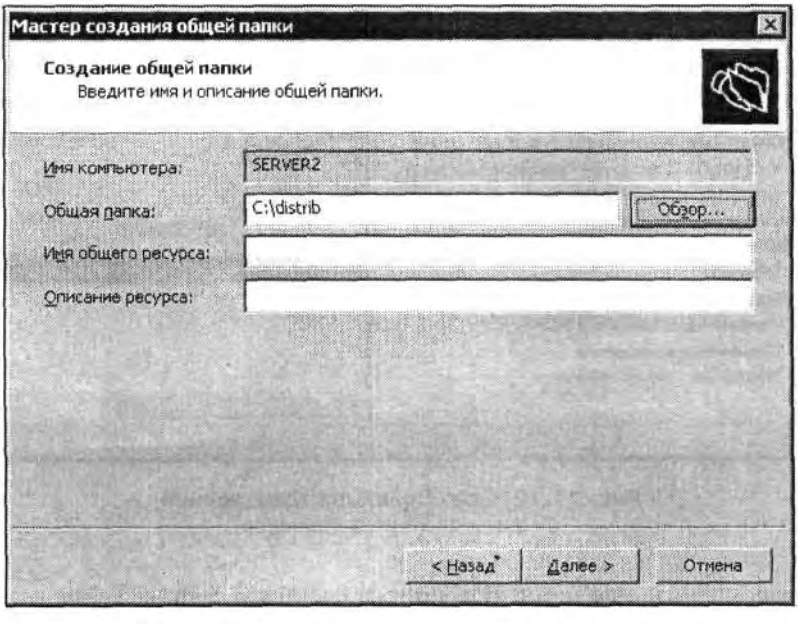


Рис. 11.11. Окно мастера создания общей папки

На рис. 11.12 можно видеть только что созданный общий ресурс **Дистрибутивы** на компьютере SERVER2. Если вы установили права на этот ресурс только для администратора, то в дальнейшем его можно использовать повторно, не опасаясь несанкционированного доступа. Если позволительно, то можно установить необходимые права на этот ресурс и для других пользователей.

Теперь достаточно найти данный ресурс в сетевом окружении и подключить на своем компьютере в качестве сетевого диска. Поиск файлов теперь возможен обычными средствами Windows. При необходимости можно создать общие ресурсы, доступные администратору на всех машинах сети и осуществлять в них поиск.

Окно **Commuter Management**, которое мы использовали для поиска файлов, может применяться 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.

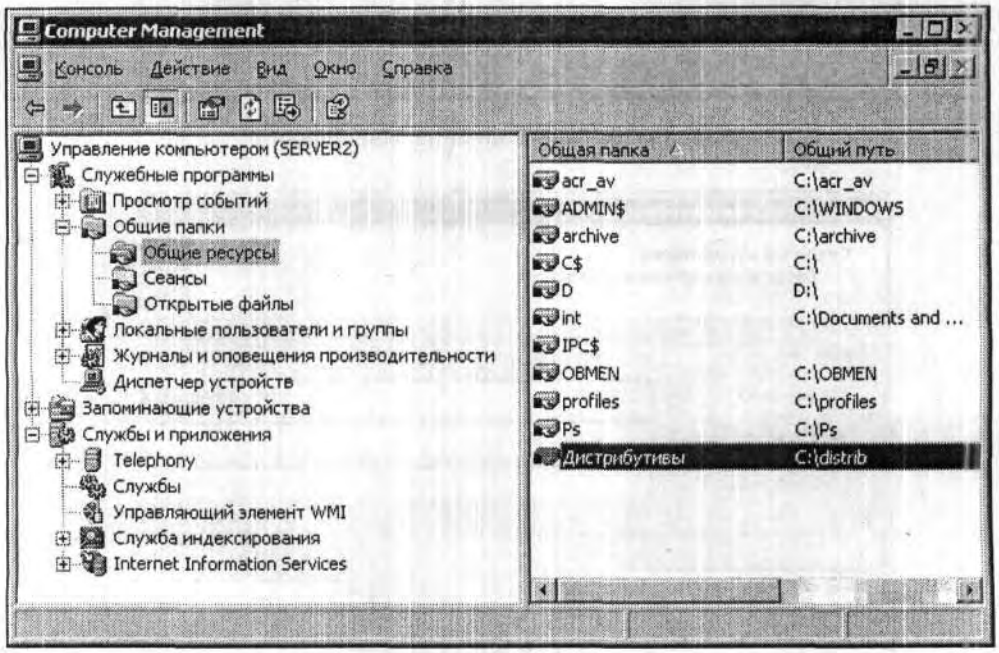


Рис. 11.12. Окно **Commuter Management** (создан новый общий ресурс)

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 **Управление компьютером (Commuter Management)** для запуска этой службы на удаленной машине. В открытом и подключенном к выбранному компьютеру окне **Commuter 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 (рис. 11.13). Нужно предварительно внести свою учетную запись в группу **TelnetClients** (в том же окне **Локальные пользователи и группы | Группы | TelnetClients**).

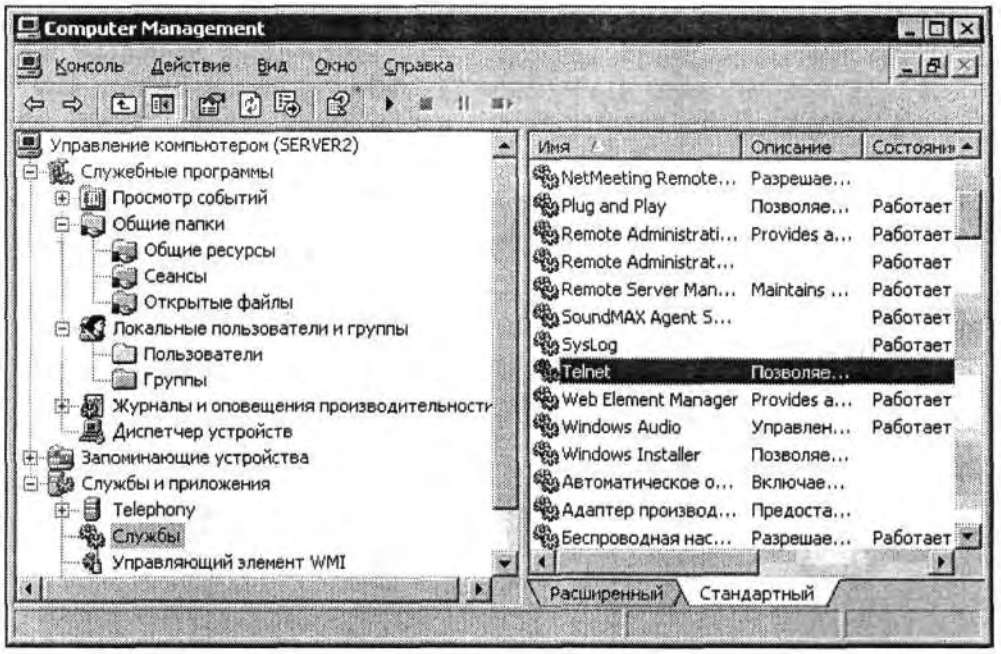


Рис. 11.13. Окно **Commuter Management** (Telnet)

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 (рис. 11.14). 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. 11.14. 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 ра-

боты 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. Для подготовки описываемых далее средств работы с файлами необходимо некоторое знакомство со сценариями на языке JScript.

Примечание

Ввиду ограничения длины строки в текстах сценариев, помещенных далее, будьте, пожалуйста, внимательны при их повторении. В текстах книги возможны неожиданные переносы строк, которые в реальных текстах сценариев переноситься не должны. Если вам трудно самостоятельно обнаружить такие места, то воспользуйтесь реальными файлами, которые можно найти по адресу в Интернете **http://www.okobox.narod.ru/scripts.htm**. Если какого-либо сценария из тех, что описаны далее, вы не найдете на указанном сайте, то пишите автору, он обязательно исправит ситуацию. Написать можно в раздел "Вопрос-ответ" на главной странице сайта.

Регулярные выражения

В описываемом далее сценарии применяются регулярные выражения, использование которых позволяет описать маски имен файлов для поиска, что, в свою очередь, позволяет гибко управлять критериями поиска. Краткое описание некоторых регулярных выражений приведено в табл. 11.1.

Таблица 11.1. *Регулярные выражения*

Регулярное выражение	Описание
.	Любой отдельный символ
*	Повторение любого символа в любом количестве или нет символов
+	По крайней мере один или большее количество предшествующих символов. Например, `ba+c` соответствует `bac`, `baac`, `baac`, но не `bc`

Таблица 11.1 (окончание)

Регулярное выражение	Описание
^	Начало строки
$	Конец строки
[]	Любой из символов, содержащихся в скобках, или любой из диапазона ASCII-символов, 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
[^]	Любой символ кроме тех, что после символа "^" в скобках или входящих в диапазон ASCII-символов, 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 ранее. Например, `100$` соответствует 100 в конце строки, но `100\$` соответствует набору символов 100$ в любом месте строки

В сценарии (листинг 11.6) использовано выражение `"^[д].*[t]\.doc$","i"`, которое соответствует имени DOC-файла, начинающегося на "д" и оканчивающегося на "t".

Листинг 11.6. 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

Часто возникает необходимость получения списка файлов, находящихся в папке. Это могут быть LOG-файлы, файлы, хранящие результат работы других сценариев, имена которых содержат дату и время выполнения. Во многих случаях такой список может стать документом, подтверждающим выполнение каких-либо процедур в определенные моменты времени. Вручную составлять подобные списки затруднительно, да и зачем, если есть средства автоматизации.

Листинг 11.7. 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 сценарии из листингов 11.6 и 11.7, используя некоторые особенности каждого из них. Так, в последнем применяется объект `SpecialFolders`, позволяющий обратиться к специальным папкам Windows, не указывая пути к ним. Кроме того, в последнем сценарии информация выводится не только на экран, но и в файл. При дальнейшей модификации можно 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 как файлов, так 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 хотелось бы в отдельном каталоге, а после их накопления хотелось бы устаревшие удалить. Вариант создания LOG-файла посредством сценария мы уже рассмотрели в предыдущем примере, поэтому коротко проанализируем варианты выполнения задачи и дополним ее другими функциями.

Создание файлов

Наиболее часто встречается задача создания текстовых файлов. Это либо LOG-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 команду:

```
COPY CON <ИМЯ_ФАЙЛА>
```

и нажать <Enter>. После этого можно набирать требуемый текст, а по окончании набора нажать <F6>. Набранный текст, видимый на экране вашего компьютера, будет сохранен в файле на удаленной машине.

Вариант 3

Снова JScript — листинг 11.8. В этом сценарии 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 11.8. 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

И еще один сценарий — листинг 11.9. Адреса локальные, но, как мы уже видели, их можно заменить на сетевые.

Листинг 11.9. 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, можно 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 ранее. 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 команду:

```
MD <ИМЯ_КАТАЛОГА>
```

и нажать <Enter>.

Для удаления каталога можно применить команду RD.

Вариант 3

Еще один сценарий JScript — листинг 11.10. Здесь для создания каталога приведен локальный путь (корневой каталог диска C:\), но его можно изменить на сетевой путь.

Листинг 11.10. 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 ***************************************************/
```

Сценарий из листинга 11.11 предназначен для удаления каталогов.

Листинг 11.11. 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 <Enter> скрипт будет выполнен. Для безопасного эксперимента можете использовать MkFld.js, а затем DelFld.js (два сценария, приведенные в листингах 11.9 и 11.10).

Изменение атрибутов файлов и каталогов

Обычно не часто приходится изменять атрибуты файлов, но иногда это оказывается необходимо. Например, в какой-либо каталог складываются файлы-отчеты. Регулярно требуется из этого каталога отбирать новые 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", 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:

- `+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 средст-

во, но, на мой взгляд, самое удобное. В среде PrimalScript (так называется эта программа) существует свойство завершения строк, когда после ввода имени объекта появляется список свойств и методов, доступных для него.

Кроме среды для создания сценариев, можно применить отладчик сценариев, который входит в состав Windows 2000 Server и Windows Server 2003. Его можно найти по адресу **http://www.microsoft.com/downloads**. При загрузке отладчика обратите внимание на его версию — должна быть версия не ниже 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.

Кликнув правой кнопкой на файле сценария FlsAll.js, выберем в контекстном меню **Edit With PrimalScript**. Откроется окно, показанное на рис. 11.15.

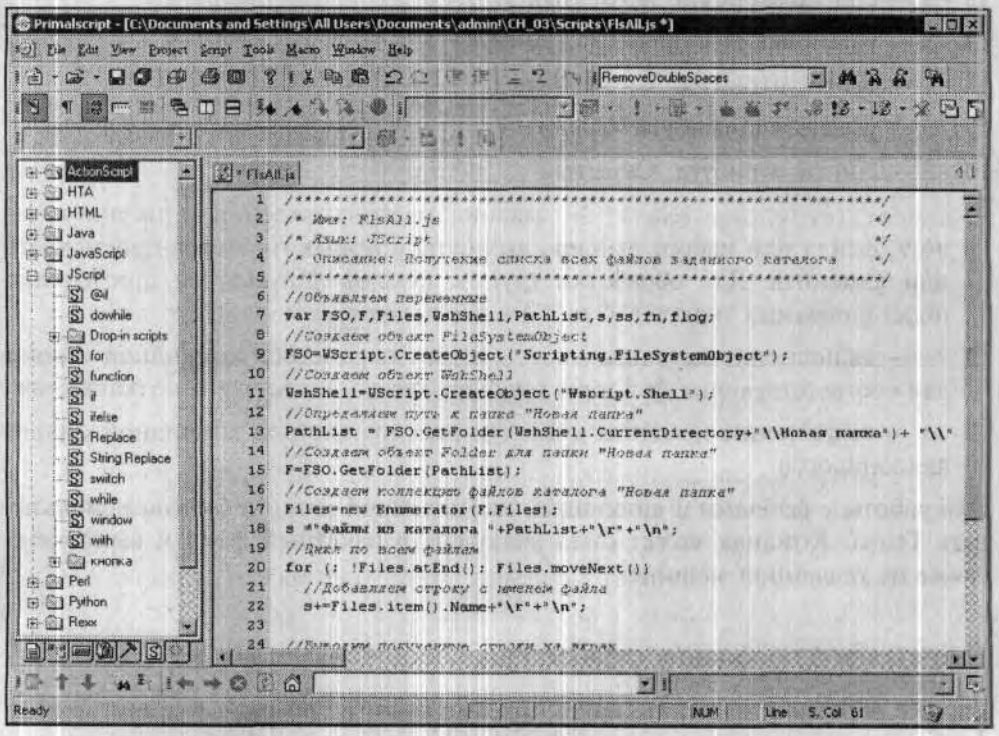


Рис. 11.15. Окно PrimalScript с открытым файлом сценария

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 указав имя нового

файла. Теперь нажмите <F7>. Сценарий будет выполнен и откроется новая вкладка **Output**, в окне которой будет результат работы сценария (рис. 11.16).

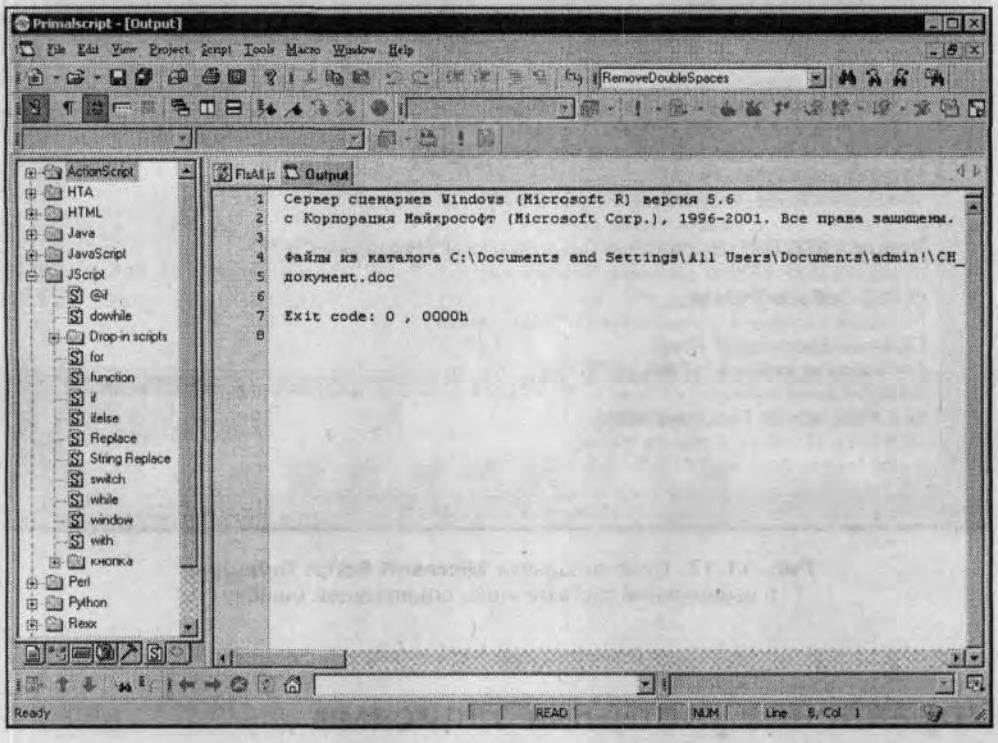


Рис. 11.16. Окно с результатом работы сценария

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 можно выполнять в пошаговом режиме (рис. 11.17).

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

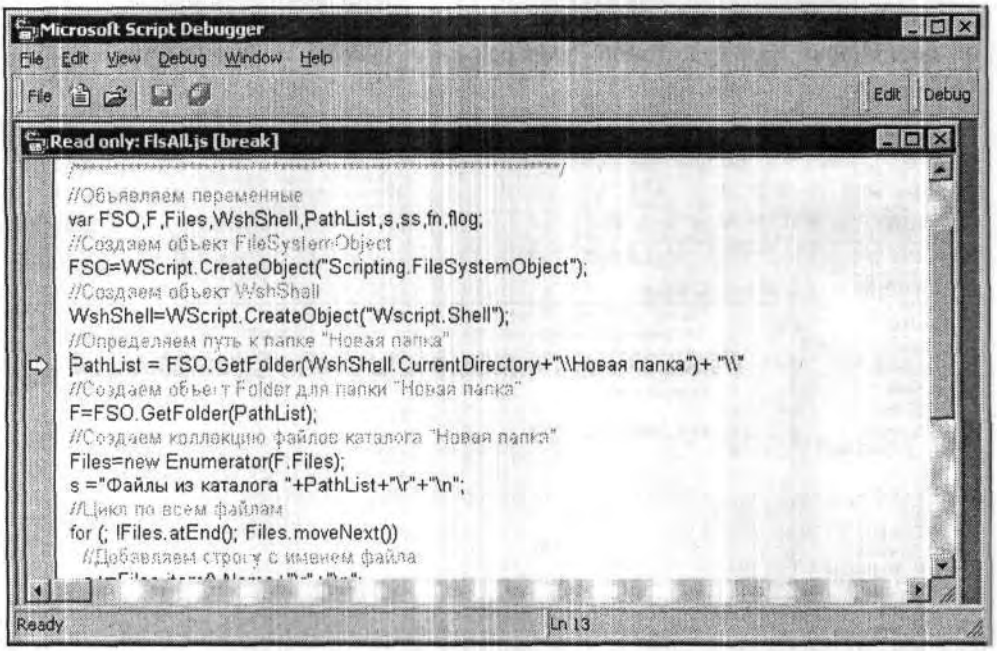


Рис. 11.17. Окно отладчика **Microsoft Script Debugger** с выделенной строкой кода, содержащей ошибку

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 выполнения подобных задач 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 **Управление компьютером**, если это не контроллер домена, просмотреть список локальных пользователей (рис. 11.18).

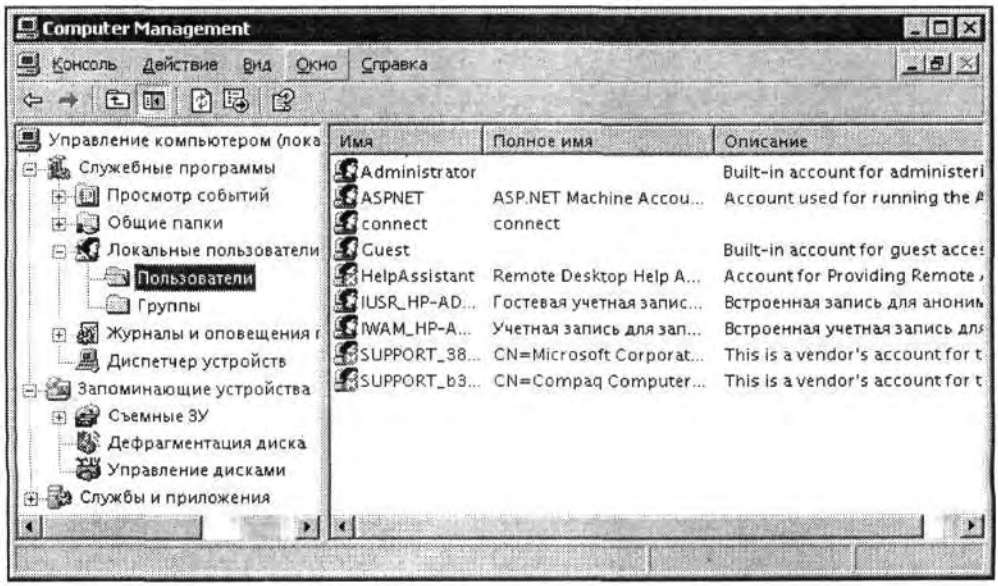


Рис. 11.18. Локальные пользователи компьютера

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 подготовлено, можно наслаждаться плодами своего труда.

Получение списка пользователей с помощью сценария VBScript

Многие задачи, решение которых может быть реализовано на VB, можно решить и с помощью VBScript. В этом случае главное, что потребуется при создании нового инструмента, — это текстовый редактор. Создайте текстовый файл, как в листинге 11.12, и измените его расширение на vbs.

Листинг 11.12. 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 11.13.

Листинг 11.13. Сценарий Users.vbs

```
'**********Список пользователей**************
'UMя - Users.vbs
'Включены полное имя и дата последнего входа в сеть
'DomainName - введите имя домена или сервера
'Требуются права 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
```

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 11.14.

Листинг 11.14. 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 11.15) 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 (выделение восклицательными знаками по обе стороны от имени группы).

Листинг 11.15. 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 дан-
ных","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 и не пытались изменить что-либо в учетных записях. Но в задачах администратора не последнее место занимают процедуры добавления, изменения, удаления объектов сети и, в том числе, изменения, связанные с учетными записями пользователей.

Внимание

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

Все сценарии и процедуры, рассмотренные ранее, универсально подходят как к сети с сервером Windows NT, так и Windows 2000/2003. Уже Windows 2000 Server позволяет организовать более сложную, но 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 ранее, 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 раньше, полностью работоспособны, если вы измените в них имена структурных единиц (OU) и имя домена на применяемые в вашей сети.

Добавление учетной записи пользователя

Сценарий, приведенный в листинге 11.16, 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 заблокированной. При вводе данных сценарий предложит значения, записанные в его тексте (значения по умолчанию), — замените их на необходимые.

Листинг 11.16. 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 должен 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 с целью организации какой-либо специальной группы пользователей. Для подготовки такого списка лучше всего подходит приложение MS Excel, позволяющее осуществлять связь данных с другими приложениями.

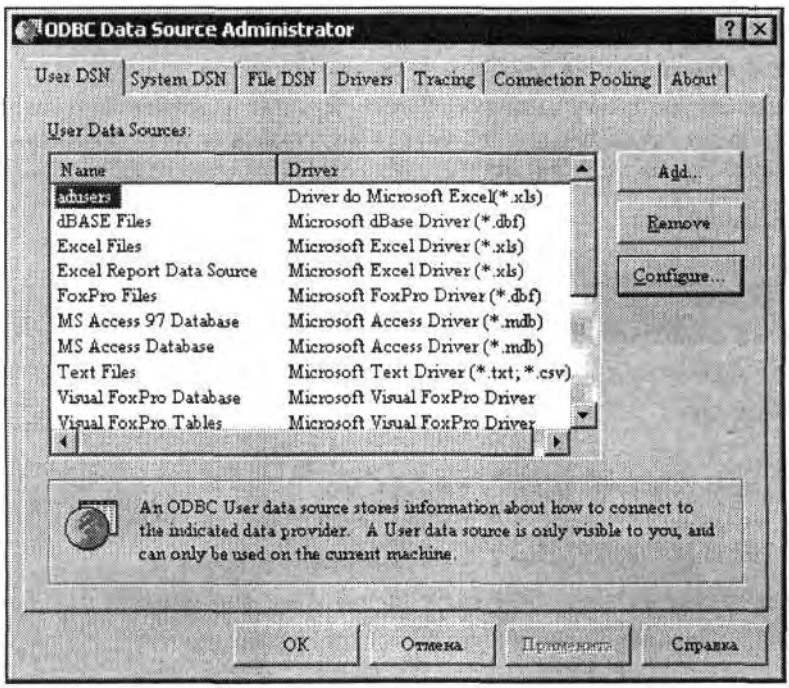


Рис. 11.19. Созданный источник данных

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. 11.19).

Сценарий из листинга 11.17 был опубликован на одном из форумов в Интернете и приводится почти без изменений.

Листинг 11.17. 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 юзеров
' См. шаблон файла в архиве и примечания к полям там же
' Кроме того, в домене должен 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
'***************************************************************************
```

В файле NewUsers.xls должен быть лист "Новые", в котором первая строка содержит 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
```

поставив одинарные кавычки перед ними (как в тексте).

В табл. 11.2 приведены несколько первых полей листа. Порядок полей значения не имеет.

Таблица 11.2. 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

Все учетные записи, созданные этим сценарием, будут заблокированы.

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 ту же самую 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, модифицировав 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 учетных записей, содержащихся в контейнере, на экран 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 в листинге 11.18 сценарий содержит строки поиска и вывода на экран имен подразделений, что не рассматривалось еще в книге. Поэтому фрагменты кода могут быть использованы для создания множества других сценариев, выполняющих различные задачи.

Листинг 11.18. 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. пользовате-
ля","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 параметры. Но иногда у администратора возникает необходимость изменить пароль пользователя (листинг 11.19). Например, есть несколько учетных записей, применяемых для временных пользователей, пароли которых известны администратору. После завершения работы временного пользователя необходимо сменить пароль учетной записи.

Листинг 11.19. 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 позволяет оперативно добавлять необходимые права. Для контроля наличия каких-либо прав пользователя достаточно получить список групп, в которые он входит. Сценарий из листинга 11.20 позволяет добавить в группу пользователя и тут же посмотреть перечень групп, в которых он состоит.

Листинг 11.20. Код UsersToGroups.vbs — добавление 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 набирать именно имя учетной записи, а не имя входа в сеть.

Изменение параметров учетной записи пользователя

Масса параметров учетной записи пользователя может быть изменена с помощью сценариев. Это может быть фамилия вышедшей замуж сотрудницы, номер телефона, номер офиса, описание и т. д. В сценарии из листинга 11.21 есть возможность изменить десять параметров. При желании их список может быть увеличен.

Листинг 11.21. 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: " & bjUser.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 списка связанных с выполнением единой задачи разрешений, применяемых для группы пользователей, определяет необходимость создания группы, в которую должны входить эти пользователи. Создание новой группы — процедура не сложная, но возможность выполнить эту процедуру с обычной рабочей станции вашей сети довольно 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 11.22) содержит процедуру создания глобальной группы, входящей в подразделение (организационную единицу).

Листинг 11.22. 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 сценарием из листинга 11.23.

Листинг 11.23. 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 к 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 11.24), а затем другими средствами настроить права более тонко.

Листинг 11.24. 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 11.25) позволяет отменить полностью общий доступ к папке.

Листинг 11.25. 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 воспользоваться сначала удалением его общего доступа, а потом назначением, но с другими параметрами.

Программы в формате HTA

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

Для успешной разработки программ в формате HTA необходимо знание основ создания HTML-страниц и написания сценариев на одном или более script-языков. 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. 11.20 и листинг 11.26.

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

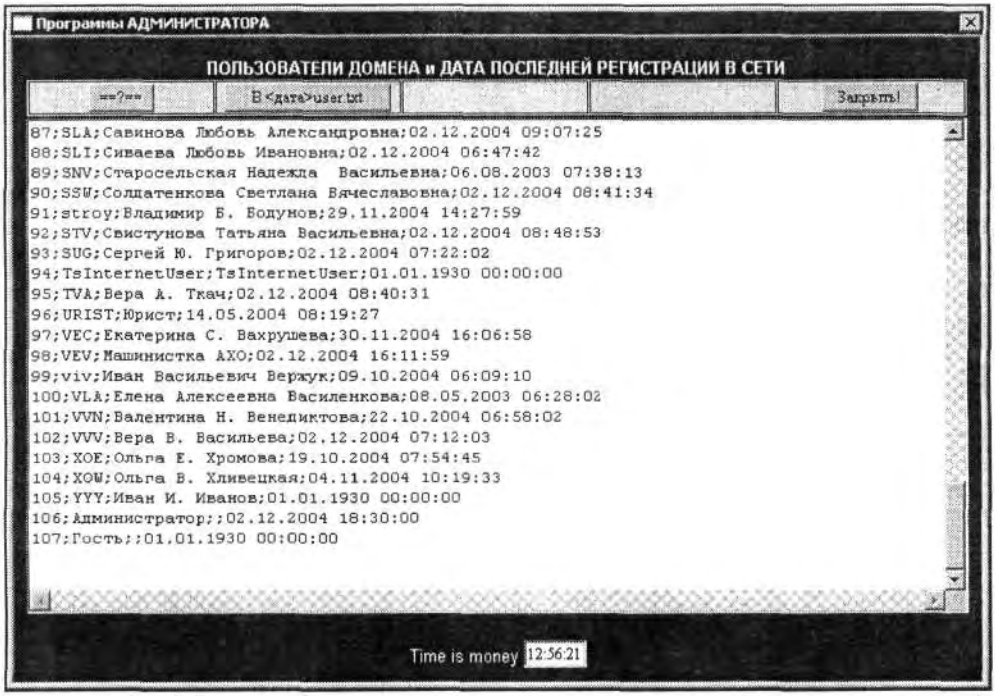


Рис. 11.20. Окно **Программы АДМИНИСТРАТОРА**

Листинг 11.26. 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 станицы идет 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" bordercolor-
dark="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>
```

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 нажатия кнопки **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 вы при запуске программы откажетесь 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 этой главе. Внимательно проверьте код сценариев и программ HTA. Все без исключения примеры действительно работают в нашей сети.

Работа сценариев на старых машинах

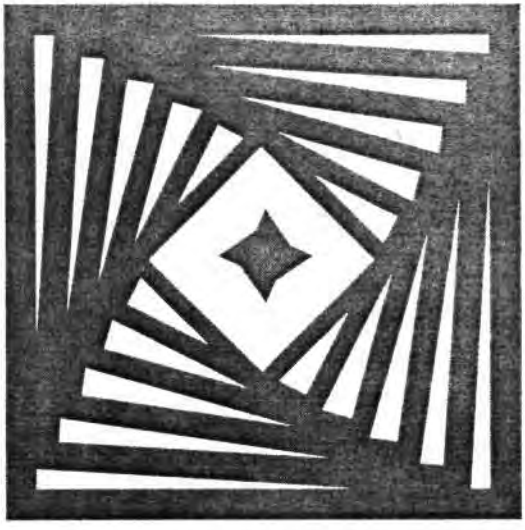
Работа со сценариями может не только принести пользу, но и предоставить возможность пользователям, не подходя к серверу, управлять им в той степени, которую допускает администратор. Например, общий доступ к ресурсу, который создал пользователь, может быть предоставлен или ограничен самим пользователем. 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, где не выполняются сценарии, для работы которых требуются провайдеры "WinNT:\\" или "LDAP:\\". Но есть

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



ЧАСТЬ V

Растущая сеть — проблемы и возможности

Как бы нам ни хотелось постоянства, оно не бывает продолжительным. Когда-то программисты создавали прекрасные программы, работающие в среде DOS, а теперь не все знают о существовании такой операционной системы. Некоторые администраторы сетей, существующих в нашем управлении, пытаясь сохранить постоянство, не переходили на новые операционные системы. Они сохраняли деньги и нервы, которые обычно тратятся в периоды серьезных модернизаций локальных сетей. Но чем дальше продвигается прогресс в области вычислительной техники, тем в большей степени проявляется необходимость взаимодействия различных сетей, тем чаще ставятся задачи, которые могут быть решены лишь при совместном использовании программных продуктов, позволяющем организовать управление предприятиями или целыми объединениями предприятий. Возможно, что вы слышали о программах Электронная Россия или Электронная Москва. Возможно, что в ваших регионах существуют аналогичные программы, которые призваны централизовать управление целыми городами. В этих программах предусматриваются как функции вычислительных сетей предприятий и управляющих структур, так и сервисы для обычных граждан — пользователей компьютеров. Уже сейчас существует множество услуг, предоставляемых через Интернет. Незаметно мы привыкаем к новым средствам общения, к возможности сделать покупки, не выходя из дома. Появилось много рабочих мест, не требующих присутствия работника в офисе организации. Теперь есть возможность получать задания, выполнять их и даже получать вознаграждение за работу, не отходя от своего персонального компьютера.

Все эти изменения были возможны потому, что на множестве компьютеров работают похожие по своим возможностям операционные системы и программы. Не развивая и не модернизируя свою сеть, вы рискуете попасть в ситуацию, когда эта модернизация станет просто необходима и потребует для ее проведения очень больших затрат. Даже домашняя (квартирная) сеть требует непрерывного развития и модернизации.



Глава 12

Некоторые проблемы администрирования

С ростом сети возникают проблемы администрирования этой сети. Проблемы могут быть вызваны применением старых компьютеров, необходимостью контроля сетевого трафика и учета большого числа машин в сети, а также необходимостью удобного и безопасного управления сетью. Некоторые инструменты, применяемые в малой сети, становятся не очень удобными, когда сеть вырастает. Рассмотрим эти проблемы подробнее.

Применение старых ОС

Но невозможно просто отказаться от старых рабочих станций и выбросить их на свалку. Многие из них до настоящего времени работают и приносят ощутимую пользу. При этом не возникает необходимости в замене ОС, установке новых версий MS Office и других программ. Однажды на мероприятии, проводимом Microsoft, я узнал из уст представителей этой компании, что до сих пор некоторые сотрудники фирмы используют Windows 3.11. Что ж, я и раньше считал, что не все старое плохо. Замена компьютера и программного обеспечения только ради замены — не слишком разумное решение. Разве есть необходимость заменять Windows XP в 2006 году на Windows Vista только потому, что эта ОС будет выпущена? Что же могут старые рабочие станции и чего они не могут в новых сетях? Как можно использовать освобождающиеся (в связи с заменой) старые компьютеры? На все эти вопросы уже не однажды были даны ответы. Если рабочая станция действительно работает, несмотря на то, что ее ОС MS-DOS, то какой смысл ее менять? Но если этот компьютер должен работать в сети, можно задуматься о реальности такого применения старой машины.

Если учесть определенные ограничения, которые накладывает прогресс на использование старой техники, определить область применения устаревших, но работающих ОС, то окажется, что машины, проработавшие 20 лет, могут

продолжать работать и далее, если их осталось немного. Они могут принести определенную пользу и в новой сети. Большому числу старых машин в новых сетях Windows, к сожалению, место найти трудно, разве что попытаться использовать их в качестве терминалов, бездисковых рабочих станций. Но это особая тема, требующая специального подхода к организации сети в целом. Если вам интересно, как можно организовать сеть на основе бездисковых рабочих станций, то начните со статьи по адресу в Интернете **http://network.xsp.ru/6_5.php**.

Наша сеть состоит из обычных рабочих станций, поэтому далее рассмотрим возможности применения в ней обычных компьютеров, но с почтенным по меркам компьютерного мира возрастом.

Настройка рабочих станций с операционной системой DOS

Начнем с рабочих станций под управлением DOS. Несмотря на бурный прогресс в области вычислительной техники и прекращение поддержки MS-DOS, в нашей стране еще работают компьютеры под управлением различных версий этой операционной системы, причем количество их весьма велико. Для доступности и универсальности подхода мы рассмотрим MS-DOS 7.1, которая входит в состав Windows 98 и наверняка доступна большинству пользователей. Несложно, выполнив команду `Sys C:`, перенести эту систему на винчестер с загрузочной дискеты Windows 98. Вы можете использовать и другие DOS, под управлением которых работают ваши компьютеры. Различные версии DOS требуют разной конфигурации памяти. Некоторые версии этой операционной системы могут работать в нашей сети не совсем так, как MS-DOS 7.1. Но если нет необходимости применять какую-либо особенную версию DOS, то почему бы не использовать MS-DOS 7.1, которая поддерживает файловую систему FAT32 и достаточно просто настраивается.

Установка операционной системы MS-DOS 7.1

Для установки и настройки этой операционной системы необходимо перенести системные файлы с загрузочной дискеты Windows 98 и дописать самостоятельно файлы конфигурации. Все файлы необходимо готовить в текстовом редакторе под управлением DOS. Можно использовать встроенный в Windows 9*x* редактор Edit.com.

Условимся, что каталог, в который устанавливается DOS, называется DOS7. В него будут помещены все необходимые файлы для работы системы, кроме

основных системных файлов. В корневом каталоге диска C: должны находиться файлы, содержание которых приведено в листингах 12.1—12.4.

Листинг 12.1. Файл Msdos.sys

```
[Paths]
WinDir=c:\dos7\
WinBootDir=c:\
HostWinBootDrv=c:\

[Options]
BootMulti=0 ; Отключает возможность множественной загрузки
BootGUI=0   ; Отключает загрузку графического интерфейса
Network=1   ; Включает возможность работы с сетью
logo=1      ; Позволяет показывать заставку (файл Logo.sys) при загрузке
```

Этот файл уже существует на диске после переноса системных файлов, и его необходимо исправить в соответствии с приведенным текстом. Заставку вы можете изготовить самостоятельно, создав в корневом каталоге файл Logo.sys из растрового рисунка с разрешением 320×400 точек.

Листинг 12.2. Файл Config.sys

```
[menu]
menuitem=D, Use Net  ; В этом разделе создается меню для выбора
menuitem=C, No net   ; вариантов загрузки
menudefault=D,10
menucolor=14,1
[D]
device=c:\dos7\himem.sys
dos=high,umb noauto
devicehigh=emm386.exe noems
devicehigh c:\net\ifshlp.sys
[C]
device=c:\dos7\himem.sys
dos=high,umb noauto
devicehigh=emm386.exe noems
[COMMON]
fileshigh=80
buffershigh=20
```

```
stackshigh=9,256
lastdrivehigh=z
INSTALLHIGH=C:\DOS7\RKM.COM    ; Загрузка русификатора, который можно
                               ; найти по ссылке:
                               ; http://win95.nm.ru/switch.htm
shell=c:\command.com /E:512 /P
FCBSHIGH=1
```

Вы можете самостоятельно изменить некоторые строки. Например, русификатор может быть любым другим, но будет лучше, если вы повторите пример полностью. Файлы emm386.exe, ifshlp.sys, choice.exe и himem.sys можно скопировать из Windows.

Листинг 12.3. Файл Autoexec.bat (вариант для начальной установки системы)

```
@echo off
set temp=c:\temp
path c:\;C:\NC;c:\dos7
lh c:\dos7\mouse

@echo "ПРИЯТНОЙ РАБОТЫ!"
```

Необходимо самостоятельно создать каталог TEMP, установить Norton Commander или другой файловый менеджер, скопировать в каталог DOS7 драйвер мыши (можно из Windows).

Листинг 12.4. Файл Autoexec.bat (окончательный вариант)

```
@echo off
set temp=c:\temp
path c:\;C:\NET;C:\NC;c:\dos7
lh c:\dos7\mouse
choice /c:SNLA /t:L,20 "Share-S сеть- N локально- L  АРАХНА- A  "
;Команда choice соответствует choice.exe из Windows.
if errorlevel 4 goto p
if errorlevel 3 goto l
if errorlevel 2 goto n
C:\NET\net initialize
C:\NET\netbind.com
C:\NET\umb.com
```

```
C:\NET\tcptsr.exe
C:\NET\tinyrfc.exe
C:\NET\nmtsr.exe
C:\NET\emsbfr.exe
C:\NET\net start
C:\NET\net start server
C:\NET\net share
cls
@echo "Сеть с доступом загружена Ctrl+Alt+N подкл.диск"
@echo "netshare - обеспечить доступ"
net
c:\net\netshare.exe
goto l

:n
C:\NET\net initialize
C:\NET\netbind.com
C:\NET\umb.com
C:\NET\tcptsr.exe
C:\NET\tinyrfc.exe
C:\NET\nmtsr.exe
C:\NET\emsbfr.exe
C:\NET\net start
cls
@echo "Сеть загружена"
net

goto l
:p   ; этот раздел файла необходим, если применяется браузер ARACHNE
c:\drv\pktdrv\hppclanp 0x60 ; пакетный драйвер сетевой платы должен быть
                            ; свой
cd\
cd arachne
arachne
:l
@echo "ПРИЯТНОЙ РАБОТЫ!"
```

Этот вариант файла пока не устанавливайте, а сохраните до заключительных действий по настройке сетевых возможностей рабочей станции DOS. В про-

цессе установки сетевого программного обеспечения файл будет изменяться автоматически, но его окончательный вид должен быть таким, как в листинге 12.4. Кроме приведенных файлов вам могут понадобиться и другие. В табл. 12.1—12.3 дан примерный перечень файлов, которые можно скопировать с загрузочной дискеты и из \Windows\Command в соответствии с их размещением на диске, полученном командой `DIR`.

Таблица 12.1. *Содержимое диска C:*

Название файла или папки	Размер файла, байт	Описание
COMMAND.COM	95 202	Командный процессор
NC <ПАПКА>		Norton Commander
NET <ПАПКА>		Директория установки клиента
DISTRIB <ПАПКА>		Дистрибутивы
EMM386.EXE	125 975	EMM386
ARACHNE <ПАПКА>		Браузер ARACHNE
TEMP <ПАПКА>		Папка для временных файлов
DRV <ПАПКА>		Хранилище драйверов
DOS7 <ПАПКА>		Системная директория
MSDOS.SYS	116	Файл MS DOS
CONFIG.SYS	432	Файл MS DOS
LOGO.SYS	129 078	Заставка
AUTOEXEC.BAT	869	Файл MS DOS

Таблица 12.2. *Содержимое папки C:\DISTRIB*

Название файла или папки	Размер файла, байт	Описание
ARCHN170.EXE	1 012 717	Браузер ARACHNE
CYRILLIC.APM	279 421	Пакет русификации для ARACHNE
DSK-1 <ПАПКА>		Клиент
DSK-2 <ПАПКА>		Клиент
DSK3-1.EXE	864 723	Клиент
DSK3-2.EXE	288 142	Клиент

Таблица 12.3. Содержимое папки C:\DOS7

Название файла или папки	Размер файла, байт	Описание
COMMAND.COM	95 192	Командный процессор
COUNTRY.SYS	30 742	Файл MS-DOS
DEBUG.EXE	20 874	Файл MS-DOS
DISPLAY.SYS	17 239	Файл MS-DOS
EDIT. COM	70 318	Текстовый редактор
EGA3.CPI	58 753	Файл MS-DOS
EMM386.EXE	125 975	Файл MS-DOS
FDISK.EXE	64 588	Файл MS-DOS
FORMAT.COM	50 071	Файл MS-DOS
HIMEM. SYS	33 191	Файл MS-DOS
IFSHLP.SYS	3708	Файл MS-DOS
KEYB.COM	20 135	Файл MS-DOS
KEYBRD3.SYS	31 633	Файл MS-DOS
MEM. EXE	32 338	Файл MS-DOS
MODE.COM	29 911	Файл MS-DOS
MOUSE.COM	34 747	Драйвер мыши
RKM.COM	41 000	Русификатор
SCANDISK.BAT	152	Файл MS-DOS
SCANDISK.EXE	150 977	Файл MS-DOS
XCOPY.EXE	3910	Файл MS-DOS
MSDOS.SYS	108	Файл MS-DOS
TEMP <ПАПКА>		Папка для временных файлов
CHOICE.COM	1610	Файл MS-DOS
DISPLAY.CPI	88 045	Файл MS-DOS
UTIL <ПАПКА>		Папка с утилитами

Вы можете самостоятельно корректировать состав необходимых вам файлов.

Теперь, если система загружается, можно начать установку сетевого программного обеспечения. Для начала скопируйте файлы dsk3-1.exe, dsk3-2.exe, nnet.exe и netshar.exe, пользуясь следующими ссылками:

- **ftp://ftp.microsoft.com/Softlib/MSLFILES/netshar.exe**
- **ftp://ftp.microsoft.com/softlib/mslfiles/nnet.exe**
- **ftp://ftp.microsoft.com/bussys/Clients/MSCLIENT/dsk3-1.exe**
- **ftp://ftp.microsoft.com/bussys/Clients/MSCLIENT/dsk3-2.exe**

dsk3-1.exe, dsk3-2.exe — это дистрибутив MS Client для DOS, nnet.exe и netshar.exe — обновления для клиента. Создайте на диске C: директорию \DISTRIB и поместите туда полученные файлы. Эти файлы позволят включить рабочие станции под управлением DOS в сеть.

Установка Microsoft Network Client v3.0 for MS-DOS

Перед началом установки проделайте следующее:

1. Создайте каталоги \DISTRIB\DISK1 и \DISTRIB \DISK2.
2. Скопируйте в них dsk3-1.exe и dsk3-2.exe.
3. Распакуйте файлы, запустив их на выполнение.
4. Перейдите в директорию DISTRIB\DISK1 и запустите setup.exe.
5. На экране появится окно программы установки клиента. Нажмите клавишу <Enter>.
6. В окне выбора каталога установки, ничего не меняя, нажмите <Enter>. Клиент будет установлен в каталог C:\NET.
7. На экране появится окно проверки системы. Дождитесь окончания проверки. Если компьютер долго не подает признаков жизни, перезагрузите его.
8. В окне выбора сетевого адаптера выберите тип вашей сетевой карты, перемещаясь по строкам клавишами со стрелками. Если ваш адаптер в списке отсутствует, выберите пункт ***Network adapter not shown on list below** (Сетевой адаптер отсутствует в списке). При этом надо указать путь к драйверу вашей сетевой карты, введя его с клавиатуры. Можно использовать драйвер с дискеты, прилагаемой к устройству, или найти его в Интернете.
9. Следующим появится окно **Set Network Buffers** (Оптимизация памяти). Если вы используете описанные ранее системные файлы, то нажмите <Enter>.

10. В появившемся окне введите имя пользователя. Вы можете выбрать любое имя длиной не более 20 символов. В нашем примере используется имя компьютера **Serdos** и имя пользователя **Admin**. Имя компьютера можно будет ввести на следующем этапе при корректировке настроек.
11. Далее потребуется скорректировать сетевую конфигурацию компьютера. Клавишами со стрелками выберите **Change Network Configuration** и нажмите <Enter>.
12. На следующем экране (рис. 12.1) можно перемещаться между окнами клавишей <Tab>, а внутри каждого окна — клавишами со стрелками. Установив курсор на пункт в верхнем окне, перейдите с помощью клавиши <Tab> в нижнее окно для выбора необходимого действия.

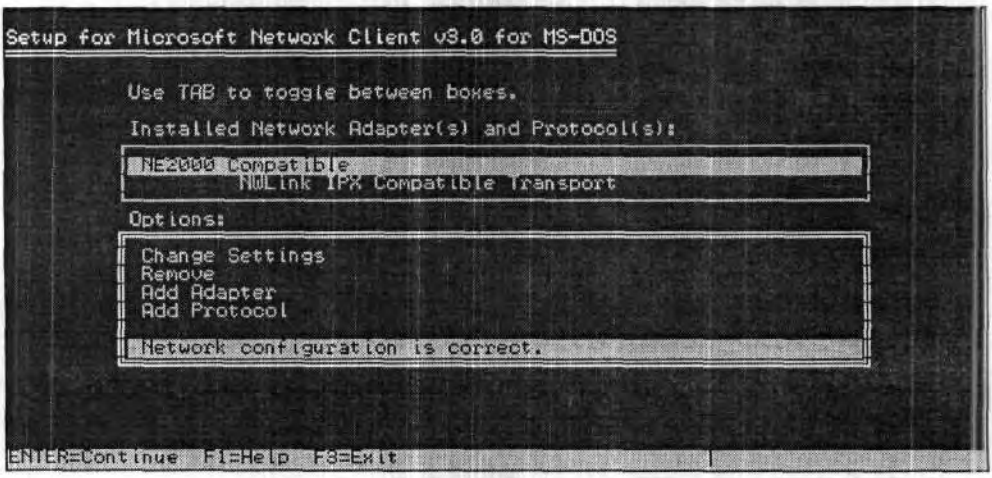


Рис. 12.1. Один из экранов
Setup for Microsoft Network Client v3.0 for MS-DOS

13. Если сетевой адаптер установлен верно, то, скорее всего, его настройки менять не надо, но необходимо установить сетевые протоколы, которые используются в нашей сети. Для этого следует установить курсор на имя сетевого протокола, перейти в нижнее окно с помощью клавиши <Tab> и выбрать **Add Protocol**. Нам потребуется добавить Microsoft TCP/IP и Microsoft NetBEUI. Протокол, который предлагался по умолчанию, следует удалить (**Remove**).
14. Теперь необходимо настроить протокол Microsoft TCP/IP. Установив курсор на имя протокола, в нижнем меню выберите **Change Settings** (Изменить настройки). Если в вашей сети есть DHCP-сервер, то можно ничего не трогать и пропустить настройку TCP/IP, но лучше установить IP-адрес из зоны зарезервированных адресов, т. е. адресов, которые не

изменяются DHCP-сервером. Это позволит работать в любой сети, минимально изменив настройки. На сервере WINS при этом желательно создать статическое сопоставление адреса и имени. Как изменить настройки сервера будет показано после описания установки клиента. В нашем примере используется адрес 192.168.0.126. Маска подсети 255.255.255.0. Вместо точек вводятся пробелы.

Будьте внимательны!

Если адрес ввести с точками вместо пробелов, то во время загрузки сети будет выведено на экран множество сообщений об ошибках и невозможности загрузить тот или иной драйвер.

15. Если все введено правильно, выберите **The listed options are correct** (Список настроек верен).

Аналогично можно изменить и настройки сети: имя компьютера, имя пользователя, имя рабочей группы и имя домена. Два последних имени в нашем случае должны совпадать. Проверить правильность настроек и подправить их можно позже, изменяя настройки напрямую в файлах конфигурации, которые будут созданы в процессе установки. После нажатия **The listed options are correct** начнется процесс копирования файлов, по завершении которого компьютер выдаст запрос на перезагрузку. Если в дисководе была дискета, выньте ее и нажмите клавишу <Enter>.

Подключите компьютер к сети. Если все настройки выполнены верно, то после перезагрузки компьютера появится надпись: **Type your user name, or press ENTER if it is USER** (Напечатайте ваше имя или нажмите ENTER, если оно, в данном случае, Admin). Если это ваше имя, то нажмите клавишу <Enter>. Или наберите другое имя и тоже нажмите <Enter>.

Появится строка: **Type your password** (Напечатайте ваш пароль). Введите пароль. Вместо букв будут выводиться звездочки, затем нажмите <Enter>.

На экран будут выводиться следующие сообщения, выделенные в тексте жирным шрифтом.

There is no password-list file for USER. Do you want to create one? (Y/N) [N] (Отсутствует запись паролей для Admin. Хотите создать?)

Нажмите <Y>, потом — <Enter>.

Please confirm your password so that a password list may be created (Пожалуйста, подтвердите пароль для создания записи паролей).

Еще раз введите пароль.

The command completed successful (Команда выполнена полностью).

Теперь ваш компьютер в сети. Но если все произошло иначе, и нет входа в сеть, не отчаивайтесь. Сначала продолжим установку клиента (она еще не

завершена), а затем проверим все настройки по содержимому файлов конфигурации.

Установите обновления для клиента. Для этого перезагрузите компьютер. При загрузке выберите пункт меню **No Net** (Без сети). Это позволит освободить память для процесса установки. Файлы nnet.exe и netshar.exe скопируйте в каталог C:\NET и распакуйте их, запустив на выполнение. Теперь замените файл Autoexec.bat на заранее подготовленный. Проверьте содержание файлов конфигурации клиента. Это два файла в каталоге C:\NET — Protocol.ini и System.ini. Содержание файлов с комментариями приведено в листингах 12.5 и 12.6, но оно может несколько отличаться в зависимости от применяемого сетевого адаптера. Тем не менее, основные настройки, которые не связаны с типом сетевого адаптера, должны быть такими же.

Листинг 12.5. Файл Protocol.ini

```
[network.setup]
version=0x3110
netcard=hwp$27247b,1,HWP$27247B,1
transport=tcpip,TCPIP
transport=ms$ndishlp,MS$NDISHLP
transport=ms$netbeui,MS$NETBEUI
lana0=hwp$27247b,1,tcpip
lana1=hwp$27247b,1,ms$netbeui
lana2=hwp$27247b,1,ms$ndishlp
;В этом разделе сведения о драйвере сетевого адаптера и установленных
;протоколах.

[TCPIP]
NBSessions=6
;Замените в следующих строках адреса сервера и компьютера на свои
WINS_SERVER0=192 168 0 15       ;адрес сервера
DefaultGateway0=192 168 0 15    ;адрес сервера
SubNetMask0=255 255 255 0       ;маска подсети
IPAddress0=192 168 0 126        ;адрес компьютера
DisableDHCP=0
DriverName=TCPIP$
BINDINGS=HWP$27247B
LANABASE=0
```

```
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP


[HWP$27247B]
DriverName=HPLANP$

[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=HWP$27247B


[MS$NETBEUI]
DriverName=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=HWP$27247B
LANABASE=1
```

Листинг 12.6. Файл Sistem.ini

```
[network]
filesharing=yes
printsharing=yes
;два предыдущих значения становятся равными "NO" при запуске настройки
;параметров командой Setup, поэтому после изменения свойств сетевого
;адаптера или его смене восстановите "YES", иначе не будет доступа к
;компьютеру из сети.
autologon=no
;autologon=yes
computername=SERDOS ;Замените на имя вашего компьютера
lanroot=C:\NET
username=ADMIN ;Замените на ваше сетевое имя
workgroup=AP15 ;Замените на имя вашей рабочей группы (имя домена)
reconnect=yes
dospophotkey=N
lmlogon=1
logondomain=AP15 ;Замените на имя вашей рабочей группы (имя домена)
```

```
preferredredir=full
autostart=full,popup
maxconnections=8

[network drivers]
netcard=hplanp.dos
transport=tcpdrv.dos,nemm.dos,ndishlp.sys,*netbeui
devdir=C:\NET
LoadRMDrivers=yes

[386enh]
TimerCriticalSection=5000
UniqueDosPSP=TRUE
PSPIncrement=2

[Password Lists]
*Shares=C:\NET\Share000.PWL
ADMIN=C:\NET\ADMIN.PWL ;Изменяется при регистрации пароля на локальном
                       ;компьютере
NET=C:\NET\NET.PWL
```

После корректировки файлов сохраните их резервные копии. При изменении этих файлов самой системой, например, после запуска Setup.exe для корректировки настроек проверяйте содержание файлов конфигурации с помощью текстового редактора.

Если все настройки верны, то при загрузке сети (пункт загрузочного меню **Use Net**) система предложит указать сетевой диск для подключения, далее для выбора компьютера и доступных ресурсов запустится специальный браузер. После выбора сетевых ресурсов система предложит предоставить сети свои ресурсы. Осталось настроить сервер для работы с нашей рабочей станцией.

"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. Особенно вероятны такие ситуации, когда приходится иметь дело с устаревшей, но еще применяемой 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 не сложна, 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, хотя бы иногда работающим в среде MS-DOS. Далее приведено содержание данного и других файлов из diskwww.zip. Для тех, кто будет пользоваться прочими дистрибутивами, эти описания также подойдут — отличия не принципиальны.

Autoexec.nos

Сразу отмечу, что символы # или `rem` предваряют все комментарии и неисполняемые команды.

Листинг 12.7 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 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 12.8 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) представлены настройки доступа к FTP-серверу. Именно с его помощью удобно загружать необходимые файлы на компьютер из сети.

Листинг 12.9. 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;
- 127 — системного администратора;
- 128 — запрещение доступа.

Формат записи:

```
<Пользователь><Пароль>[Буква диска:] \<Путь1> <Доступ>;
\<Путь2><Доступ>
```

Звездочка обозначает пустой пароль. Буква для диска A: может быть опущена. С указанными настройками сервер работает в сети с сервером Windows 2000 Server 192.168.0.15 с маской подсети 255.255.255.0. Причем независимо от операционной системы 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

- `?` — 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 не велико, 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 WWW/FTP-серверов (на FTP-сервере могут храниться полезные файлы, а на страницах WWW-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).

Настройки DHSP и WINS на сервере Windows 2000 Server

Протокол TCP/IP, который используется рабочей станцией DOS, несколько отличается от того, который применяется сервером Windows 2000. В связи с этим настройка сервера для общения с Microsoft Network Client v3.0 for MS-DOS имеет некоторые особенности. IP-адрес, который мы назначили рабочей станции, может быть изменен сервером при первом удачном входе в сеть. Для того чтобы в дальнейшем быть уверенным, что связь с компьютером будет надежной, как со стороны сервера, так и со стороны других рабочих станций, необходимо проделать следующее:

1. Войдите на сервер в качестве администратора домена и создайте, если еще не создан, пользователя с именем Admin или другим именем, которое вы применили для пользователя рабочей станции DOS.

2. Нажмите кнопку **Пуск**.
3. Выберите **Программы | Администрирование | DHCP**. Откроется окно **DHCP** (рис. 12.2).

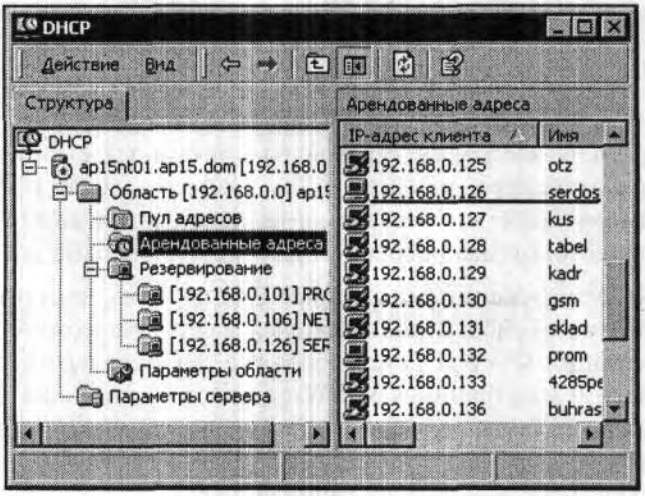


Рис. 12.2. Окно **DHCP**

4. Раскройте папку **Область**, соответствующую адресам вашей сети, выделите папку **Арендованные адреса** и в списке справа найдите адрес рабочей станции DOS (в нашем случае 192.168.0.126), ориентируясь по имени компьютера (**serdos**). Если адрес отличается от того, что был установлен в параметрах рабочей станции, отредактируйте файлы конфигурации рабочей станции DOS в соответствии с новым значением адреса и перезагрузите ее.
5. Выделите папку **Резервирование**, щелкните правой кнопкой мыши и выберите пункт **Создать резервирование**.
6. В открывшемся окне введите имя рабочей станции, ее IP-адрес и при необходимости комментарий.
7. Нажмите кнопку **Добавить**.
8. Закройте окно **DHCP**.
9. Нажмите кнопку **Пуск**.
10. Выберите **Программы | Администрирование | WINS**. Откроется окно **WINS** (рис. 12.3).
11. Выделите папку **Активные регистрации**.
12. Щелкните правой кнопкой мыши и выберите **Статическое сопоставление**.

13. В открывшемся окне введите имя рабочей станции, MAC-адрес сетевого адаптера и его IP-адрес. Для того чтобы узнать MAC-адрес адаптера на рабочей станции DOS, достаточно внимательно посмотреть на строки, появляющиеся на экране в процессе загрузки с установленным Microsoft Network Client v3.0 for MS-DOS.
14. Нажмите **OK**.

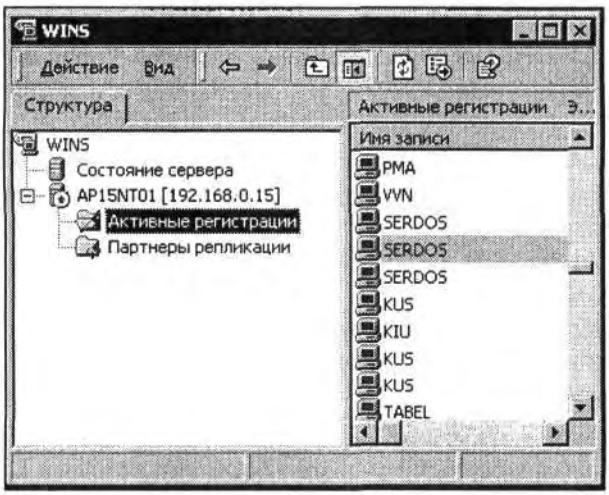


Рис. 12.3. Окно **WINS**

Теперь IP-адрес рабочей станции DOS не будет изменяться по воле сервера и при установке программного обеспечения, которое требует указания адреса компьютера, вы будете уверены, что вводите действительный адрес. Компьютеры сети, не использующие сервис, предоставляемый сервером, также смогут подключаться к рабочей станции DOS и предоставлять ей свои ресурсы.

Применение настроек рабочей станции DOS при обслуживании компьютеров сети

Если вам удалось настроить рабочую станцию DOS для работы в вашей сети, то у вас в руках оказался очень полезный инструмент, который можно применять для настройки и установки программного обеспечения на новых компьютерах сети.

Для этого понадобится приобрести небольшую деталь — Flash Drive. Эти миниатюрные устройства теперь достаточно широко распространены. Замечательная особенность Flash Drive состоит в том, что он может быть загру-

зочным. Практически все современные компьютеры имеют в BIOS-SETUP режим загрузки компьютера с устройства USB-ZIP. Создав загрузочный Flash Drive и установив на него Microsoft Network Client v3.0 for MS-DOS, вы получите возможность загружать новый компьютер (без установленной операционной системы), устанавливать по сети или копировать инсталляционные файлы программ. В случае необходимости полного форматирования диска вы можете не носить с собой дистрибутивы, а записать их на доступный по сети диск и подключаться к ним даже с "пустой" машины. Если учесть, что в организациях иногда экономят на приводах CD-ROM, а современные компьютеры все чаще предлагаются без floppy-дисковода, то загрузка с Flash Drive может оказаться единственным вариантом загрузки компьютера, не требующим его вскрытия.

Установка Microsoft Network Client v3.0 for MS-DOS на Flash Drive не сложнее, чем на обычный диск. Следует лишь учесть, что диск будет обозначаться буквой "A". Соответственно все пути должны соответствовать букве диска. Современные сетевые платы обычно имеют в составе дистрибутивной дискеты необходимые драйверы. У распространенного сетевого адаптера ReadyLINK Express RE 100ATX/WOL есть подходящий драйвер, расположенный в папке Ndis2. Некоторые сетевые адаптеры снабжены специальными драйверами для Microsoft Network Client v3.0 for MS-DOS.

Универсальность описываемого инструмента может пострадать, если с каждым новым компьютером вы получаете новый тип сетевого адаптера. В этом случае можно всегда иметь при себе адаптер для временной замены штатного или приобретать компьютеры с одинаковыми сетевыми платами.

Перед установкой Microsoft Network Client v3.0 for MS-DOS на Flash Drive все дистрибутивы можно записать туда же. Когда программа установки будет запрашивать загрузочную дискету или дискету с дистрибутивом, потребуется только нажимать клавишу <Enter>. Для указания местонахождения драйвера сетевой платы придется вводить путь вручную. При этом средства, подобные файловому менеджеру, отсутствуют.

Загрузочный диск, полученный средствами Windows и с помощью инструментов, прилагаемых к Flash Drive, может быть легко дополнен необходимыми компонентами для загрузки сети. При этом вы не ограничены размером дискеты. Полный текст файлов Autoexec.bat и Config.sys, откорректированный для нашего случая, приведен в листингах 12.10 и 12.11.

Листинг 12.10. Файл Autoexec.bat для Flash Drive

```
@ECHO OFF
IF "%config%"=="SUPERDISK" GOTO SUPER ;добавлено
if "%config%"=="SUPERDISK1" GOTO SUPER ;добавлено
```

```
set EXPAND=YES
SET DIRCMD=/O:N
set LglDrv=27 * 26 Z 25 Y 24 X 23 W 22 V 21 U 20 T 19 S 18 R 17 Q 16 P 15
set LglDrv=%LglDrv% O 14 N 13 M 12 L 11 K 10 J 9 I 8 H 7 G 6 F 5 E 4 D 3
C
cls
call setramd.bat %LglDrv%
set temp=c:\
set tmp=c:\
path=%RAMD%:\;a:\;%CDROM%:\
copy command.com %RAMD%:\ > NUL
set comspec=%RAMD%:\command.com
copy extract.exe %RAMD%:\ > NUL
copy readme.txt %RAMD%:\ > NUL

:ERROR
IF EXIST ebd.cab GOTO EXT
echo Вставьте загрузочный диск 2 для Windows 98
echo.
pause
GOTO ERROR

:EXT
%RAMD%:\extract /y /e /l %RAMD%: ebd.cab > NUL
echo Средства диагностики находятся на диске %RAMD%.
echo.

IF "%config%"=="NOCD" GOTO QUIT
IF "%config%"=="HELP" GOTO HELP
LH %ramd%:\MSCDEX.EXE /D:mscd001 /L:%CDROM%
echo.
GOTO QUIT

:HELP
cls
call help.bat
echo После перезагрузки будет выведено загрузочное меню.
echo.
echo.
```

```
echo.
echo.
echo.
echo.
echo.
echo.
echo.
echo.
restart.com
GOTO QUIT

:QUIT
echo Для получения справки наберите HELP и нажмите клавишу ввода.
echo.
rem clean up environment variables
set CDROM=
set LglDrv=

goto ex  ;далее добавлены строки


:SUPER
echo mem +
set temp=c:\TEMP
set tmp=c:\TEMP
path=a:\;a:\NET

choice /c:SNLA /t:L,20 "Share-S сеть-N локально-L"
if errorlevel 3 goto l
if errorlevel 2 goto n
a:\NET\net initialize
a:\NET\netbind.com
a:\NET\umb.com
a:\NET\tcptsr.exe
a:\NET\tinyrfc.exe
a:\NET\nmtsr.exe
a:\NET\emsbfr.exe
a:\NET\net start
```

```
a:\NET\net start server
a:\NET\net share
cls
@echo "Сеть с доступом загружена Ctrl+Alt+N подкл.диск"
@echo "netshare - обеспечить доступ"
net
a:\net\netshare.exe
goto l

:n
a:\NET\net initialize
a:\NET\netbind.com
a:\NET\umb.com
a:\NET\tcptsr.exe
a:\NET\tinyrfc.exe
a:\NET\nmtsr.exe
a:\NET\emsbfr.exe
a:\NET\net start
cls
@echo "Сеть загружена"
net
goto l
:l
@echo "ПРИЯТНОЙ РАБОТЫ!"
:ex
```

Листинг 12.11. Файл Config.sys для Flash Drive

```
[menu]
menuitem=CD, Start computer with CD-ROM support.
menuitem=NOCD, Start computer without CD-ROM support.
menuitem=HELP, View the Help file.
menuitem=SUPERDISK, NET?. ;Можно выбирать загрузку с доступом к сети
menuitem=SUPERDISK1, Mouse and RKM.
menudefault=CD,30
menucolor=14,1
```

```
[CD]
dos=high,umb
device=himem.sys /testmem:off
device=oakcdrom.sys /D:mscd001
device=btdosm.sys
device=flashpt.sys
device=btcdrom.sys /D:mscd001
device=aspi2dos.sys
device=aspi8dos.sys
device=aspi4dos.sys
device=aspi8u2.sys
device=aspicd.sys /D:mscd001
devicehigh=ramdrive.sys /E 2048
lastdrive=z
device=display.sys con=(ega,,1)
country=007,866,country.sys
install=mode.com con cp prepare=((866) ega3.cpi)
install=mode.com con cp select=866
install=keyb.com ru,,keybrd3.sys

[NOCD]
dos=high,umb
device=himem.sys /testmem:off
devicehigh=ramdrive.sys /E 2048
lastdrive=z
device=display.sys con=(ega,,1)
country=007,866,country.sys
install=mode.com con cp prepare=((866) ega3.cpi)
install=mode.com con cp select=866
install=keyb.com ru,,keybrd3.sys

[HELP]
dos=high,umb
device=himem.sys /testmem:off

[SUPERDISK]
dos=high,umb,noauto
```

```
device=himem.sys /testmem:off
device=emm386.exe noems
devicehigh=A:\display.sys con=(ega,,1)
country=007,866,country.sys
install=mode.com con cp prepare=((866) ega3.cpi)
install=mode.com con cp select=866
installhigh=keyb.com ru,,keybrd3.sys
devicehigh a:\net\ifshlp.sys


[SUPERDISK1]
dos=high,umb
device=himem.sys/testmem:off
devicehigh=emm386.exe noems
installhigh=rkm.com
installhigh=mouse.com

[COMMON]
dos=high,umb
fileshigh=80
buffershigh=20
stackshigh=9,256
lastdrivehigh=z
FCBSHIGH=1
shell=a:\command.com /E:512 /P
```

Просмотрите внимательно тексты файлов. Возможно, вы что-либо измените в них, добавите запуск утилит или программ. Но следует иметь в виду, что Flash Drive — не слишком быстрый диск. Если программа требует высокой скорости операций (например, видео), то файлы необходимо копировать на жесткий или виртуальный диск. Однако для целей, которые были обозначены ранее, быстродействия Flash Drive вполне достаточно. Flash Drive, построенный на основе файлов обычной загрузочной дискеты с добавлением Microsoft Network Client v3.0 for MS-DOS и его обновлений, сохраняет возможности загрузочной дискеты, но имеет режим загрузки сети. Как и в случае с рабочей станцией DOS, при установке Microsoft Network Client v3.0 for MS-DOS откажитесь от автоматического изменения этих файлов и исполь-

зуйте заранее подготовленные образцы. При необходимости позже вы их сможете откорректировать в соответствии с вашими потребностями.

Замечание

Применяя загрузочный Flash Drive с доступом к сети, не забывайте изменять имя компьютера в файле \NET\System.ini, а если в сети используется DHCP-сервер, то не указывайте IP-адрес компьютера: DHCP-сервер выдаст адрес самостоятельно. В одноранговой сети и сети без DHCP указывать адрес обязательно, но необходимо следить за его уникальностью в пределах сети.

Настройка рабочих станций с операционной системой Windows 9*x*

Если операционная система установлена корректно, то настройка рабочих станций под управлением Windows 9*x* проще, чем для рабочих станций DOS. Тем не менее, при настройке требуются аккуратность и внимание. Если вам придется переводить всю сеть на работу под Windows, то устранение допущенных ошибок при массовой настройке рабочих станций отнимет у вас очень много времени.

Чтобы компьютер с операционной системой Windows 9*x* смог работать в сети с сервером Windows 2000 Server, этот компьютер необходимо подключить к сети и проделать следующее.

1. Нажмите кнопку **Пуск**.
2. В открывшемся меню выберите **Настройка | Панель управления**.
3. В открывшемся окне найдите значок **Сеть** и двойным щелчком по нему откройте одноименное окно (рис. 12.4).
4. Если еще не добавлены компоненты **Клиент для сетей Microsoft**, **TCP/IP**, **Тип сетевого адаптера**, **Служба доступа к файлам и принтерам сетей Microsoft**, то добавьте их.

   Для добавления компонентов нажмите кнопку **Добавить**, откроется окно **Выбор типа компонента**. В этом окне выберите тип компонента, например, **Клиент**, **Протокол** или **Служба** в соответствии с типом устанавливаемого компонента. После выбора типа компонента станет доступной кнопка **Добавить**. Нажав ее, вы сможете выбрать необходимый компонент.

   Вполне возможно, что вы использовали уже ваш компьютер для подключения к Интернету. В этом случае у вас будет установлено два протокола TCP/IP, но с различной привязкой. Один будет работать с сетевым адап-

тером, а другой с контроллером удаленного доступа, который уже установлен. Это необходимо учесть, когда будем настраивать работу сети. Протокол, работающий с контроллером удаленного доступа, настраивать не следует, чтобы не испортить свойства подключения к Интернету.

Выбирать следует компоненты, разработанные корпорацией Microsoft.

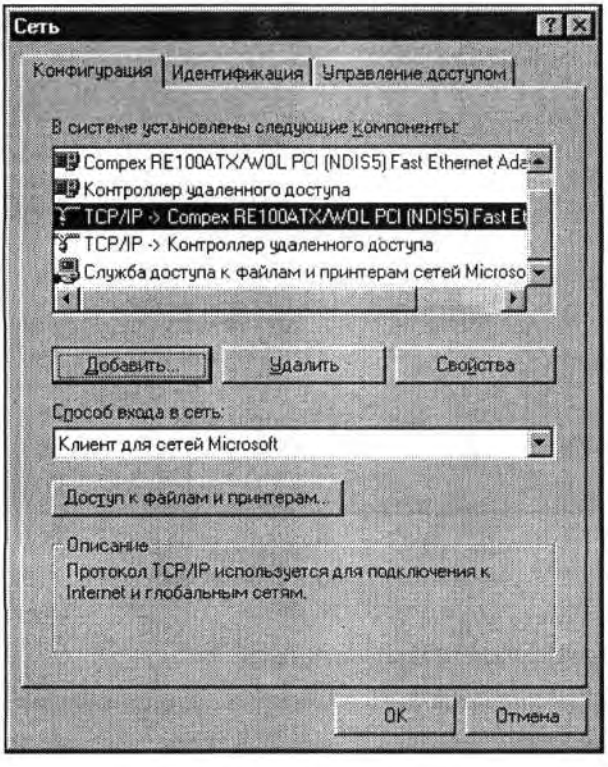


Рис. 12.4. Окно **Сеть**

5. В окне **Сеть** на вкладке **Конфигурация** (рис. 12.4) выделите протокол TCP/IP.
6. Нажмите кнопку **Свойства**.
7. В открывшемся окне **Свойства: TCP/IP** на вкладке **IP-Адрес** установите переключатель в положение **Получить IP-адрес автоматически**, если было установлено иное.
8. Если используется сервер DNS, откройте вкладку **Конфигурация DNS** (рис. 12.5). Если DNS не используется, переходите к пункту 12.

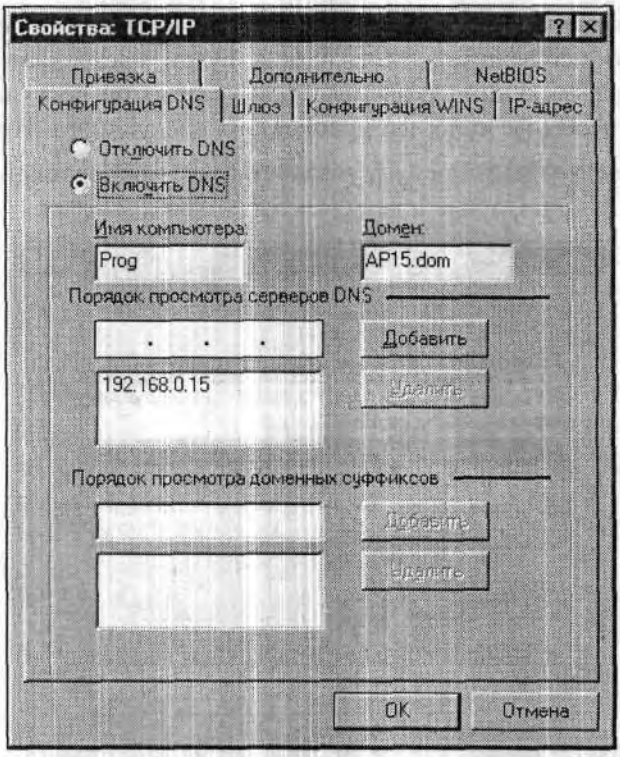


Рис. 12.5. Окно **Свойства: TCP/IP**, вкладка **Конфигурация DNS**

9. Отметьте переключатель **Включить DNS**.
10. Введите имя компьютера и имя домена в соответствующие поля ввода.
11. В разделе **Порядок просмотра серверов DNS** введите IP-адрес вашего сервера и нажмите кнопку **Добавить**.
12. Если применяется WINS-сервер без сервера DNS, то откройте вкладку **Конфигурация WINS**.
13. Установите переключатель в положение **Включить распознавание WINS** (рис. 12.6).
14. Введите IP-адрес вашего сервера и нажмите кнопку **Добавить** (при наличии сервера DHCP отмечается только переключатель **Использовать DHCP для распознавания WINS**).
15. Нажмите кнопку **OK**.
16. Откройте вкладку **Идентификация** окна **Сеть**.

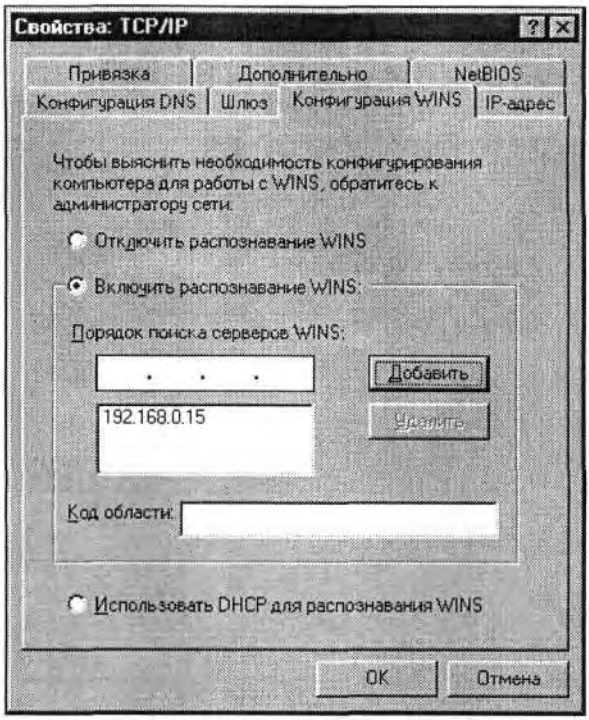


Рис. 12.6. Окно **Свойства: TCP/IP**, вкладка **Конфигурация WINS**

17. Введите имя компьютера, имя рабочей группы и описание компьютера. Имя рабочей группы должно совпадать с именем домена без суффикса (рис. 12.7).
18. На вкладке **Конфигурация** установите **Способ входа в сеть** как **Клиент для сетей Microsoft**.
19. При необходимости нажмите кнопку **Доступ к файлам и принтерам** и в открывшемся окне отметьте флажки, разрешающие доступ к компьютеру, нажмите кнопку **OK**.
20. Выделите **Клиент для сетей Microsoft**.
21. Нажмите кнопку **Свойства**.
22. В открывшемся окне **Свойства: Клиент для сетей Microsoft** (рис. 12.8) установите флажок **Входить в домен Windows NT** и внесите имя домена (опять без суффикса).
23. В разделе **Параметры входа в сеть** выберите подходящий вам вариант.

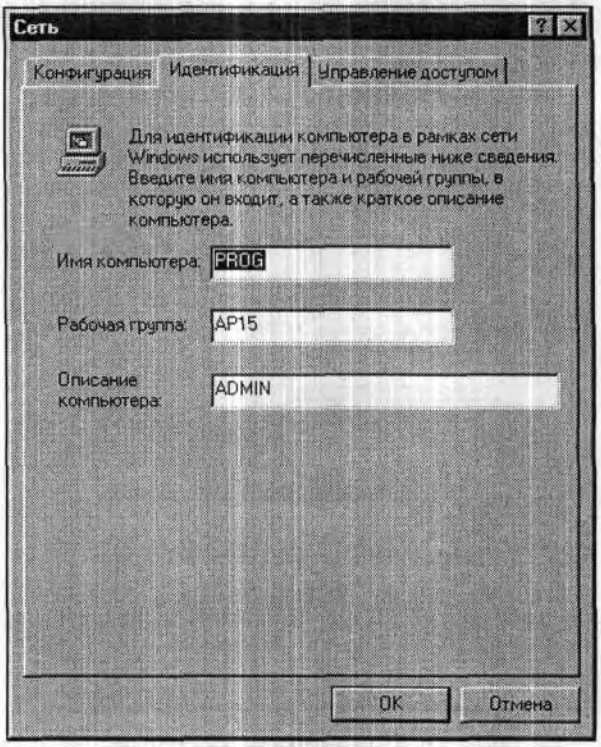


Рис. 12.7. Окно **Сеть**, вкладка **Идентификация**

24. Нажмите кнопку **OK**.
25. На вкладке **Управление доступом** установите желаемый вариант доступа к компьютеру. Доступ на уровне ресурсов даст возможность подключаться к компьютеру с рабочих станций, не зарегистрированных на сервере (не входящих в домен), доступ на уровне пользователей позволяет подключаться к компьютеру только зарегистрированным в сети пользователям. Для второго варианта необходимо заполнить поле **Взять список пользователей с сервера**, но указать нужно имя домена без суффикса.
26. Нажмите кнопку **OK** и перезагрузите компьютер.
27. После перезагрузки, если не удастся войти в сеть, проверьте еще раз все настройки и исправьте ошибки.
28. На этом настройка рабочей станции под управлением Windows 9*x* завершена.

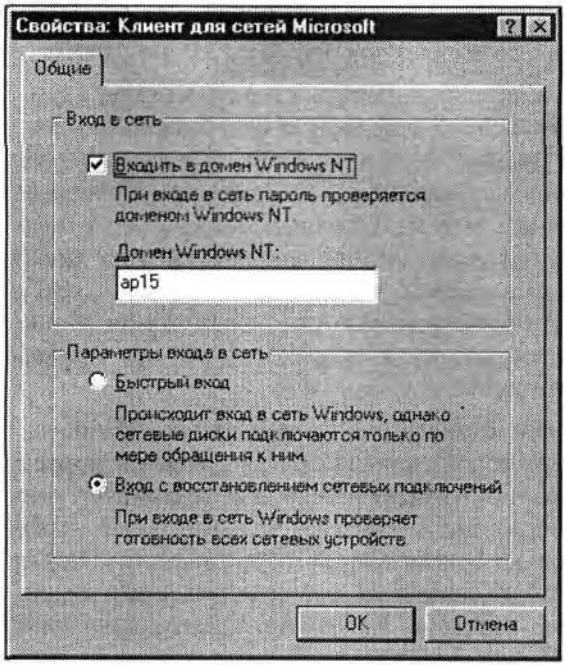


Рис. 12.8. Окно **Свойства: Клиент для сетей Microsoft**

Ограничения для старых ОС в новых сетях

Нам удалось настроить старые рабочие станции для работы в сети. Но ввиду того, что со времени окончания поддержки DOS и ранних версий Windows претерпели некоторое изменение протоколы TCP/IP, эти рабочие станции не смогут работать в новой сети настолько комфортно, как новые, с ОС Windows XP, например. Поэтому применение этих рабочих станций определено некоторыми ограничениями. Скорее всего, в доменной сети не удастся получить доступ к ресурсам DOS рабочей станции через обозреватель сети. HTTP и FTP-серверы, тем не менее, будут доступны для всех рабочих станций. Вполне вероятно, что и доступ с DOS-рабочих станций к ресурсам сервера будет невозможен, но если применяется какой-либо интернет-браузер, работающий в среде DOS, то доступ к Web-серверу на сервере сети возможен.

Для рабочих станций с Windows 98 тоже есть некоторые ограничения. Но они не так заметны на первый взгляд, как ограничения для DOS. Часть ограничений снимается, если установить дополнительно клиент для работы

в AD *(см. главу 11)*. Но предоставить рабочей станции права администратора домена, что вполне возможно для Windows XP, не удастся.

Все же, применить старые рабочие станции в новой сети с пользой вполне возможно, если подходить к решению возникающих задач творчески. А задачи могут быть самыми неожиданными. Например, в одной из организаций долго применялась местная АТС, которая управлялась из среды DOS через окно терминала, и в этой же среде можно было получать отчеты о работе станции и телефонов. Отчеты записывались на дискету (другого варианта их сохранения в данной АТС не предусмотрено), но с дискеты по сети передавались на рабочую станцию под управлением Windows 98, где проходили дальнейшую обработку и были доступны при необходимости для других рабочих станций сети.

Для старой рабочей станции под управлением Windows 98 можно найти применение и в качестве принт-сервера. Многие современные принтеры имеют встроенный принт-сервер, что делает принтер доступным для всей сети без подключения его к компьютеру, но старые и недорогие принтеры могут работать только с компьютером или внешним принт-сервером. В нашей сети, например, исправно работает на протяжении нескольких лет струйный цветной принтер. Его возможности, как принтера, устраивают всех пользователей, он был подключен когда-то к рабочей станции одного из пользователей и был доступен всем. Но объем печати постоянно увеличивался, и пользователь попросил освободить его от обязанности невольного оператора печати. К тому времени освободилась рабочая станция, которую трудно было применить для нормальной работы, ввиду морального устаревания. Ее и использовали в качестве принт-сервера. Вот уже около двух лет она работает самостоятельно, почти не перезагружаясь круглосуточно. (Куда делась нестабильность Windows 98?) Настройку такого принт-сервера описывать нет смысла, поскольку это обычные настройки для принтера общего доступа, подключенного к рабочей станции.

Обслуживание рабочих станций

Вместе с расширением и ростом сети у ее администратора появляется все больше забот, которых раньше просто не замечали. Если сеть обслуживает работу организации, где необходим учет вычислительной техники, постоянно растущий парк компьютеров требует все больше и больше усилий, чтобы отследить перемещения рабочих станций, их модернизацию, проведенные ремонты и общее состояние. Иногда изменения в сети происходят неожиданно. Причины таких изменений могут быть различными, но упорядочить документы, отражающие сведения об имеющемся сетевом оборудовании и компьютерах, бывает не просто. Значительную помощь в этом вопросе мо-

гут оказать программы, которые автоматически собирают сведения о компьютерах и конфигурации сети. Одна из таких программ разработана IT-службой одного из банков.

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. Эти сведения можно дополнять информацией о проведенных работах и модернизациях, использовать при планировании обслуживания.

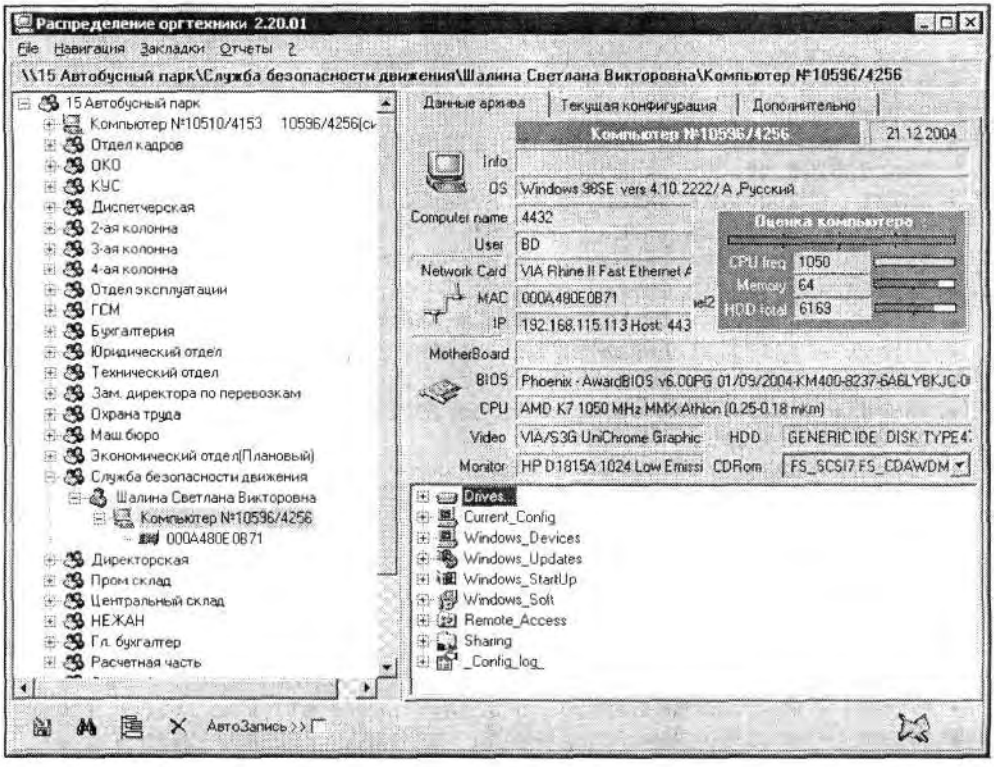


Рис. 12.9. Главное окно программы учета вычислительной техники

Программа позволяет получать отчеты, форму которых можно корректировать самостоятельно, учитывать сведения о ремонтах и модернизациях. Далее приведен почти без сокращений отчет "Сводные данные по предприятию". Подробность сведений в отчете позволяет оценить полезность программы для администратора сети.

Сводные данные по предприятию

На 21.11.2005 учтено компьютеров - 53

Список материнских плат :

- AMIBIOS 070010 04/02/01 K7VMM+ Release 01/27/200 62-0127-009999-00101111-040201-VIA_K7 K7VMM 01/27/03 - 1 шт.
- ASUS - 42302E31 ASUS P4PE-X__ - 1 шт.
- ASUS P4B266__ - 1 шт.
- ECS (Elitegroup) VIA VT8366/VT8233 chipset with Award BIOS v6.00 - 2 шт.
- ELITEGROUP COMPUTER CO., LTD. K7SOM+ RELEASE 01/20/200 - 2 шт.
- ELITEGROUP COMPUTER CO., LTD. K7SOM+ RELEASE 11/19/200 - 1 шт.
- Epox & 2TheMax 6A6LY - 1 шт.
- GIGA BYTE CO., LTD. 7VMM F4 MST - 1 шт.
- Giga-byte Intel 440BX/ZX chipset (Pentium II/III based chipset) - 6 шт.
- HOLCO (Shuttle) VIA VT8365 (KM-133)/VT8364 (KL-133) chipset with Award BIOS v6.00 - 1 шт.
- INTEL - 20030226 INTEL_ D845GBV2 - 2 шт.
- INTEL - 20030624 INTEL_ D865GBF_ - 2 шт.
- INTEL - 20030924 D865GBF_ INTEL_ D865GBF_ - 1 шт.
- INTEL - 20040412 INTEL_ D865GLC_ - 2 шт.
- IntelR - 42302e31 AWRDACPI INTELR AWRDACPI - 1 шт.
- Nvidia - 42302e31 AWRDACPI NVIDIA AWRDACPI - 1 шт.
- Nvidia - 42302e31 NVIDIA AWRDACPI - 6 шт.
- Phoenix - AwardBIOS v6.00PG 01/09/2004-KM400-8237-6A6LYBKJC-00 01/09/04 - 1 шт.
- Phoenix NuBIOSB 07/30/97 - 2 шт.
- Phoenix NuBIOSB 09/19/96 - 4 шт.
- Phoenix NuBIOSB 10/14/97 - 1 шт.
- Phoenix NuBIOSB 12/17/96 - 1 шт.
- Phoenix NuBIOSB 12/21/95 - 2 шт.
- Phoenix Technologies Ltd 08/24/95 - 1 шт.
- Phoenix-Award BIOS v6.00PG 09/22/2003-nVidia-nForce-6A61BBK9C-00 09/22/03 - 1 шт.
- PTLTD - 6040000 HP nx9010 (DG231A) ATI MS2_1535 - 1 шт.
- PTLTD - 6040000 Pavilion ze8500 (DJ316A) ATI MS2_1535 - 1 шт.
- SE7500CW2 Server BIOS - Version 1.18 SE7500CW2 INTEL PLUMAS - 1 шт.
- Soltek VIA VT8365 (KM-133)/VT8364 (KL-133) chipset with Award BIOS v6.00 - 3 шт.
- VIA694 - 42302e31 MS-6378 VIA694 AWRDACPI - 1 шт.

Список процессоров :

- 2x Intel Pentium 4 2390 MHz MMX Nortwood - 2 шт.
- 2x Intel Pentium 4 2400 MHz MMX Nortwood - 1 шт.
- 2x Intel Pentium 4 2790 MHz MMX Nortwood - 1 шт.

- 2x Intel Pentium 4 2790 MHz MMX Prescott - 2 шт.
- 4x Intel Pentium Xeon 1990 MHz MMX Nortwood - 1 шт.
- AMD K7 1050 MHz MMX Athlon (0.25-0.18 mkm) - 1 шт.
- AMD K7 1290 MHz MMX Athlon (0.25-0.18 mkm) - 1 шт.
- AMD K7 1300 MHz MMX Athlon (0.25-0.18 mkm) - 1 шт.
- AMD K7 1400 MHz MMX Athlon (0.25-0.18 mkm) - 1 шт.
- AMD K7 1666 MHz MMX Athlon (0.25-0.18 mkm) - 1 шт.
- AMD K7 1820 MHz MMX Athlon (0.25-0.18 mkm) - 1 шт.
- AMD K7 1833 MHz MMX Athlon (0.25-0.18 mkm) - 7 шт.
- AMD K7 800 MHz MMX Athlon (0.25-0.18 mkm) - 2 шт.
- AMD K7 900 MHz MMX Athlon (0.25-0.18 mkm) - 7 шт.
- Intel Celeron A 333 MHz MMX Mendocino (0.25 mkm) - 4 шт.
- Intel Celeron A 433 MHz MMX Mendocino (0.25 mkm) - 1 шт.
- Intel Pentium 133 MHz P54C (0,50mkm) - 3 шт.
- Intel Pentium 166 MHz P54C (0,50mkm) - 2 шт.
- Intel Pentium 4 1600 MHz MMX Nortwood - 1 шт.
- Intel Pentium 4 1720 MHz MMX Willamette (0.18 mkm) - 1 шт.
- Intel Pentium 4 2400 MHz MMX Nortwood - 2 шт.
- Intel Pentium 4 2680 MHz MMX Nortwood - 1 шт.
- Intel Pentium 4 2800 MHz MMX Nortwood - 1 шт.
- Intel Pentium 80 MHz P54C (0,50mkm) - 2 шт.
- Intel Pentium 90 MHz P54C (0,50mkm) - 1 шт.
- Intel Pentium II 233 MHz MMX Klamath (0.35 mkm) - 1 шт.
- Intel Pentium III 650 MHz MMX Coppermine (0.18 mkm) - 1 шт.
- Intel Pentium MMX 166 MHz MMX P55C (0,28mkm) - 1 шт.
- Intel Pentium Pro 200 MHz P6 (0.35 mkm) - 1 шт.

Распределение оперативной памяти :

- 1024 Mb - 1 шт.
- 120 Mb - 3 шт.
- 16 Mb - 3 шт.
- 192 Mb - 1 шт.
- 20 Mb - 1 шт.
- 224 Mb - 11 шт.
- 24 Mb - 2 шт.
- 248 Mb - 6 шт.
- 256 Mb - 3 шт.
- 32 Mb - 4 шт.
- 40 Mb - 1 шт.
- 48 Mb - 1 шт.
- 480 Mb - 1 шт.
- 496 Mb - 6 шт.
- 508 Mb - 2 шт.
- 64 Mb - 4 шт.
- 96 Mb - 2 шт.

Список операционных систем :
- Windows 2000 build 2195(Domain Controller)/Service Pack 3,Русский - 1 шт.
- Windows 2000 build 2195/Service Pack 2,Русский - 1 шт.
- Windows 2003 build 3790(Server)/,Русский - 1 шт.
- Windows 95/ B,Русский - 1 шт.
- Windows 95/,Русский - 1 шт.
- Windows 98SE vers 4.10.2222/ A ,Русский - 28 шт.
- Windows ME vers 4.90.3000/ ,Русский - 1 шт.
- Windows XP build 2600/Service Pack 1, v.1081,Русский - 7 шт.
- Windows XP build 2600/Service Pack 1,Русский - 9 шт.
- Windows XP build 2600/Service Pack 2,Русский - 2 шт.

Список мониторов :

Список принтеров :

Компьютеров с ошибочной конфигурацией записей - 1 шт. Список :
- Иванов Иван Иванович\Vectra 5/90 №10576/4235(мон) 10620/4283 MAC addr:0800098F6D53

Приводов CD-Rom - 40 шт. Список :
- 15 Автобусный парк : Компьютер №10510/4153 10596/4256(сист)
- 15 Автобусный парк : Компьютер №10510/4153 10596/4256(сист)
- Поляк-Брагинский Александр Владимирович : Компьютер №10596/4256(мон)
- Поляк-Брагинский Александр Владимирович : Компьютер №10596/4256(мон)
- Поляк-Брагинский Александр Владимирович : Компьютер №10596/4256(мон)
- Поляк-Брагинский Александр Владимирович : Ноутбук HP №11336/6162

Список по структуре предприятия :
- Отделов - 29
- Сотрудников - 52
- Компьютеров - 53

Сетевых карт - 53

Есть возможность учета ремонтов и модернизаций, перемещений, наличия дополнительного оборудования, самовольных модификаций программного и аппаратного обеспечения. Можно формировать шаблоны отчетов, чтобы привести их формы к принятым в вашей организации. На сайте разработчика очень подробное описание и дополнительные утилиты, разработанные не только автором программы.

Найти это средство учета компьютеров можно по адресу **http://checkcfg.narod.ru/index.htm**.

Существуют, конечно, и другие бесплатные и коммерческие продукты для сбора и учета информации о компьютерной технике. Мы остановили выбор на этой программе, как самодостаточного инструмента, не требующего дополнительных средств, в отличие от других, которые удалось найти в Интернете. Но, возможно, 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, с июня 2004 года AIDA больше не доступна. Ее сменил коммерческий проект EVEREST, а бесплатная версия новой программы не согласуется с программой учета. Но если вы имеете опыт программирования на Visual Basic, то на сайте доступен исходный код программы учета. Следовательно, вы можете подогнать ее под свои требования.

Применяя подобные программы, вы сможете наладить учет техники, даже если до настоящего времени никто этим по-настоящему не занимался.

Конечно, в домашней сети эти программы могут не найти широкого применения, но это уже решать вам.

Учет трафика в сети

Небольшая сеть, состоящая из двух-трех компьютеров, обычно не требует раздельного контроля сетевого трафика для рабочих станций. Рост и расширение сети могут вызвать необходимость такого контроля. Если сеть имеет выход в Интернет, и за трафик приходится платить, то совсем не вредно знать, кто и сколько использовал трафика. Иногда может возникнуть необходимость оперативно посмотреть на текущий трафик, определить, откуда он идет, а при необходимости заблокировать этот источник. В нашей сети такая необходимость возникает, когда кто-либо нарушает требования к пользователям Интернета в организации и посещает развлекательные сайты в рабочее время, использует Интернет в личных целях, расходуя значительный трафик. В домашней (квартирной) сети тоже можно контролировать трафик, но цели могут быть иными. Если вы предоставляете доступ в Интернет через свое подключение соседям по дому, то, естественно, у вас возникнет желание учитывать расходуемый ими трафик для справедливого взимания оплаты.

Существует много средств, позволяющих решать перечисленные задачи. Одни предназначены для очень серьезного учета трафика в домовых сетях, другие — для индивидуального учета на отдельном компьютере. Но есть программы, которые можно использовать как индивидуально, так и в сети с небольшим числом компьютеров. Одна из таких программ — BWMeter

(рис. 12.10). Сайт программы находится по адресу **http://www.desksoft.com/BWMeter.htm**.

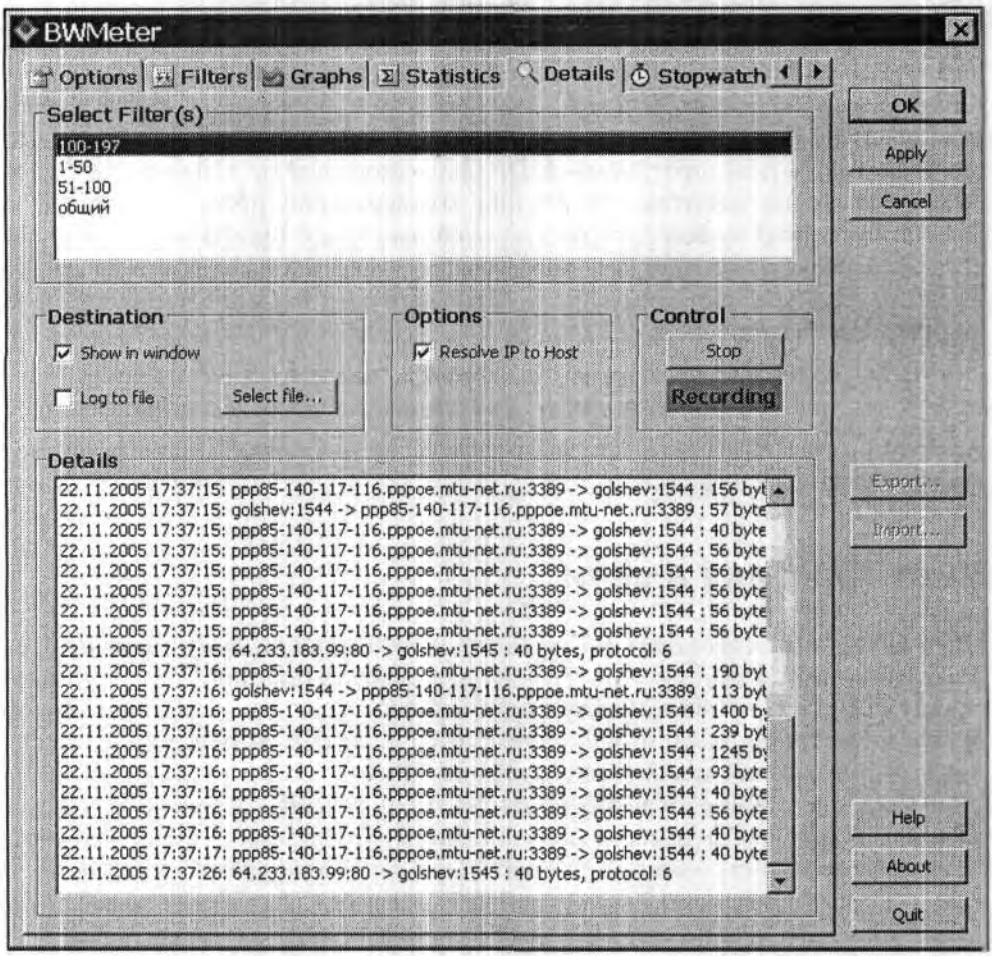


Рис. 12.10. Окно программы BWMeter, вкладка **Details**

На рис. 12.10 показана вкладка **Details** (Подробно), на которой виден процесс регистрации сетевого обмена между рабочей станцией и компьютером в Интернете. В программе можно выбрать сетевой адаптер, через который должен проходить учитываемый трафик, создать фильтры как для отдельных компьютеров сети, так и для целых групп. Можно просматривать статистику соединений за любой интервал времени и по любому настроенному фильт-

ру. Есть возможность ограничения скорости обмена для какого-либо фильтра и даже полного запрещения трафика для него.

Очень помогает при работе с программой возможность графического представления необходимых фильтров (рис. 12.11). При этом окна графиков можно произвольно располагать на рабочем столе.

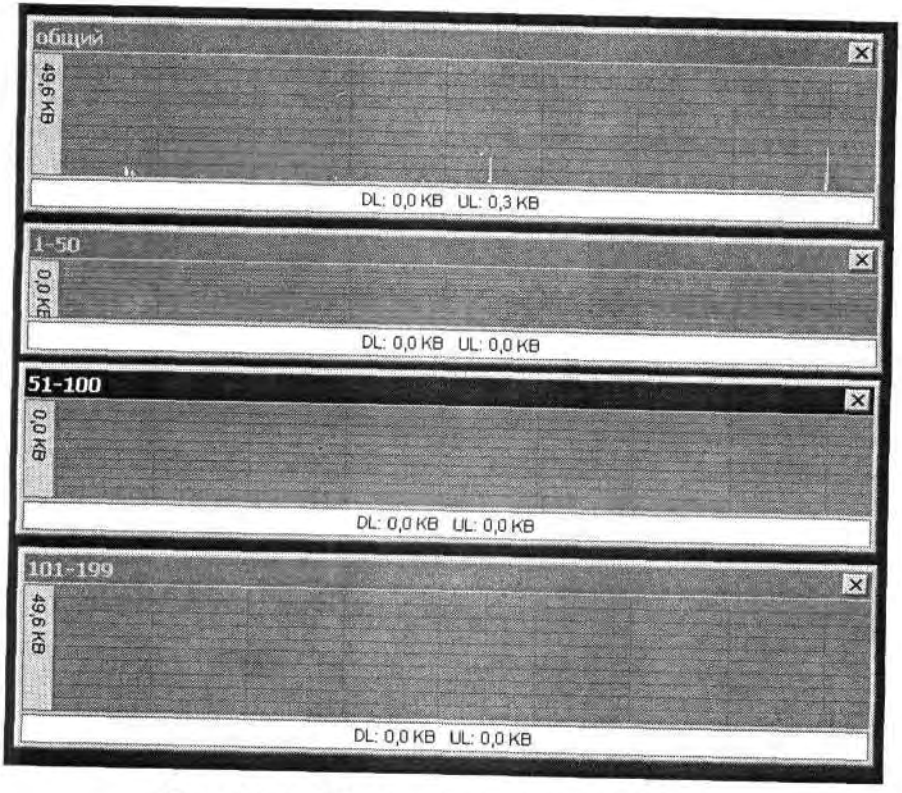


Рис. 12.11. Окна графиков программы BWMeter на рабочем столе сервера

Фильтры могут быть настроены как по IP-адресам, так и по MAC-адресам сетевых адаптеров рабочих станций. Можно указывать диапазоны IP-адресов. Это позволяет сократить число постоянно открытых окон, и наблюдать за расходом трафика группой пользователей, IP-адреса которых принадлежат определенному диапазону. Если рабочих станций не очень много, то можно вести постоянное наблюдение за использованием трафика. Наличие хорошего подключения к Интернету позволяет слушать радиопередачи с сайтов радиостанций. При этом расход трафика получается очень большим. Если у вас не безлимитное подключение, то расход в объеме 20—

30 Мбайт в минуту приведет к большим финансовым проблемам. Поглядывая время от времени на окна фильтров, вы сможете вовремя обнаружить лишний трафик и моментально принять меры к его снижению, заблокировав или снизив скорость трафика для отдельного компьютера или для целой группы компьютеров.

Управление удаленным компьютером

Вполне возможны ситуации, когда появляется необходимость передать какой-либо файл в определенный каталог удаленного компьютера, а иногда и запустить программу на удаленной машине. Причем это может быть связано совсем не с хакерскими интересами, а просто с уменьшением числа шагов администратора в течение дня. Одна из наиболее полезных программ для удаленного администрирования — Telnet. С помощью этого средства на удаленном компьютере можно выполнить любую программу командной строки, произвести действия с файлами. В качестве примера рассмотрим подключение сетевого каталога в качестве сетевого диска.

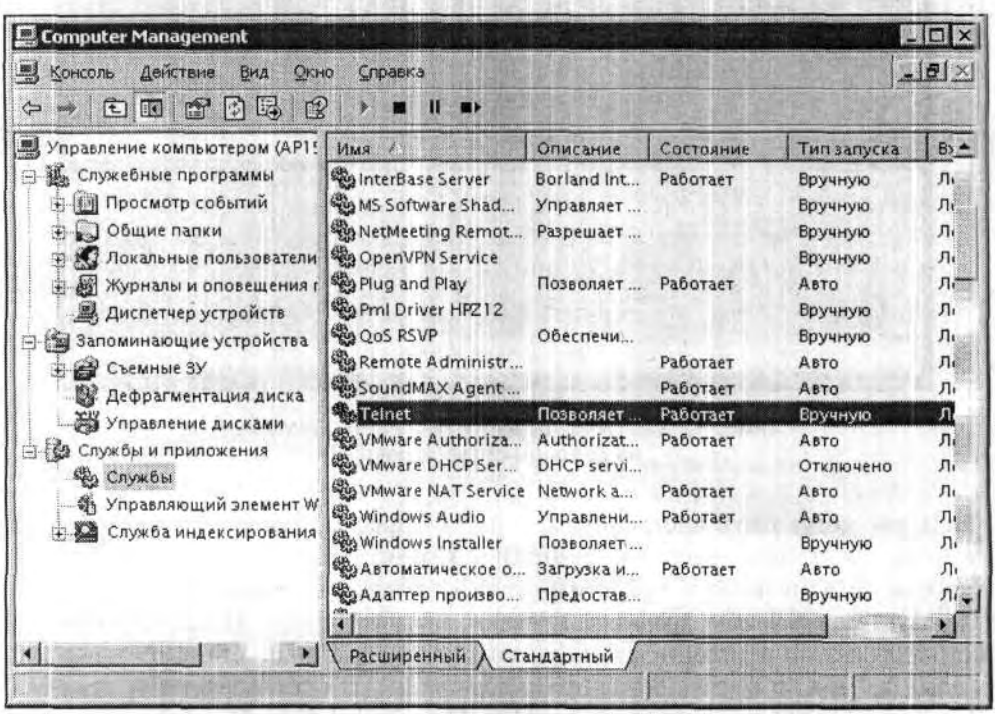


Рис. 12.12. Окно **Computer Management**

Интересно, что подключенный сетевой диск будет виден только в сеансе Telnet и не виден работающему за компьютером пользователю.

Обычно в Windows XP служба Telnet отключена, а чтобы ей воспользоваться, необходимо ее запустить. Для этого следует открыть окно **Управление компьютером (Администрирование | Управление компьютером)**. Но для его открытия нужно воспользоваться пунктом контекстного меню **Запуск от имени** и ввести параметры учетной записи администратора домена. Затем в меню **Действие** выбрать **Подключиться к другому компьютеру** и ввести в открывшемся окне имя удаленного компьютера или его IP-адрес. Откроется окно **Управление компьютером** (рис. 12.12), которое будет выглядеть аналогично окну управления локальным компьютером. В дереве объектов найдите и выделите **Службы и приложения | Службы**, а затем, найдя службу Telnet, запустите ее.

Теперь, когда служба Telnet работает, можно открывать сеанс Telnet. Для этого выполните **Пуск | Выполнить | telnet**. В открывшемся окне введите команду `open <имя_компьютера>` (рис. 12.13). После ввода имени компьютера нажмите <Enter>.

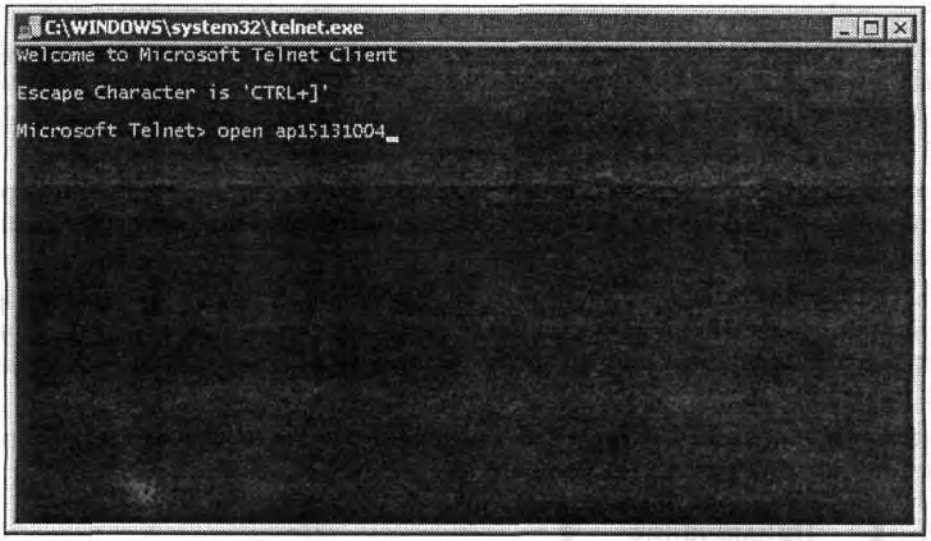


Рис. 12.13. Окно telnet.exe — ввод имени компьютера

Теперь откроется окно сеанса Telnet (рис. 12.14).

В нем необходимо ввести имя пользователя и пароль. Пароль при вводе отображаться не будет. Имя пользователя может принадлежать локальной учетной записи или администратору домена.

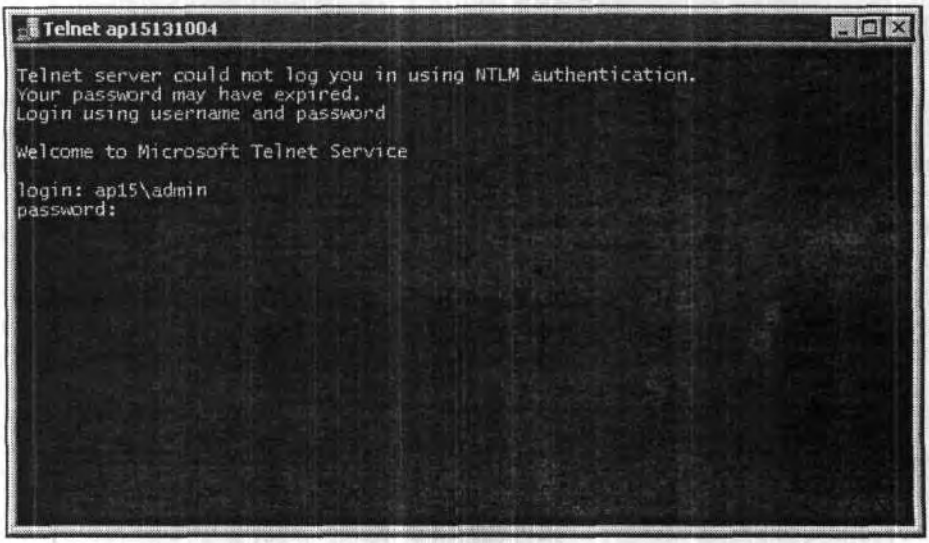


Рис. 12.14. Окно **Telnet <имя_компьютера>** — ввод имени пользователя и пароля

Теперь можно вводить команды, как в обычном окне командной строки. Зная доступный сетевой ресурс, вводим команду его подключения в качестве сетевого диска (рис. 12.15):

```
Net use <буква_диска>: \\<имя_сервера>\<имя_каталога>
```

Можно работать с подключенным сетевым диском, как обычно — копировать файлы с него в любой каталог компьютера и обратно, создавать файлы и удалять их.

При необходимости можно выполнять любые доступные из командной строки команды. Например, если у вас есть сомнения в исправности винчестера удаленного компьютера, можно воспользоваться командой `Chkdsk` для его проверки.

Для выхода из сеанса следует ввести команду `Exit`, а для выхода из программы Telnet — команду `Quit`.

Примечание

Для обеспечения безопасности удаленного компьютера следует остановить службу Telnet после завершения работы с ней.

Если заранее подготовить сценарий или командный файл с необходимыми командами, то есть возможность установки некоторых программ на удаленный компьютер (например, распространенной программы удаленного администрирования Radmin). Необходимо заранее поместить файлы программы

в доступный в сети сетевой каталог, скопировать файл сценария на диск удаленного компьютера и выполнить его через Telnet.



Рис. 12.15. Окно **Telnet <имя_компьютера>** — ввод команд

Сценарий установки предложен разработчиками программы и показан в листинге 12.12.

Листинг 12.12. Сценарий установки Radmin

```
net use z: \\<имя_сервера>\<имя_каталога>
copy "z:\install\radmin\r_server.exe" "c:\%Windir%\system32\r_server.exe"
copy "z:\install\radmin\raddrv.dll" "c:\ %Windir%\system32\raddrv.dll"
c:\ %Windir%\system32\r_server.exe /install /silence
regedit.exe /s z:\install\settings.reg
net use z: /delete
```

Telnet и Windows 98

Наличие в сети старых машин приводит к осложнениям при удаленном управлении ими. Конечно, Radmin справляется с такой задачей прекрасно, но при необходимости можно использовать и Telnet!

Правда, telnet.exe, входящий в Windows XP, некорректно работает в этом случае. Необходимо либо иметь компьютер с установленной Windows 98, либо установить виртуальный компьютер с этой ОС на вашу рабочую станцию под управлением Windows XP, либо (это проще) на Windows XP использовать HiperTerminal. Эта программа традиционно входит в состав Windows.

Для того чтобы Windows 98 получила telnet-сервер, необходимо использовать небольшую программу 123-Terminal-Server. По ссылке

http://www.download.com/123-Terminal-Server/3000-2155_4-10254733.html

можно найти последнюю версию этой программы.

Ее достаточно разархивировать в любую папку и запустить. После запуска останется только указать имя и пароль пользователя, под которым будет производиться подключение, и исходный каталог.

Сценарии входа в сеть

Рост сети приводит к осложнениям при обслуживании большого числа рабочих станций. Если подойти к двум-трем компьютерам пользователей и произвести их настройку совсем не сложно, то при наличии десятков рабочих станций даже простые действия с ними могут отнимать много времени и сил. Автоматизация получения параметров сети по DHCP — это один из первых шагов по снижению затрат времени администратора. Значительно более интересные результаты можно получить, применяя сценарии входа в сеть. Они могут быть написаны на любом языке сценариев. Это могут быть как обычные пакетные или командные файлы с расширениями bat или com, так и файлы сценариев с расширениями vbs, js и другими, которые могут выполняться на рабочих станциях вашей сети. Важно, чтобы все рабочие станции принадлежали вашему домену. В этом случае все разрешения для пользователей, установленные на сервере, назначаются пользователям при входе в сеть. Сценарии входа тоже выполняются при регистрации пользователя в сети. Это позволяет администратору иметь уверенность в том, что настройки рабочей станции будут именно такими, которые разрешены или необходимы пользователю, вошедшему в сеть с этой рабочей станции.

Для того чтобы файл сценария выполнялся при регистрации пользователя в сети, необходимо выполнить два условия.

- Файл сценария должен быть доступен всем пользователям сети для его выполнения. При установке Active Directory каталог для сценариев, доступный всем пользователям домена, создается системой автоматически. Обычно это каталог %systemroot%\SYSVOL\sysvol\<имя_домена>\scripts\. По умолчанию он не содержит никаких файлов. Только от вас зависит,

какие сценарии вы будете использовать в сети. Для пользователей сети путь к сценариям будет выглядеть, конечно, иначе:
`\\<Имя_сервера>\sysvol\<имя_домена>\scripts\`.

- Язык сценария должен поддерживаться операционной системой рабочих станций.

Сценарии могут быть как общими для большинства, так и различными для отдельных пользователей. Далее мы приведем пример сценария, состоящего из двух файлов, выполняемых последовательно. Вполне возможно использование одного файла сценария, но иногда удобнее управлять ходом сценария, применяя последовательно два и более файлов, которые могут использоваться и отдельно. Если применяются рабочие станции с Windows 98, то придется для их пользователей создавать отдельные файлы сценария входа в сеть. В примере, приведенном здесь, рассматривается сценарий входа для рабочих станций под управлением Windows XP Pro или Windows 2000. ОС Windows XP Home Edition не предназначена для работы в доменной сети. Несмотря на то, что доступ к сети возможен с таких рабочих станций, вход в домен и выполнение сценариев входа на них не возможны.

Данный сценарий выполняет следующие действия:

1. Производит дополнительную индивидуальную настройку сетевых параметров для пользователя.
2. Подключает личные и специальные сетевые каталоги пользователей.

Дополнительная настройка сети может потребоваться в случаях, когда доступ в Интернет должен контролироваться и не предоставляться всем пользователям сети, либо для разных категорий пользователей доступ в Интернет предоставляется по разным каналам. Эта настройка выполняется из пакетного файла logon.bat (листинг 12.13).

Второй файл logon.vbs (листинг 12.14) управляет подключением личных и специальных каталогов. Для каждого пользователя необходимо создать личный каталог, вложенный в общедоступный каталог users, например. Этот каталог по умолчанию не создается, и вам придется создать его самостоятельно. Данный сценарий дополнительно создает файл с описанием сетевых настроек рабочей станции, на которой он выполнен.

В примере использованы следующие предположения:

- имя сервера — mh2003s;
- имя сетевого подключения на рабочих станциях — LocalNet;
- имя домена — myhome.dom;
- IP-адрес шлюза в Интернет — 192.168.1.1;
- имя каталога, содержащего личные каталоги пользователей — Users;

- имена личных каталогов совпадают с именами учетных записей пользователей;
- информация о сброшенных сетевых настройках при входе в сеть собирается в локальных файлах C:\reset.txt на рабочих станциях;
- имена файлов сценариев на сервере Logon.bat и Logon.vbs.

Листинг 12.13. Сценарий входа в сеть Logon.bat

```
netsh int ip reset "C:\reset.txt"
netsh int ip add addres "LocalNet" gateway=192.168.1.1 gwmetric=2
\\Mh2003s\sysvol\myhome.dom\scripts\logon.vbs
```

Листинг 12.14. Сценарий входа в сеть Logon.vbs

```
On Error Resume Next

Set wshNetwork = CreateObject("WScript.Network")
' Подключаем личный каталог пользователя
wshNetwork.MapNetworkDrive "X:", "\\mh2003s\Users\" & wshNetwork.UserName

Set ADSysInfo = CreateObject("ADSystemInfo")
Set CurrentUser = GetObject("LDAP://" & ADSysInfo.UserName)
strGroups = LCase(Join(CurrentUser.MemberOf))
'Подключаем каталог администраторов
If InStr(strGroups, "administrators") Then
MsgBox strGroups & "  " & wshNetwork.computername
wshNetwork.MapNetworkDrive "Y:", "\\mh2003s\Book"

Else

' Запускаем программу диагностики (ipconfig /all)
Set objShell = CreateObject("WScript.Shell")
Set objExec = objShell.Exec("ipconfig /all ")

IsBreak=False
  Do While True  ' Бесконечный цикл
    ' Проверяем, достигнут ли конец выходного потока команды
    If (Not ObjExec.StdOut.AtEndOfStream) Then
```

```
    ' Считываем полностью выходной поток команды
    s=s+ObjExec.StdOut.ReadAll
    End If
    If IsBreak Then
      Exit Do  ' Выходим из цикла
    End If
    ' Проверяем, не завершилось ли выполнение команды
    If ObjExec.Status=1 Then
      IsBreak=True
    Else
      WScript.Sleep 100 ' Приостанавливаем сценарий на 0,1 сек
    End If
  Loop
ArrS=Split(s,vbCrLf)  ' Формируем массив строк
ColStr=UBound(ArrS)  ' Количество строк в сообщении команды
strtxt=""
For i=1 To ColStr
strtxt=strtxt+ArrS(i-1) & VbCrLf
Next
strtxt=strtxt & Err.Description
set FSO = CreateObject("Scripting.FileSystemObject")
        txtlog = "\\mh2003s\Users\" & wshNetwork.computername & ".txt"
        Set LogFile = FSO.CreateTextFile(txtlog, True)
             LogFile.WriteLine  Date & " " & Time &  vbCrLf & strtxt
        LogFile.Close

End If
```

Файл Logon.bat выполняется одинаково на всех рабочих станциях, если именно он указан в свойствах учетной записи, как файл сценария входа в сеть. Из него вызывается Logon.vbs, вариант выполнения которого зависит от учетной записи регистрирующегося пользователя. Если эта учетная запись входит в группу administrators, то происходит подключение личного каталога пользователя и специального каталога \\mh2003s\Book, доступ к которому необходим администраторам. Если вход осуществляет обычный пользователь, то специальный каталог не подключается, но выполняется сбор информации о сетевых настройках рабочей станции с помощью программы ipconfig. Результат работы этой программы помещается в текстовый файл с именем компьютера, на котором он создается, а сам файл помещается в каталог \\mh2003s\Users.

Наличие этой информации позволяет контролировать правильность настроек при неполадках с сетью на рабочих станциях, помогает идентифицировать рабочие станции при анализе работы сети. При необходимости в сценарий входа можно включать и другие команды, позволяющие проводить оперативную диагностику сети. Используя в сценариях диалоговые окна, можно просить пользователей вносить какую-либо дополнительную информацию, сохраняющуюся в передаваемом файле. Познакомившись с Windows Script Host, вы сможете совмещать в одном файле сценарии на разных языках, используя преимущества каждого. Начать поиск информации о Windows Script Host можно по адресам в Интернете:

- **http://www.codenet.ru/progr/other/wsh.php**
- **http://www.networkdoc.ru/insop/whs.html**

Средства устранения неисправностей

В разрастающейся сети поиск неисправностей практически не отличается от поиска неисправностей в обычной маленькой офисной сети. Но физически выросшие расстояния между узлами сети заставляют задуматься о методах работы, позволяющих сократить путешествия по территории, занимаемой сетью. Чем больше пользователей сети, тем большее значение имеет наличие удобных инструментов для анализа работы сети. К счастью, в наше время таких инструментов разработано и доступно много. Уже имея опыт обнаружения проблем в небольшой сети, вы сможете без больших усилий найти неисправность в укрупнившейся сети, осознанно применяя доступные инструменты.

Не рассматривая подробно работу с этими инструментами, перечислим адреса, по которым можно найти упомянутые средства, и коротко укажем их назначение.

По адресу **http://www.famatech.com/ru/index.php** находятся несколько программ.

- **Remote Administrator** (Radmin) — это одна из лучших программ безопасного удаленного администрирования для платформы Windows, которая позволяет полноценно работать сразу на нескольких удаленных компьютерах с помощью обычного графического интерфейса. Наряду с поддержкой модели безопасности NT и локализацией на любые языки, возможна работа в режимах File transfer и Telnet, что позволяет рассматривать Radmin как интегрированное решение для удаленного управления организацией любого масштаба.
- **Advanced IP Scanner** — это быстрый, надежный и простой в использовании сканер локальной сети (LAN) для Windows, который может интегрироваться с Radmin 2.2. Он позволяет с легкостью получать различную

информацию о компьютерах в локальной сети за считанные секунды! Дает доступ в "один клик" ко многим полезным функциям, таким как удаленное включение и выключение компьютера, и многое другое.

- **Advanced Port Scanner** — это компактный, быстрый, надежный и простой в использовании сканер портов для платформы Win32. Он использует технологию многопоточности (multithread), поэтому на мощных компьютерах вы можете сканировать порты с очень высокой скоростью. Также он содержит описания стандартных портов и может выполнять сканирование на предустановленном диапазоне портов.
- **Advanced IP Address Calculator** — это простой в использовании калькулятор IP-адресов подсети, который позволяет рассчитать параметры конфигурирования вашей подсети всего за пару щелчков мышью.
- **Advanced LAN Scanner** — это компактный, простой в использовании и очень быстрый сканер для платформы Win32 с большим количеством настроек.

По адресу **http://www.lantricks.narod.ru/** вы можете найти сразу целый комплект инструментов, основанных на стандартных функциях операционной системы, но имеющих весьма широкие возможности.

- **LanScope** — это многопотоковый сканер ресурсов NetBIOS (разделяемых) и FTP. Сканирует заданные диапазоны адресов и определяет доступность ресурсов (чтение, запись). Позволяет искать ресурсы с заданным именем (Music, Video и т. п.). Определяет наличие установленных сервисов (FTP, HTTP) на удаленном хосте.
- **LanSpy** — это сканер компьютеров в сети, который позволяет получить различную информацию о компьютере: доменное и NetBIOS-имена, MAC-адрес, информацию о сервере, информацию о домене и контроллере домена, удаленное управление, время, диски, транспорты, пользователи, глобальные и локальные группы пользователей, настройки безопасности, разделяемые ресурсы, сессии, открытые файлы, сервисы, информацию из реестра и журнала событий.
- **LanSend** — позволяет отправлять сообщения на компьютер или группу компьютеров в реальном режиме времени, также вы можете отправить сообщение заданное количество раз через определенный промежуток времени.
- **LanSafety** — эта программа поможет вам установить параметры Windows таким образом, чтобы ваша работа в сети стала более безопасной. Поможет скрыть ваш компьютер в сетевом окружении, запретить анонимный доступ, отключить административные ресурсы.
- **LanShutDown** — эта программа позволит вам выключить питание или перегрузить компьютер под управлением W2K/XP по сети. Дополни-

тельно вы можете написать сообщение, которое будет показано перед выключением.

- **LanCalculator** — это программа, которая позволит вам без труда рассчитать диапазон адресов в подсети и маски подсети, а также широковещательный адрес, адрес сети, префикс сети и инверсию маски сети, которая используется в списках доступа (ACL) сетевого оборудования Cisco. Введите адрес и маску сети, нажатием одной кнопки вы сможете рассчитать все параметры.
- **LanWhoIs** — это программа, позволяющая узнать, кем, где и когда зарегистрирован интересующий вас домен или сайт, а также информацию о тех, кто его обслуживает. Программа **LanWhoIs** ответит на ваши вопросы, рассказав все о владельце домена (сайта) или IP-адреса!
- **LanLoad** — это менеджер закачек в локальных сетях. LanLoad предназначен для копирования файлов (папок) в локальных сетях с неустойчивой связью между компьютерами. Программа обладает возможностью приостановки и продолжения процесса копирования.

Можно испытать и другие средства, вероятно, они пригодятся именно вам. По адресу **http://www.killprog.com** можно найти **NetView** — довольно мощный инструмент для мониторинга и администрирования локальных сетей с не менее мощным инструментарием для выполнения вспомогательных функций. Потенциал NetView можно расширить с помощью плагинов. На сайте размещено множество утилит для работы в сети.

На **http://www.tmeter.ru/** доступна небесплатная программа **Tmeter**. С ее помощью вы можете производить точный подсчет интернет-трафика для офисной сети, организовать гибкую и полноценную систему учета трафика ваших пользователей. Там же можно получить бесплатную программу **LanSpector** — многофункциональный сетевой сканер/сниффер — основные возможности которой — это просмотр доступных (shared) ресурсов в локальной сети, поиск и проверка паролей к ресурсам для всех версий Windows, сканирование диапазона IP-адресов на общеупотребительные сервисы, запрос функций NetBIOS, простой Telnet-клиент, простой SMTP-клиент, вывод статистики по сетевым подключениям (NetStat).

Скорее всего, вы не станете применять все эти инструменты, но "на вкус и цвет товарищей нет", и вы подберете утилиты самостоятельно. Со временем вы найдете в Интернете более сложные утилиты, сами будете создавать для себя вспомогательные средства, работая со сценариями. Простые средства могут быть предназначены для решения конкретных задач, связанных, например, с многократным продолжительным сканированием одного и того же IP-адреса для выявления нестабильного дефекта связи между двумя узлами сети.



Глава 13

О развлечениях

Сеть — это не только работа и деловое общение. Сеть — это и среда развлечений. Игры, музыка и кино доступны каждому, у кого есть хороший доступ в Интернет или в сеть, которая содержит соответствующие ресурсы. Дело не только в том, что есть доступ к этим развлечениям, но в качестве и удобстве этого доступа. Чем больше сеть, тем скорее может появиться необходимость в организации сервисов, которые в малой сети могут не иметь особой актуальности. По числу компьютеров эта сеть может и не быть большой, но если у вас дома три-четыре компьютера, то для квартиры это уже большая сеть.

Беспроводная сеть дома

Возможно, вам приходилось посещать интернет-кафе, где для привлечения клиентов применяется бесплатный беспроводной доступ в Интернет с ноутбука посетителя. Такой способ подключения к сети может быть удобен и в домашних условиях или в офисе. При этом не приходится подключать кабели к ноутбуку, чтобы подключиться к домашней сети, прогуляться в Интернет, поиграть в игры или послушать музыку. И не только ноутбуки могут иметь такое подключение. Кто мешает подключить без проводов обычную рабочую станцию? Существуют также беспроводные медиаплееры и другие устройства, которые можно подключать к сети. Проведя в квартиру кабель домовой сети или организовав доступ в Интернет через ADSL-модем, вы можете и не прокладывать по квартире кабели для обеспечения работы всех домашних компьютеров. Достаточно приобрести средства радиодоступа к сети. В последнее время таких средств выпускается все больше и больше. Качество соединений и их безопасность повышаются.

Оборудование

Какой тип оборудования вы будете применять в своей практике, зависит от ваших потребностей и возможностей. Рассматривая следующий пример,

мы совершенно не настаиваем на использовании именно такого оборудования. Просто в нашем распоряжении оказался именно этот комплект, на базе которого был подготовлен пример. Комплект был приобретен обычным пользователем ПК для организации доступа к домовой сети и Интернету с ноутбука.

В состав комплекта входило следующее оборудование:

- модем D-Link DFM-562E;
- беспроводный адаптер D-Link DWL-G122 USB стандарта 802.11g;
- беспроводной 802.11g VPN маршрутизатор DI-824VUP+.

Модем D-Link DFM-562E — это аналоговый модем V.92/V.90, 56 Кбит/с, разработанный для сетей малых офисов и дома. Его можно подключить к любому телефонному порту для предоставления настольным и портативным компьютерам доступа к Интернету через телефонную линию. Модем подключается к любой настенной телефонной розетке, исполняя роль устройства набора номера при запросе от компьютера. Этот недорогой модем позволяет пользователю путешествовать по Интернету и получать доступ к почтовому серверу. В дополнение к коммуникационному программному обеспечению, совместимому с AT-командами, модем DFM-562E предлагает средства передачи и приема факсов на скорости до 14,4 Кбит/с. Модем выполняет V.42bis и MNP 2-4 сжатие данных, а также коррекцию ошибок для быстрого и надежного приема/передачи.

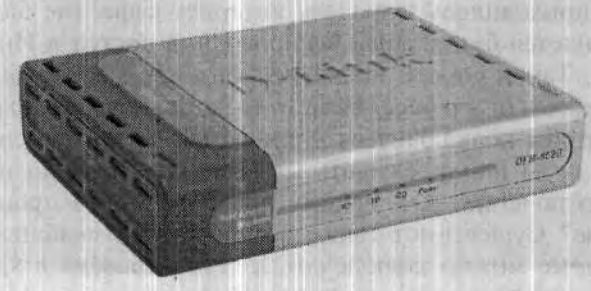


Рис. 13.1. Вид модема D-Link DFM-562E

В примере не описываются настройки модема, поскольку для большинства модемов они похожи. А в большинстве случаев такие настройки вообще не требуются. Но если будет необходимость применения модема совместно с маршрутизатором, который используется в примере, то желательно, чтобы оба устройства были одного изготовителя. Следует также иметь в виду, что модемы выпускаются с различными вариантами подключения. Этот модем подключается к COM-порту компьютера или маршрутизатора.

Но в последнее время на ноутбуках часто отсутствует COM-порт. В этом случае для подключения к компьютеру необходимо приобретать модем с USB-подключением.

Беспроводный адаптер D-Link DWL-G122 USB стандарта 802.11g используется для соединения компьютера с высокоскоростной беспроводной сетью. Этот адаптер легко подключается к компьютеру через быстрый порт USB 2.0 и обеспечивает скорость беспроводного соединения до 54 Мбит/с. DWL-G122 поддерживает стандарт взаимодействия 802.11g, сохраняя обратную совместимость с устройствами 802.11b, и обеспечивает установку Plug-and-Play. Адаптер DWL-G122 поддерживает скорость передачи данных до 54 Мбит/с при совместной работе с другими беспроводными устройствами стандарта 802.11g. Это выгодно отличает его от адаптеров 802.11b, которые работают только на скорости до 11 Мбит/с. Как и устройства 802.11b, DWL-G122 использует один диапазон частот 2,4 ГГц, избегая сложностей, присущих двухдиапазонным сетям. Совместимость стандарта 802.11g с существующими стандартами беспроводных сетей означает, что нет необходимости менять все сетевое оборудование для поддержки соединения. DWL-G122 и другие устройства стандарта 802.11g можно постепенно добавлять в существующую сеть, в то время как остальное оборудование сети сможет продолжать взаимодействовать. Реализация Wi-FI Protected Access в DWL-G122 предоставляет необходимые протоколы и средства обеспечения безопасности, поэтому пользователи могут общаться между собой с сохранением конфиденциальности, а при получении доступа к важной информации компании или передаче данных динамически выполняется шифрование данных. WPA обеспечивает авторизацию и идентификацию пользователей на основании секретного ключа, который автоматически меняется по истечении некоторого периода времени. При совместной работе с сервером RADIUS WPA использует протокол TKIP (Temporal Key Integrity Protocol, протокол целостности временного ключа) для смены временного ключа каждые 10 000 пакетов. Это обеспечивает более высокий уровень безопасности, чем стандарт Wep, который требует смены ключа вручную. DWL-G122 оснащен быстрым портом USB 2.0 и кабелем USB для подключения к компьютеру, обеспечивая пропускную способность до 480 Мбит/с между сетевым адаптером и компьютером. Это примерно в 40 раз быстрее, чем предыдущая спецификация USB 1.1, что и позволяет использовать преимущества высокой скорости беспроводной связи 54 Мбит/с данного адаптера. Благодаря возможности "горячей" установки и функции Plug-and-Play DWL-G122 обеспечивает быстрое и легкое соединение с другими беспроводными устройствами вне зависимости от того, используют ли они стандарт 802.11b или более быстрый 802.11g.

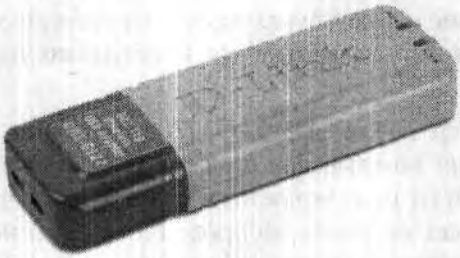


Рис. 13.2. Вид адаптера D-Link DWL-G122 USB

Беспроводной 802.11g VPN маршрутизатор DI-824VUP+ объединяет функции широкополосного доступа в Интернет с надежной VPN-защитой межсетевым экраном, встроенным принт-сервером и 4-портовым коммутатором для подключения принтера и рабочих станций. Маршрутизатор обеспечивает высокую скорость передачи по беспроводной сети, безопасные VPN-подключения, расширенную защиту межсетевым экраном и фильтрацию содержимого пакетов, основанную на политиках. Это устройство предоставляет экономичный способ установки безопасной и быстродействующей сети с каналом связи без узких мест к внешнему миру. Благодаря встроенной беспроводной точке доступа, 4-портовому коммутатору 10/100 Мбит/с и принт-серверу данный маршрутизатор обеспечивает готовое подключение для рабочих станций и серверов. Таким образом, эти встроенные функции позволяют избежать проблем, связанных с установкой отдельной точки доступа, коммутатора Ethernet и принт-сервера. При работе с другими устройствами серии D-Link AirPlusG+ DI-824VUP+ обеспечивает пропускную способность в 10 раз выше, чем у стандарта 802.11b. При работе с другими устройствами 802.11g DI-824VUP+ поддерживает передачу данных на скорости до 54 Мбит/с. Маршрутизатор совместим со всеми беспроводными устройствами стандарта 802.11b/b+. Он имеет встроенную поддержку VPN, что позволяет создавать множество туннелей IPSec для удаленных офисов. Реализация IPSec использует шифрование DES, 3DES, AES и управление ключами (Automated Key Management) согласно спецификации IKE/ISAKMP. Туннель VPN может быть активирован от маршрутизатора к удаленному офису или мобильному пользователю для безопасной передачи потока данных с применением шифрования triple DES — пользователи могут конфиденциально получать доступ и передавать важную информацию. Множество туннелей VPN могут быть легко созданы без необходимости определения правил протокола обмена ключами (Internet Key Exchange, IKE). В дополнение к туннелям VPN, маршрутизатор также поддерживает VPN в режиме pass-through для тех пользователей, кто хочет применять собственное ПО клиента VPN. Защита межсетевым экраном включает Intrusion Detection System (IDS, детектор вторжений) и механизм анализа содержимого пакетов

(Stateful Packet Inspection, SPI). Маршрутизатор защищает сеть от атак и ведет файл регистрации для его последующего анализа с целью выявления нежелательных событий. Блокировка URL и фильтрация доменов являются частью основных функций, предлагаемых маршрутизатором. Эти функции ограничивают доступ к нежелательным ресурсам Интернета. Маршрутизатор блокирует и перенаправляет определенные порты, ограничивая сервисы во внутренней сети, к которым внешние пользователи могут получить доступ. Виртуальный сервер используется для перенаправления сервисов на несколько серверов. Маршрутизатор может быть настроен таким образом, что отдельные FTP, Web и игровые серверы смогут совместно использовать один, видимый извне IP-адрес и, в то же время, останутся защищенными от атак хакеров. Установки DMZ (демилитаризованная зона) применяются для единичного клиента (например, Web-сервера), находящегося за маршрутизатором, для полного доступа к нему из Интернета и гарантии полной совместимости приложений Интернета, даже если определенный порт не известен. Это позволяет поддерживать Web-сервер и использовать средства электронной коммерции, обеспечивая безопасность локальной офисной сети. Маршрутизатор имеет двунаправленный параллельный и USB-порты для подключения принтера — пользователи офисной сети могут совместно применять параллельный и USB-принтеры для печати файлов и Web-страниц.



Рис. 13.3. Вид маршрутизатора DI-824VUP+

Примечание

Информация о применяемых компонентах получена со страниц сайта **http://dlink.ru**.

Как видно из описаний, возможности этого оборудования весьма широки. В примере мы используем лишь небольшую их часть.

Организация сети

Один из распространенных вариантов использования беспроводного оборудования — это подключение к сети офиса или квартиры. На рис. 13.4 представлена схема домашней сети с использованием маршрутизатора DI-824VUP+. Версия устройства "цифрового дома", которую можно увидеть на странице **http://www.dlink.ru/products/home/dhome.php**, отличается значительно большим числом точек радиодоступа и других устройств беспроводной связи.

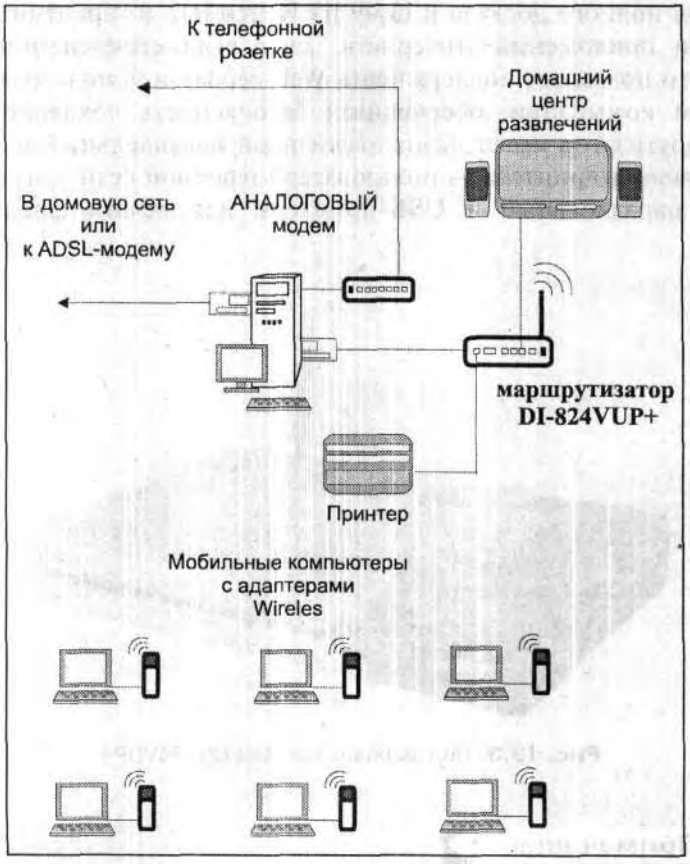


Рис. 13.4. Общая схема домашней сети с использованием маршрутизатора DI-824VUP+

Мы выбрали вариант, который может подойти многим пользователям домашних и офисных сетей с различным уровнем доходов. Предполагается, что подключение к Интернету обеспечивается одним из распространенных способов.

Обычно это:

- подключение через обычный модем с обеспечением общего доступа к этому подключению;
- высокоскоростное подключение через ADSL-модем или выделенную линию. Возможно, что линия связана с более крупной домовой сетью, через которую обеспечено предоставление доступа в Интернет. К этому подключению также обеспечивается общий доступ.

Канал связи с Интернетом может быть подключен непосредственно к маршрутизатору, но сначала мы рассмотрим вариант, когда он подключен к компьютеру или локальной сети. Это было вызвано тем, что, во-первых, во многих домашних и офисных сетях такое общее подключение к Интернету уже работает, а во-вторых, тем, что не всякое модемное подключение может работать через применяемый маршрутизатор. Подключение к некоторым провайдерам вообще не удавалось, когда попытка соединения делалась со стороны маршрутизатора. Вероятно, в таких случаях проверялась версия операционной системы или интернет-браузера. Естественно, что маршрутизатор не может сообщить такие данные о себе. Позднее мы рассмотрим вариант удачной настройки при подключении аналогового модема к маршрутизатору.

А пока нашему маршрутизатору предстоит подключиться к сетевому адаптеру, который "смотрит внутрь" нашей сети.

Примечание

Возможно подключение и к коммутатору, который связан с этим сетевым адаптером. Либо присоединение дополнительных устройств к имеющимся Esernet-портам самого маршрутизатора, который может выполнять функции коммутатора в сети.

Для того чтобы иметь возможность изменять настройки маршрутизатора, контролировать его работу, необходим компьютер. Для того чтобы работа маршрутизатора уже на самом начальном этапе была близка к реальной, мы использовали ноутбук с подключенным к нему беспроводным адаптером D-Link DWL-G122 USB стандарта 802.11g.

Достаточно установить программное обеспечение, прилагаемое к адаптеру, и вы уже можете соединяться с маршрутизатором для его настройки и администрирования, подключив его, конечно, к источнику питания. Для подключения к маршрутизатору через радиоканал необходимо в адресной стро-

ке Internet Explorer набрать 192.168.0.1. Именно такой адрес по умолчанию имеет маршрутизатор. Для подключения нужно ввести имя и пароль администратора (рис. 13.5). Для нового устройства это имя admin, а пароль просто пустой (отсутствует). Конечно, есть возможность изменить и имя, и пароль, но до завершения всех настроек этого делать не стоит.

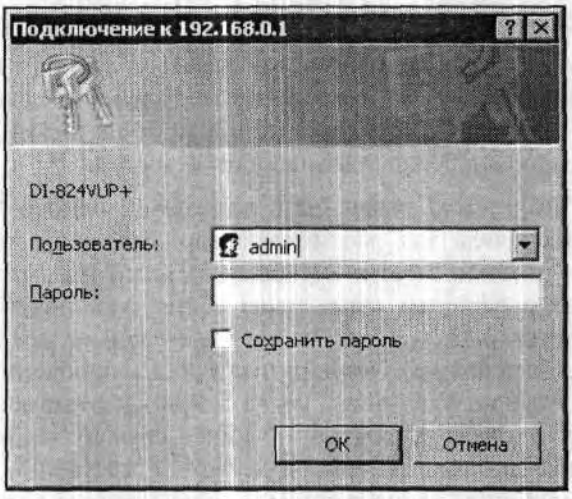


Рис. 13.5. Подключение к 192.168.0.1 (окно авторизации)

После успешной авторизации появится страница, предлагающая воспользоваться мастером настройки, который поможет выполнить быстрое подключение к Интернету (рис. 13.6). Для этого следует нажать кнопку **Run Wisard**.

Несколько ответов, и подключение настроено. После завершения работы мастера требуется перезагрузка маршрутизатора. После того как снова установится подключение, будет доступна корректировка выполненных настроек или повторный запуск мастера конфигурации.

Некоторых настроек мастер конфигурации не касается. В их числе и параметры сети, в которой должен работать маршрутизатор (рис. 13.7). Нажав кнопку LAN, можно увидеть и при желании изменить эти настройки. Но в этом редко возникает необходимость. Значительно чаще требуются настройки внешней для маршрутизатора WAN-сети. Нажав кнопку WAN, вы получите доступ к этим настройкам (рис. 13.8). Маршрутизатор может быть подключен к сети как одно из рядовых устройств. Поэтому IP-адрес маршрутизатора не отличается какими-либо особенными признаками. В примере внешняя для маршрутизатора сеть может иметь шесть устройств, включая главный компьютер (сервер) и сам маршрутизатор. Ограничение, конечно,

условно. Просто установлена маска подсети 255.255.255.248. В данном случае маршрутизатор настраивается для доступа в Интернет, который обеспечен внешней сетью. В полях для адресов DNS-серверов вводим доступные адреса. Один из них соответствует сети еще более крупной (городской), в которой работает поставщик услуг доступа в Интернет, но все-таки и эта сеть тоже локальная. Адрес 10.109.0.1 не может принадлежать Интернету. Для компьютеров, которые будут подключены по радиоканалу к нашему маршрутизатору, будут доступны как ресурсы домашней (квартирной, офисной) сети, так и ресурсы внешней городской сети (FTP и Web-серверы), и ресурсы Интернета.

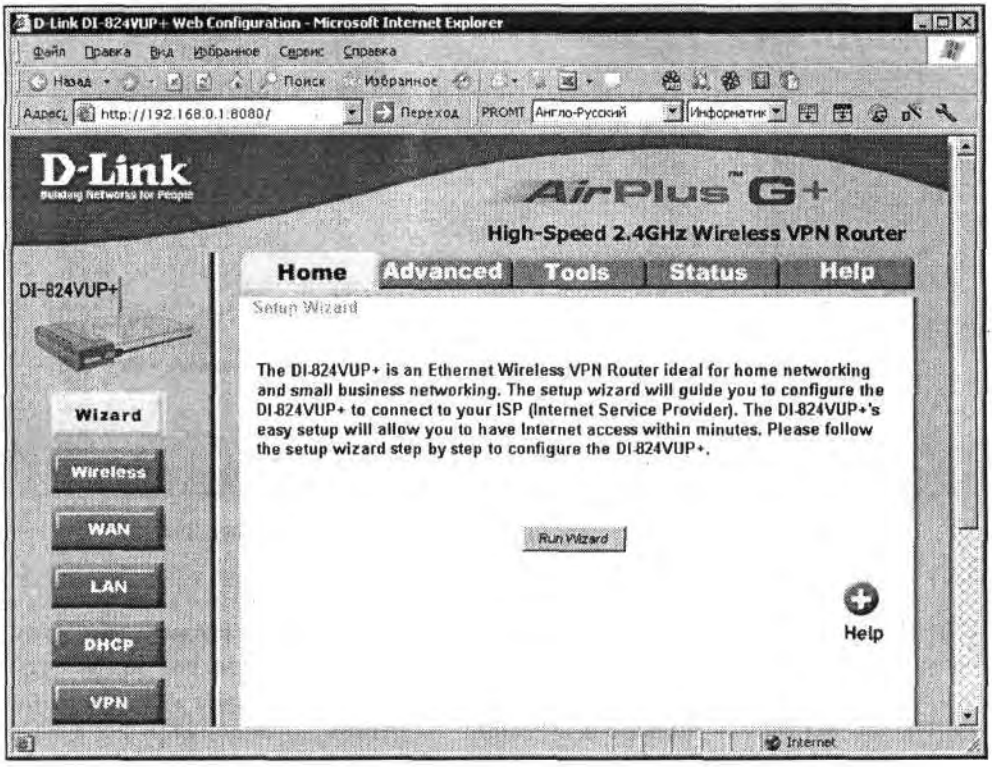


Рис. 13.6. Окно конфигурации маршрутизатора DI-824VUP+

Если в домашней (квартирной) сети находятся устройства, допускающие управление через сеть (в нашем примере условный центр развлечений), то, приходя с ноутбуком домой, вы сможете удобно устроиться в кресле, а ваш ноутбук позволит и управлять сетевой техникой, и прогуляться по Интернету или ресурсам городской сети, ну и, конечно, просто поработать или на-

писать электронное письмо, которое тут же может быть отправлено. Можно посетить свою сеть на работе, если такое подключение настроено и разрешено. Это позволит вовремя обнаружить признаки надвигающихся проблем, предпринять необходимые меры, а если проблем не обнаружено, то просто приобрести спокойствие и уверенность в том, что ваша сеть работает прекрасно, не доставляя вам лишних хлопот и неприятностей.

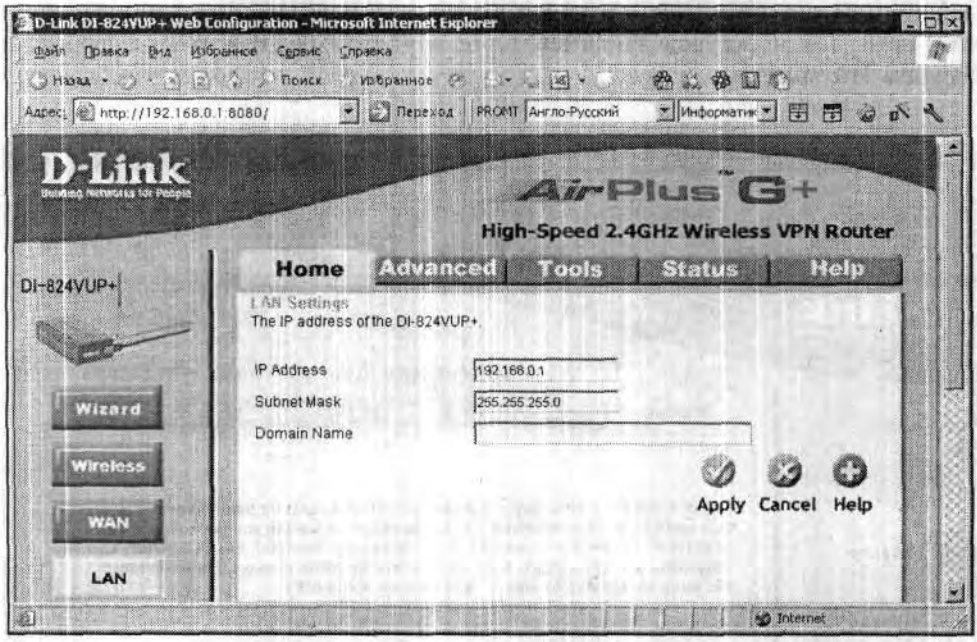


Рис. 13.7. Окно конфигурации маршрутизатора DI-824VUP+. **LAN** (настройка локальной сети)

Если вам придется иметь дело именно с таким маршрутизатором, который рассмотрен ранее, то вы увидите, что его возможности много шире, чем описанные в примере. Но не стремитесь использовать сразу все. Так, например, не пытайтесь подключить маршрутизатор к двум каналам доступа к Интернету. Маршрутизация может быть обеспечена к одному источнику. Можно, конечно, подключить все и при необходимости воспользоваться тем или иным вариантом подключения изменять настройки маршрутизатора.

Среди прочих устройств на схеме сети (рис. 13.4) изображен принтер. У DI-824VUP+ есть порты LPT и USB для подключения принтера. При этом не требуется иметь компьютер, управляющий принтером. Задания печати будут направляться без посредников на получившийся принт-сервер. IP-адрес принт-сервера такой же, как и у самого маршрутизатора.

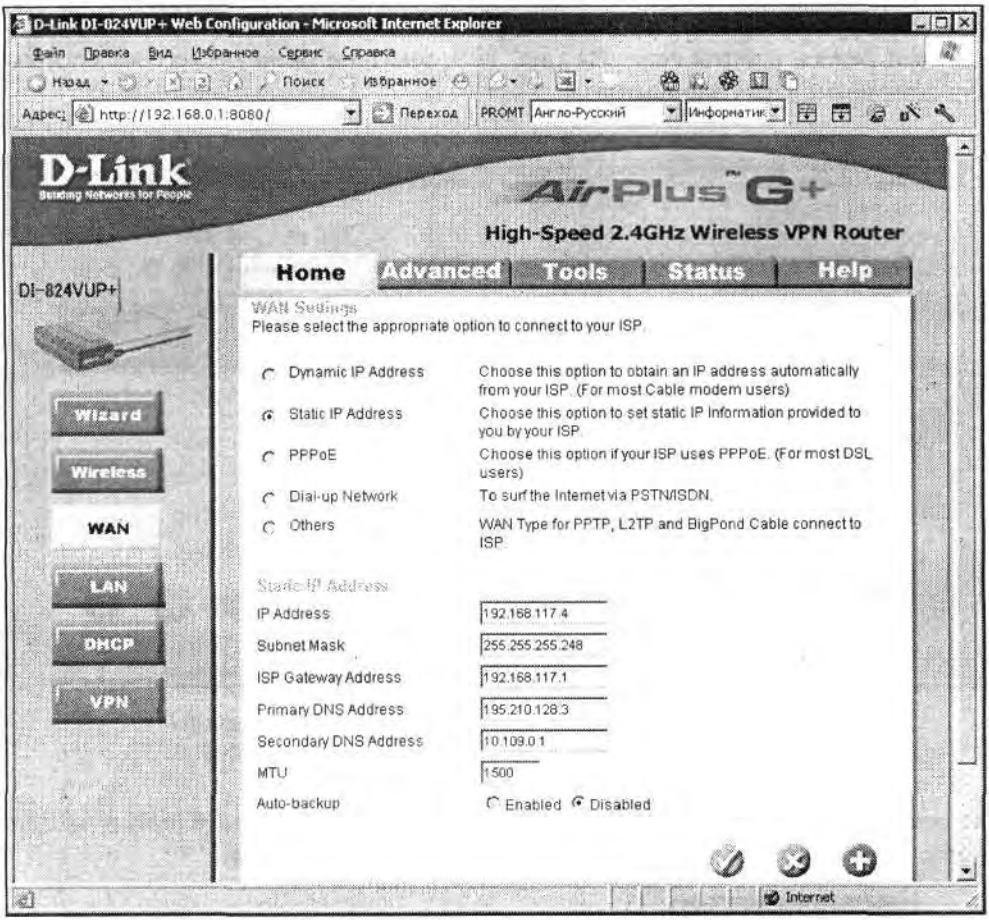


Рис. 13.8. Окно конфигурации маршрутизатора DI-824VUP+. **WAN** (настройка параметров глобальной сети)

Остальные настройки вы сможете рассмотреть подробно, если столкнетесь именно с таким устройством. Но прежде, чем вы будете приобретать необходимое оборудование, нужно проанализировать потребности и не покупать устройства с излишне широкими возможностями. Давно замечено, что чем уже специализация, тем выше качество работы устройств, меньше сбоев и непонятных процессов.

Не стоит забывать и о защите. Как только к ноутбуку подключился Wireless-сетевой адаптер DWL-G122 USB, появляется теоретическая возможность подключения к этому компьютеру из другой радиосети. Но это осуществимо только при выключенном брандмауэре для данного подключения. Независимо от наличия защиты на компьютерах сети возможен доступ к настрой-

кам маршрутизатора со стороны злоумышленника. Можно выбрать защищенный режим работы сети. На рис. 13.9 показано окно настройки сети со списком возможных вариантов.

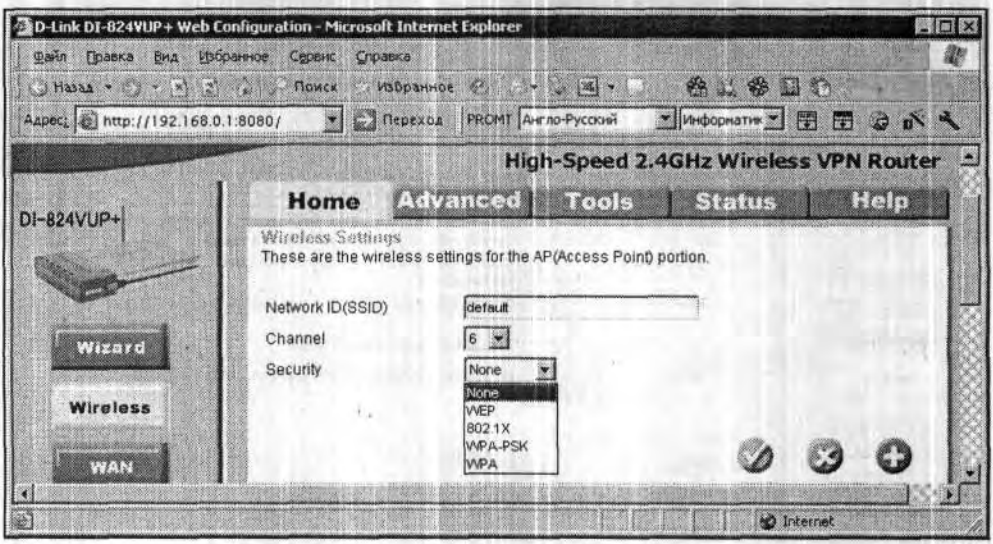


Рис. 13.9. Окно конфигурации маршрутизатора DI-824VUP+. **Wireless** (настройка параметров защиты радиосети)

На рис. 13.10 уже выбран вариант шифрования информации в сети и введен ключ, который только что пришел в голову администратору.

Внимание

Запишите этот ключ, не закрывая страницу в интернет-браузере! Теперь у вас нет доступа к сети, ноутбук настроен на работу с открытой сетью без шифрования!

Ну, на самом деле паниковать не стоит. Откройте свойства вашего подключения (рис. 13.11) и введите тот же самый ключ в поле **Ключ сети**. Сохраните изменения, соединение должно восстановиться. Если все же произошла ошибка, то выход опять есть — он в сбросе всех настроек маршрутизатора кнопкой **reset**, которая находится около гнезда питания на задней панели устройства. Для нажатия этой кнопки придется воспользоваться каким-либо тонким предметом, например, спичкой.

После перезагрузки маршрутизатора подключение должно восстановиться в исходном режиме. Придется прописать все работавшие уже настройки и повторить опыт с переходом на шифрование информации, но более аккуратно.

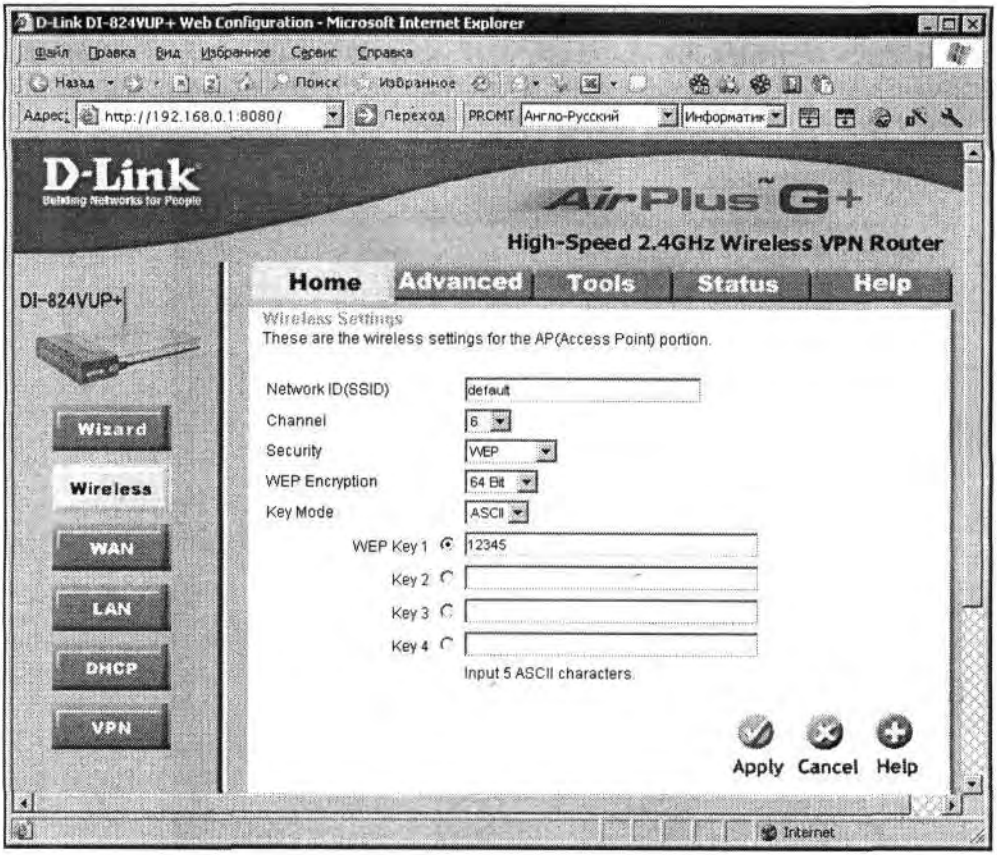


Рис. 13.10. Окно конфигурации маршрутизатора DI-824VUP+. **Wireless** (настройка параметров защиты радиосети, выбор варианта шифрования)

Если все получилось, то можно наслаждаться работой в сети без проводов. Но как бы вам не понравилась работа в такой сети, следует учитывать, что радиосвязь не так надежна, как кабель. Какие-либо очень ответственные операции в сети (а особенно в удаленной сети) лучше проводить, подключившись кабелем. Во время экспериментов с радиосетью наблюдалось пропадание связи. Причем наиболее частыми перерывы были до включения брандмауэра и шифрования информации. Похоже, что не только от непрошенных вторжений, но и от обычных помех помогает защита сети шифрованием. Вполне вероятно, что такое поведение может быть присуще и другим видам устройств Wireless-сети.

После завершения всех настроек есть смысл изменить имя и пароль администратора этого маршрутизатора. Это особенно важно, если сеть работает без шифрования. Любой человек, оказавшийся в зоне действия сети с ноут-

буком, снабженным Wireless-адаптером, сможет подключиться к маршрутизатору для изменения его настроек, если оставлены имя и пароль, предложенные изготовителем устройства. В описанном варианте защиты применен самый простой алгоритм шифрования данных, передаваемых по сети.

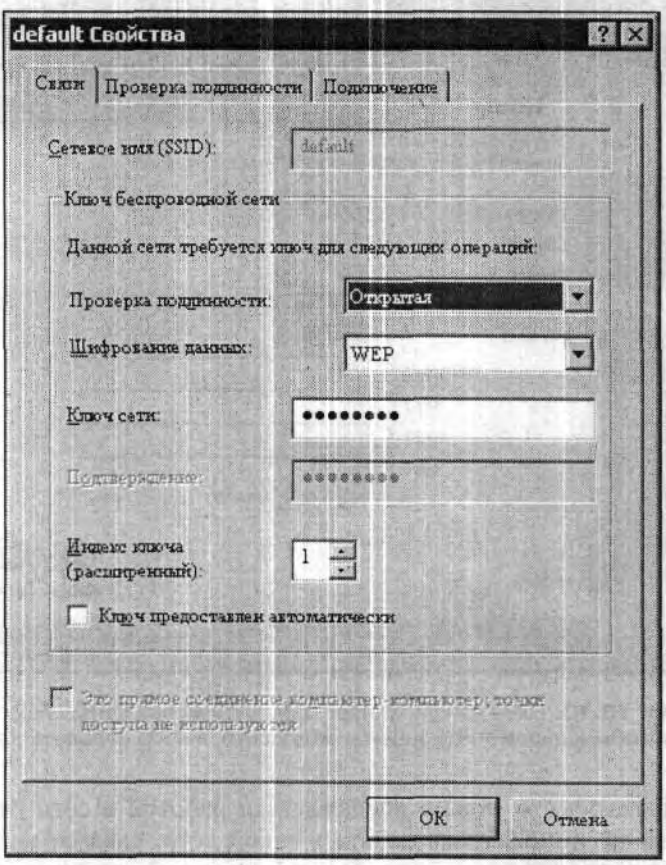


Рис. 13.11. Окно свойств Wireless-подключения на компьютере. Ввод ключа сети

Тема защиты радиосетей достаточно широка, и если вы хотите ознакомиться с другими методами защиты беспроводной сети, обратитесь к справочной информации Windows или ресурсам Интернета:

- **http://www.rozetka.de/publication/cat_4**
- **http://www.cir-sanych.ru**
- **http://www.citforum.netis.ru/nets/wireless/seti_efir**

Модем

А теперь опишем подключение аналогового модема к маршрутизатору с целью получения выхода в Интернет через коммутируемое соединение без компьютера-посредника.

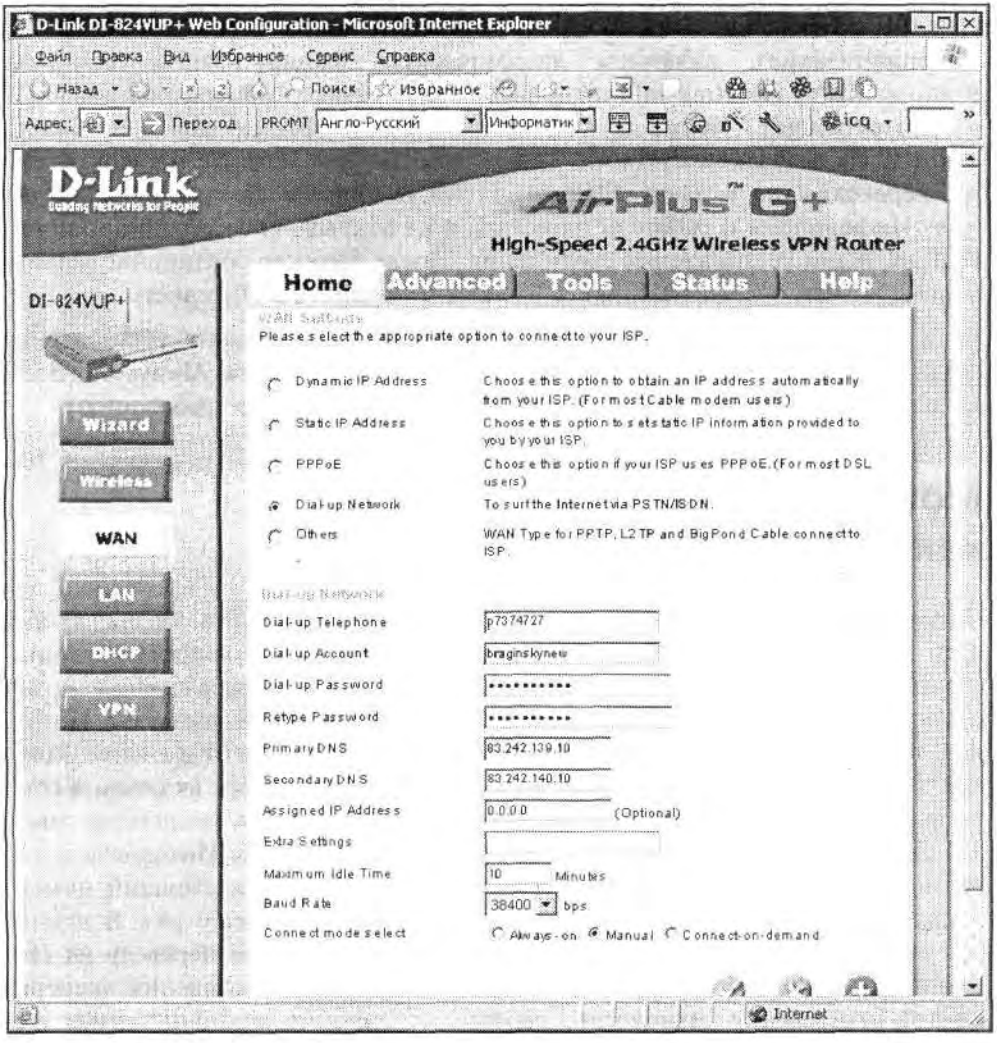


Рис. 13.12. Окно конфигурации маршрутизатора DI-824VUP+. **WAN** (настройка параметров глобальной сети для модемного коммутируемого подключения)

На странице настройки **WAN** выбираем вариант **Dial-up Network** и заполняем поля известными данными.

Assigned IP Address и **Extra Settings** оставляем такими, как есть, **Baud Rate** (скорость порта в Бодах) ставим минимально доступной из списка — 38 400. Позднее можете попробовать увеличить это значение, но только после успешного подключения.

Перейдя на вкладку **Advansed** (Расширенные) и нажав кнопку меню **Routing** (Маршрутизация), включаем динамическую маршрутизацию (Dynamic Routing) RIPv1 (Routing Information Protocol, протокол обмена информацией о маршрутизации). Ниже на той же странице несколько полей для ввода данных. Их оставляем пустыми. Теперь подключаем модем к маршрутизатору, переходим на вкладку **Status** (Статус), выбираем кнопку меню **Device Info** (Информация о работе устройства), а на открывшейся странице кнопку **Dial-up**. Ждем установления соединения. После того как соединение установилось, можем открывать Internet Explorer и выходить в Интернет.

Если все нормально работает, то остается выбрать вариант установления связи. На вкладке **Home** меню **WAN** доступно три варианта. **Always-on** (Всегда включено), **Manual** (Вручную) и **Connect-on-demand** (По требованию).

Мобильный Web-сайт как средство общения

Организация доступа из Интернета к своему ноутбуку! Эта задача, скорее всего, не станет насущной необходимостью при решении вопросов администрирования локальной сети. Но в качестве сетевого развлечения может представлять интерес. Если вы пользователь услуги GPRS-доступа в Интернет, то доступ к вашему ноутбуку возможен в любой момент времени, когда вам это необходимо. Если в настоящий момент мой ноутбук включен в сеть, то вы можете посмотреть экспериментальную страничку, созданную мной для демонстрации. Для этого достаточно подключиться к Интернету и набрать в адресной строке **http://okobox.webhop.net**. Если в настоящий момент подключиться не удалось, попробуйте через пару часов еще раз. Я думаю, что эта страница станет доступной постоянно, когда я ее переведу на стационарный компьютер. Данная страница — база для проведения экспериментов и отработки технологий, поэтому содержание страницы может меняться периодически без определенной системы, но способ доступа к ней и ее адрес будут неизменны.

В чем же здесь изюминка? Дело в том, что большинство обычных пользователей ПК считают, что Web-сервер обязан находиться на настоящем серве-

ре. Создание своей страницы они считают делом достаточно сложным и серьезным. Использовать Web-сервер как средство общения вообще не приходит в голову.

Но в современных условиях, когда доступ к Интернету становится распространен, почти как телефон, можно подумать о создании средства общения со своими друзьями и/или сотрудниками, совмещенного со своим ноутбуком или персональным компьютером.

В чем особенности этого средства общения?

На каждом компьютере — участнике системы устанавливается простой Web-сервер. Windows XP Professional обладает для этого всем необходимым. С помощью сценариев можно создать гостевую книгу, записи в которой можно делать и удаленно, и локально. Рисунки, которые внедряются в HTML-страницу, можно редактировать любым графическим редактором или просто менять ссылки на заранее подготовленные рисунки. Введя функцию авторизации при входе на страницу, вы можете полностью оградить себя от непрошенных гостей, того самого спама, от которого многие пользователи электронной почты не могут найти реального спасения.

Что может помешать созданию такого канала общения в первую очередь?

В подавляющем большинстве случаев, подключаясь к Интернету, пользователь может получить только временный IP-адрес. Он может просуществовать на протяжении всей сессии подключения, а в отдельных случаях, когда длительность сессии очень велика, поменяться и во время сессии. При организации различных сервисов для общения пользователей Интернета используются серверы со статическими IP-адресами, доступные для всех. Форумы, почтовые ящики, серверы ICQ и другие средства общения расположены на серверах с известными всем адресами, что позволяет использовать их для свободного общения в Интернете.

Но есть ситуации, когда нам не требуется постоянный доступ к почтовому ящику или серверу ICQ. Мы заранее договариваемся о моменте встречи, и вся информация передается именно в эти моменты. Я думаю, что у вас были ситуации, когда электронная почта использовалась для доставки материалов во время телефонного разговора. Сервис ICQ позволяет обмениваться как файловой, так и текстовой, и даже видеоинформацией. Для применения описанных (и других подобных) сервисов необходимо на компьютере пользователя установить программу-клиент, которая будет связываться с соответствующим сервером в Интернете.

Наше средство общения не предполагает централизации. Войти на персональный Web-сервер можно только в присутствии пользователя (при установленном подключении к Интернету). Это аналогично визиту на квартиру

знакомого — визит возможен, когда знакомый дома, но в отличие от визита домой, не требуется совпадения географических координат хозяина и гостя.

Реализация идеи

Прежде всего следует обеспечить уверенный поиск вашего мобильного сервера. Мало того, что IP-адрес может быть динамическим, но и подключаться к Интернету вы можете из разных мест, используя различные технологии. В этих условиях не обойтись без услуг некоторого сервиса в Интернете и соответствующей программы-клиента на вашем компьютере. Один из таких сервисов находится по адресу **https://www.dyndns.org/about/home_solutions.html**.

Нас интересуют бесплатные сервисы Dinamic DNS и WebHop. Первый позволяет по заданному символьному имени и номеру порта гарантированно обнаружить ваш IP-адрес, когда на компьютере работает клиент этого сервиса. Второй позволяет организовать перенаправление (редирект) с одного символьного адреса на другой. В условиях, когда ваш провайдер ограничивает использование многих портов для доступа к вашему компьютеру из Интернета (Стрим Мту-Интел, например), приходится выбирать другие порты. При этом адрес вашего мобильного сервера может выглядеть как `<символьный адрес>.<имя домена>:NNNN`, где `NNNN` — номер используемого порта. Перенаправление позволяет использовать обычный символьный адрес, но с него автоматически направлять подключение на ваш сложный адрес с номером порта. Регистрация этих услуг бесплатна, требуется только реальный адрес электронной почты для получения сообщения о регистрации и возможности ее подтверждения. Если этого не сделать, регистрация будет аннулирована.

Установив программу-клиент, вы получите возможность сообщать сервису Dinamic DNS в любой момент времени свой реальный IP-адрес в Интернете, даже когда вы сами его не знаете.

Предупреждение

Для пользователей Интернета, подключенных к нему через локальные сети (домовые, районные, городские). Часто все пользователи такой сети имеют один реальный IP-адрес на всех. Настоящий IP-адрес может выделяться за дополнительную плату. Для получения возможности подключения к своему компьютеру из Интернета необходимо выполнение одного из двух условий. Либо вы получаете реальный IP-адрес (пусть даже динамический), либо просите администратора, если это не вы сами, перенаправлять на ваш локальный адрес пакеты по выбранному номеру порта.

Абсолютно без всяких проблем работа мобильного Web-сайта будет проходить при персональном подключении к Интернету одним из следующих способов:

- обычное модемное подключение (Dial-up);
- подключение по технологии Стрим;
- подключение по технологии ADSL;
- подключение через модем GPRS (сотовый телефон).

Если вы подключаетесь к Интернету через свою квартирную или другую сеть, то посмотрите рекомендации в примечании ранее. Порт для подключения можно выбрать любой из неиспользуемых в вашей системе и сети. Можно применять порты 9081—9099, которые используются крайне редко и почти наверняка свободны в вашей системе.

Как и квартиру, свой мобильный сайт каждый может оформить по своему вкусу и соответственно своим возможностям. Здесь мы приведем только настройки, необходимые для обеспечения работы мобильного сайта, а решение, чем он будет наполнен, оставим вам.

Локальные компоненты

Прежде всего, проверьте — все ли компоненты операционной системы, необходимые для работы сайта, установлены. В контрольный перечень этих компонентов входят составляющие Internet Information Services (IIS).

- Internet Information Services Snap-In
- World Wide Web Service
- SMTP Service
- File Transfer Protocol (FTP) Service

Internet Information Services Snap-In — это компонент системы, который устанавливает средства администратора сайта, World Wide Web Service — это сам сервис, позволяющий работать сайту, два последних компонента не обязательны. SMTP Service — позволяет настроить отправку электронной почты прямо с вашего компьютера, минуя внешние SMTP-серверы. File Transfer Protocol (FTP) Service — позволяет настроить обмен файлами с другими компьютерами сети и Интернета по FTP-протоколу. Настройку электронной почты и обмена файлами здесь рассматривать не будем. Эта задача для вас должна быть уже понятной. А с Web-сервисом разберемся подробнее.

После установки необходимых компонентов системы в корне диска C:\ появится каталог Inetpab, а внутри него каталог wwwroot. Этот каталог должен содержать файлы вашего сайта.

Откройте **Администрирование | Internet Information Services** (рис. 13.13).

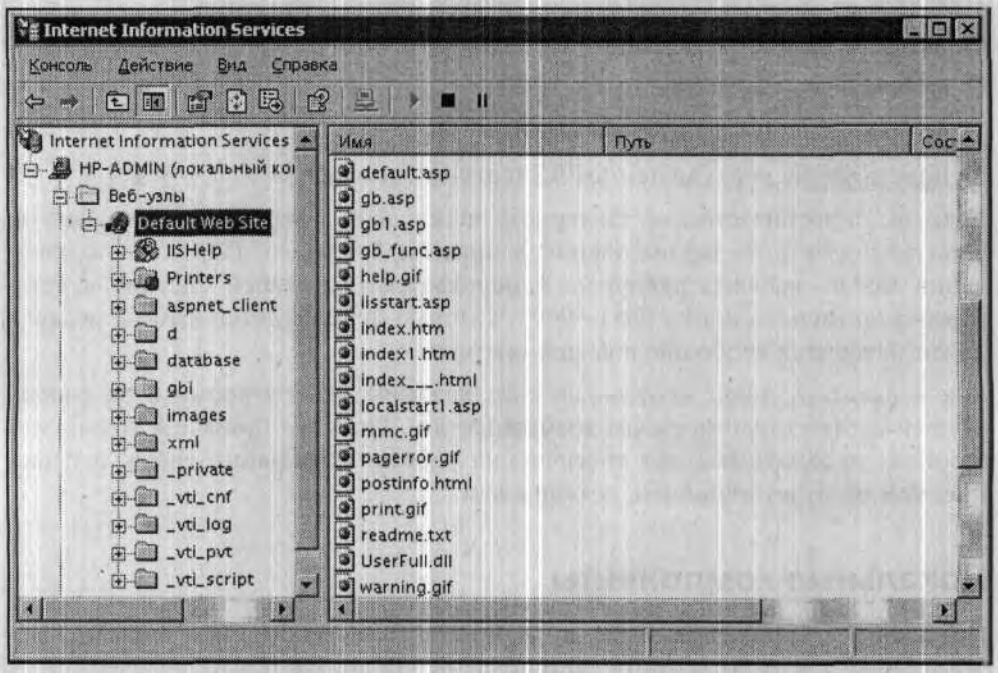


Рис. 13.13. Окно **Internet Information Services** с содержанием Web-узла по умолчанию

В дереве узлов в левой части окна разверните **Веб-узлы** и выделите **Default Web Site**. В правой части вы увидите все содержимое каталога wwwroot. Пользуясь контекстным меню при нажатии правой кнопки мыши, вы можете открыть любую страницу, подготовленную вами для сайта. Чтобы установить тип документа, который будет открываться по умолчанию при посещении сайта, необходимо открыть свойства **Default Web Site**, выбрав соответствующий пункт в контекстном меню правой кнопки мыши, и перейти на вкладку **Документы** (рис. 13.14).

Здесь вы можете установить необходимый формат документа по умолчанию. В большинстве случаев при создании сайта для основной страницы используют имя **Index.htm** или **Index.html**. Но вы можете задать любое имя и расширение для документа по умолчанию. Правда, если расширение документа не поддерживается браузером посетителя страницы, то он не сможет открыть этот документ.

На вкладке **Веб-узел** (рис. 13.15) вы можете установить значения порта, который будет использоваться для подключения к вашему сайту.

На вкладке **Безопасность каталога** вы можете оставить анонимный вход пользователей или установить режим обязательной аутентификации пользователей.

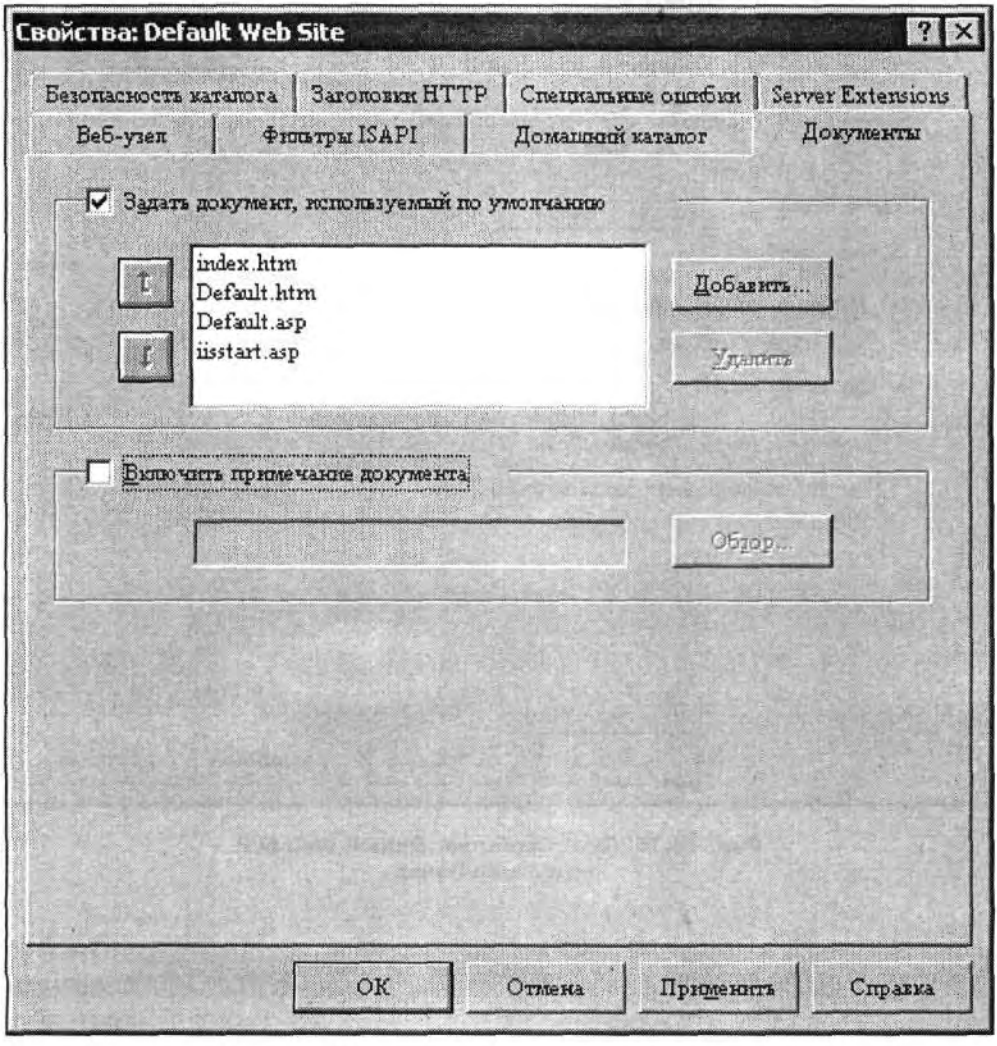


Рис. 13.14. Окно **Свойства: Default Web Site**, вкладка **Документы**

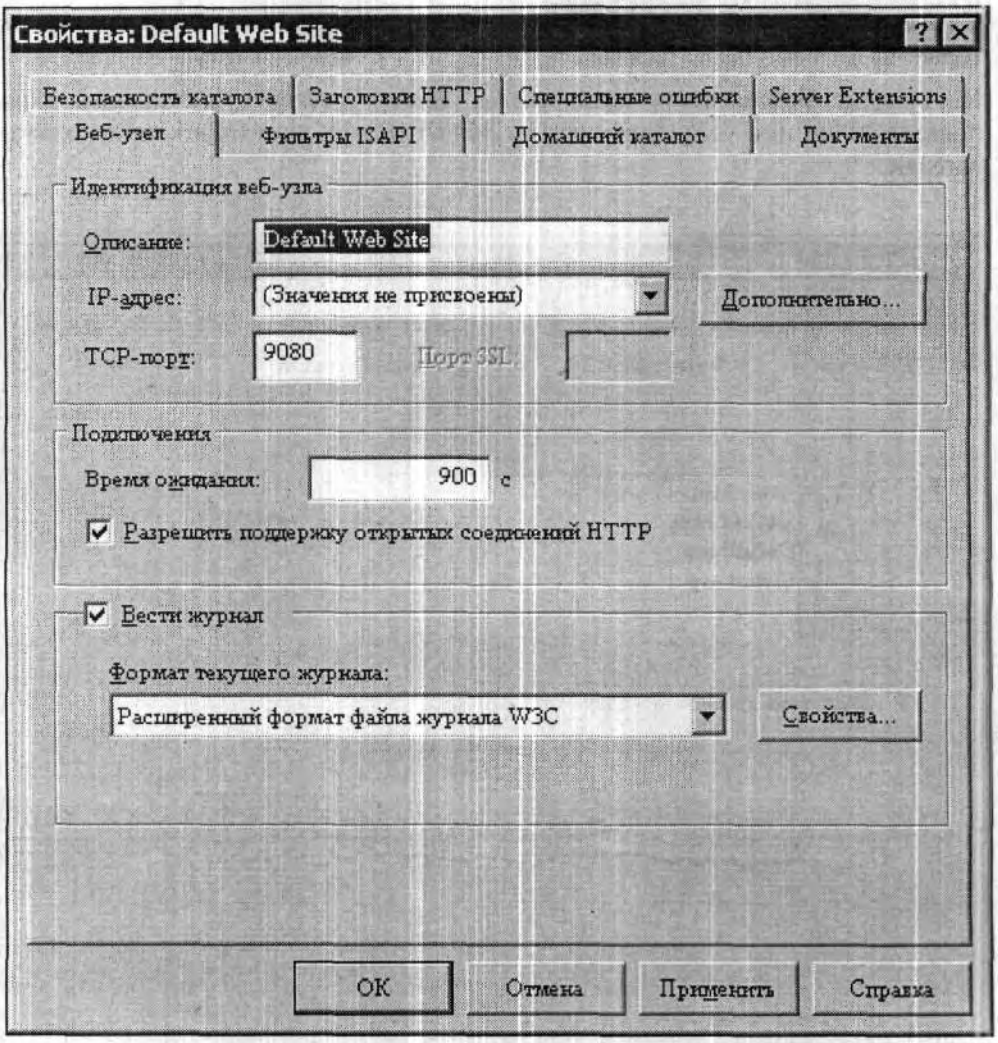


Рис. 13.15. Окно **Свойства: Default Web Site**, вкладка **Веб-узел**

Листинг 13.1. Код простой HTML-страницы

```
<html>
<head>
<title>Всем, всем, всем!</title>
</head>
```

```
<table border="1" width="100%">
  <tr>
    <td width="8%"> </td>
    <td width="85%">
      <p align="center"><span lang="ru"><font size="5"
       color="#0000FF">Моя первая страница</font></span></td>
    <td width="7%"> </td>
  </tr>
</table>
<p><span lang="ru"><font color="#0000FF">Эксперименты с мобильным
сайтом</font></span></p>
</html>
```

Внешний вид станицы из листинга 13.1 приведен на рис. 13.16.

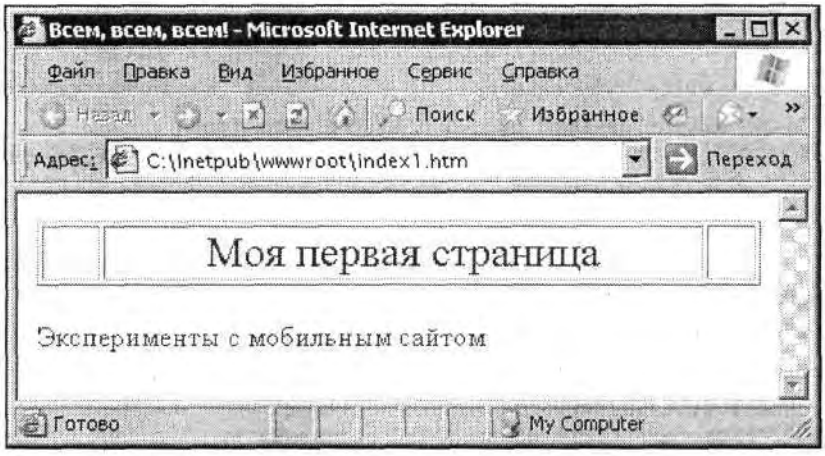


Рис. 13.16. Вид простой HTML-страницы

Довольно интересной может быть возможность подключения к странице документов в формате XML. Язык расширенной разметки используется уже достаточно широко. Правда, при разработке сайтов его применение несколько увеличивает трудоемкость этой работы. Но результаты могут быть очень интересными. Так, можно создать страницу, форма которой будет задана документом, находящимся на вашем компьютере, а содержание документа будет загружаться из документа, находящегося на одном из серверов в Интернете (например, вместе с вашей персональной бесплатной страницей).

XML-документы имеют строго организованную структуру, поэтому при определенных навыках программирования вы можете заставить сервер се-

ти или другой компьютер готовить их автоматически. Для отображения таких документов необходимо создать страницу, способную получать из них данные.

Создайте текстовый документ с именем xml3 и расширением html в соответствии с текстом листинга 13.2.

Листинг 13.2. Код документа xml3.xml

```
<HTML>
<head>
<title></title>
<script language="javascript">
<!--
var xmldoc = new ActiveXObject("msxml");
var xmlsrc = "http://localhost:9080/xml/journal2.xml";
function viewTitle(elem){  // Отображение заголовка документа,
                           // определяемого элементом <title>
this.document.writeln('<center><table width="100%" border=0><tr><td
width="100%" align="center" bgcolor="silver"><b><font
color="black">'+elem.text+'</font></b></td></tr></table></center><br>');
}
function viewContactsList(elem){ // Отображение содержимого
                                  // дочерних элементов <author-list>
this.document.writeln('<tr><td align="right" colspan="2"
bgcolor="gray"><b><font color="white">
Мои координаты</font></b></td></tr>');
this.document.writeln('<tr><td bgcolor="silver"
colspan="2"><center><table width="80%" border=0>');
 if(elem.type==0){
  if(elem.children!=null){
    this.document.writeln('<tr><td colspan=2 width="100%"> </td></tr>');
     var cur_item=elem.children.item("address");
     if(cur_item!=null){
      this.document.writeln('<tr><td><font
color="blue">Адрес</font></td><td align="right" ><b>
<font color="green">'+cur_item.text+'</font></b></td></tr>');
     }
     var cur_item=elem.children.item("tel",0);
     if(cur_item!=null){
```

```
      this.document.writeln('<tr><td><font
color="blue">Телефон</font></td><td align="right" ><b>
<font color="red">'+cur_item.text+'</font></b></td></tr>');
     }
     var cur_item=elem.children.item("email");
     if(cur_item!=null){
      this.document.writeln('<tr><td><font color="blue">E-
Mail</font></td><td align="right"><b><font
color="green">'+cur_item.text+'</font></b></td></tr>');
     }
     var cur_item=elem.children.item("url");
     if(cur_item!=null){
      this.document.writeln('<tr><td>
<font color="blue">URL</font></td><td align="right">
<b><font color="green">'+cur_item.text+'</font></b></td></tr>');
     }
    }
 }
this.document.writeln('<tr><td colspan=2 width="100%"> </td></tr>');
this.document.writeln('</table></center></td></tr>');
}
function viewMessages(elem){ // Отображение содержимого
                             // дочерних элементов <messages>
this.document.writeln('<tr><td align="right" colspan="2"
bgcolor="gray"><b><font color="white">Сообщения</font></b></td></tr>');
this.document.writeln('<tr><td bgcolor="silver"
colspan="2"><center><table width="80%" border=0>');
 if(elem.type==0){
  if(elem.children!=null){
   for(i=0;i<elem.children.length;i++){
    var cur_author = elem.children.item("author",i);
    this.document.writeln('<tr><td colspan=2 width="100%"> </td></tr>');
    if(cur_author.children!=null){
     var cur_item=cur_author.children.item("data");
     if(cur_item!=null){
      this.document.writeln('<tr><td>
<font color="blue">Дата</font></td><td align="right" ><b>
<font color="green">'+cur_item.text+'</font></b></td></tr>');
     }
```

```
    var cur_item=cur_author.children.item("heading");
    if(cur_item!=null){
     this.document.writeln('<tr><td><font
color="blue">Тема</font></td><td align="left" ><b><font
color="blue">'+cur_item.text+'</font></b></td></tr>');
    }
    var cur_item=cur_author.children.item("message");
    if(cur_item!=null){
     this.document.writeln('<tr><td><font
color="blue">Текст</font></td><td align="left"><b><font
color="black">'+cur_item.text+'</font></b></td></tr>');
    }
   }
  }
 }
this.document.writeln('</table></center></td></tr>');
}
function viewError(){
this.document.writeln('<center><hr>Error was detected');
}
function parse(root){
if(root==null) return;
 var i=0;
 var elem;
if(root.children!=null){     // Если вложенные элементы не были
          // определены, то свойство children будет установлено в null
this.document.writeln('<center><table width="80%" border=0><tr><td>');
             // Перебор дочерних элементов
 for(i=0;i<root.children.length;i++){
  elem=root.children.item(i);
  if(root.children.item(i).tagName=="TITLE"){
    viewTitle(elem);    // Разбор подэлементов <title>
  }
  if(elem.tagName=="CONTACTS"){
    viewContactsList(elem);      // Разбор подэлементов <contacts>
  }
  if(elem.tagName=="AUTHORS-LIST"){
    viewMessages(elem);       // Разбор подэлементов <messages>
  }
 }
```

```
this.document.writeln('</td></tr></table>');
  }
}
function viewDocument(){
xmldoc.URL = xmlsrc;      // Загрузка XML-документа
this.document.writeln('<body bgcolor="white">');
parse(xmldoc.root);       // Начало разбора документа
this.document.writeln('</body>');
}
// Генерирование страницы
viewDocument();
//-->
</script>
</head>
```

Созданная страница требует документа с данными. Сформируем такой документ. Это тоже текстовый документ, назовем его jurnal2.xml. Текст документа приведен в листинге 13.3.

Листинг 13.3. Документ с данными jurnal2.xml

```
<?xml version="1.0" encoding="windows-1251" ?>

<journal>
<language>ru</language>
<title>Информация</title>
<contacts>
<address>Зеленоград</address>
<tel>при необходимости сообщу</tel>
<email>braginsky@email.ru</email>
<url>http://okobox.webhop.net</url>
</contacts>

<issues-list>
<issue index="2">
<articles>
<article ID="3">
<article-finished/>
    </article>
```

```
<article ID="4">
<title/>
<url/>

<hotkeys/>
            </article>
         </articles>
      </issue>
   </issues-list>
<authors-list>

<author ID="1">
<data>21.06.2005</data>
<heading>Проба технологии XML
</heading>
<message>
Сегодня попробовал XML на сайте своего
 персонального компьютера. Вы видите результат.
</message>
      </author>

<author ID="2">
<data>24.06.2005</data>
<heading>Проба технологии XML</heading>
<message>
Заработало получение данных с локального компьютера
</message>
      </author>

<author ID="3">
<data>-------</data>
<heading>-----------</heading>
<message>---------</message>
      </author>

   </authors-list>
</journal>
```

Поместите документ xml3.xml в каталог C:\inetpab\wwwroot\, а документ jurnal2.xml в каталог C:\inetpab\wwwroot\xml\.

Не забудьте изменить номер порта в седьмой строке `xml3.xml` на тот, что применили вы. Теперь наберите в строке адреса Internet Explorer **http://localhost:9080/xml3.htm**, заменив номер порта на свой. Вы увидите страницу, изображенную на рис. 13.17.

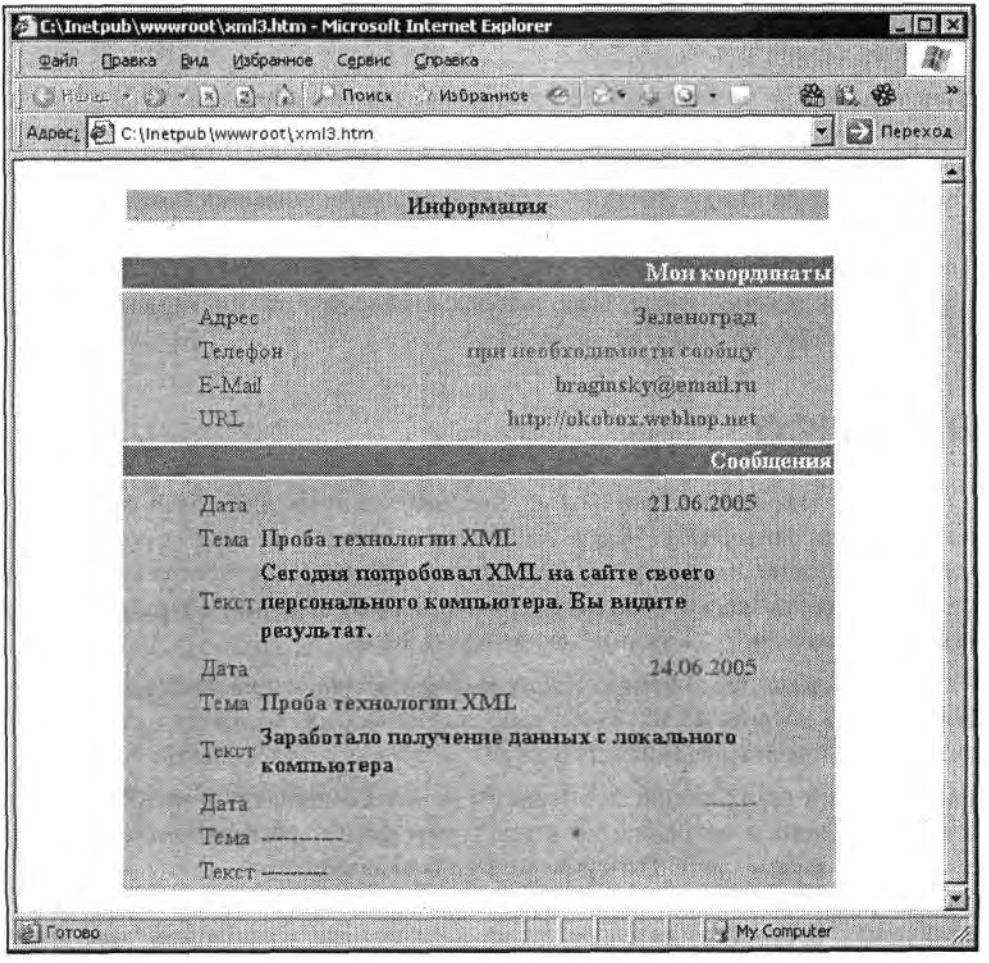


Рис. 13.17. Изображение страницы, использующей данные из XML-документа

Если ссылку на документ xml.htm поместить на основной странице сайта с соответствующей подписью, то каждый посетитель сайта сможет увидеть эту информацию.

Документ с данными (jurnal2.xml) имеет достаточно простую структуру, и его легко редактировать вручную, добавляя новые сообщения или редактируя старые. Указав вместо локального адреса этого документа адрес вашего сайта в Интернете, вы получите возможность оперативно менять его текст во время связи с собеседником, который тоже имеет такой сайт. Мы получили средство общения, клиент и сервер которого находятся на компьютерах пользователей. Для получения обновленной информации в окне Internet Explorer понадобится только время от времени нажимать клавишу <F5>, обновляя страницу.

Конечно, есть и более удобные программы для общения в сети. Но творческий подход к предложенному способу общения может принести определенную пользу. Развивая свой мобильный сайт, вы можете поместить на него и гостевую книгу. Тогда этот способ общения окажется более удобным. Код для гостевой книги имеет довольно большой объем, и поместить его здесь не представляется возможным. Но если вам понравится гостевая книга с моего мобильного сайта **http://okobox.webhop.net**, то по вашему запросу поделюсь информацией о ее создании.

Лавры ICQ

Существует множество разработок, предназначенных для связи по локальной сети или Интернету. ICQ — наиболее известная из таких программ. Но всегда интересно попробовать самостоятельно написать программу — простое средство связи, которое не требовало бы регистрации, обладало именно теми возможностями, которые нас интересуют.

Как выяснилось, выполнение такой задачи доступно практически каждому. Посмотрите на рис. 13.18. Здесь изображена форма, созданная как HTML-страница и предназначенная для организации связи в локальной сети.

Работа с этой программой, написанной на языке сценариев, подобна работе с ICQ. Но записи сохраняются в текстовом файле, расположение которого вы можете задать сами. По сути, местонахождение этого файла определяет сервер системы связи. В данной версии программы у клиентов должен быть подключен в качестве сетевого диска каталог, где расположен этот файл. Форму можно запускать как по сети с компьютера-сервера, так и в локальном варианте. Локальный вариант работает несколько быстрее.

Код серверной страницы (листинг 13.4) и клиентской отличаются только путями к текстовому файлу. В листинге 13.4 приведены оба варианта с комментариями.

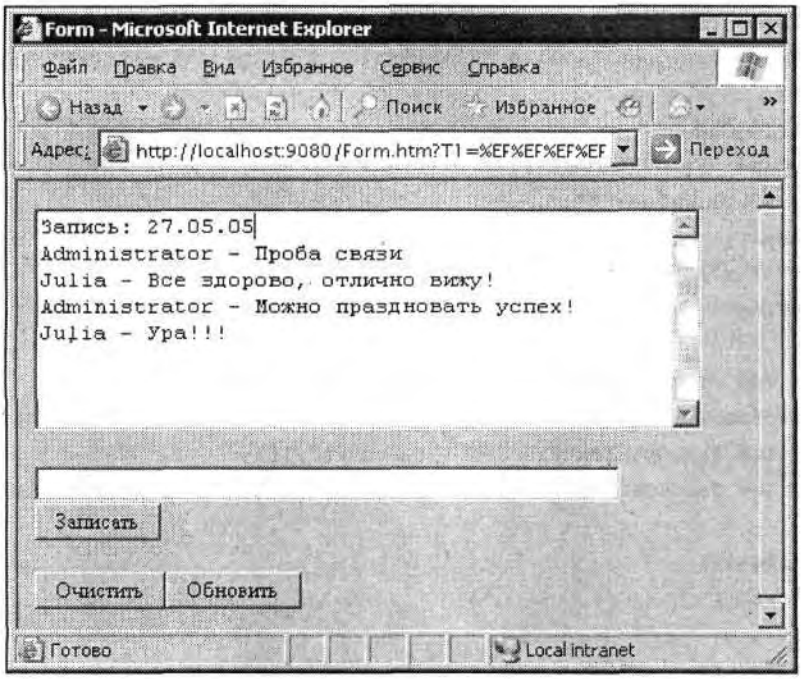


Рис. 13.18. Окно браузера с формой для связи по локальной сети

Листинг 13.4. Код HTML-страницы, предназначенной для сетевого общения

```
<html>
<head>
<title>Form</title>
<script language="JavaScript">
function first()
 {
var fso= new ActiveXObject("Scripting.FileSystemObject");
var Netwk = new ActiveXObject("WScript.Network");

var myString= Netwk.UserName + " - " +  document.F2.T1.value;
document.myForm.S1.value= document.myForm.S1.value + myString +"\r"+"\n"

// Далее три строки с вариантами подключения к текстовому файлу
var File= fso.OpenTextFile("C:\\Inetpub\\wwwroot\\test\\test.txt",1);
```

```
// var File= fso.OpenTextFile("W:\\test.txt",1);
// var File= fso.OpenTextFile("\\\\192.168.1.2\\test\\test.txt",1);

var myStringOld
myStringOld=  File.ReadAll();
document.F2.T1.value= "";
File.Close();
var s= ""+"\r"+"\n";
s+= myString;

// Далее три строки с вариантами подключения к текстовому файлу
var File= fso.OpenTextFile("C:\\Inetpub\\wwwroot\\test\\test.txt",1);
// var File= fso.OpenTextFile("W:\\test.txt",1);
// var File= fso.OpenTextFile("\\\\192.168.1.2\\test\\test.txt",1);

File1.Write(s);
File1.Close();

document.myForm.S1.value=  myStringOld +"\r"+"\n" + myString
}

function Second()
{
var fso= new ActiveXObject("Scripting.FileSystemObject");

File1= fso.OpenTextFile("C:\\Inetpub\\wwwroot\\test\\test.txt", 2);
// Далее три строки с вариантами подключения к текстовому файлу
var File1= fso.OpenTextFile("C:\\Inetpub\\wwwroot\\test\\test.txt",2);
// var File1= fso.OpenTextFile("W:\\test.txt",2);
// var File1= fso.OpenTextFile("\\\\192.168.1.2\\test\\test.txt",2);

File1.Write("Запись: " + document.F2.T1.value );
document.F2.T1.value= "";
document.myForm.S1.value= "";
File1.Close();
}
function Third()
{
var fso= new ActiveXObject("Scripting.FileSystemObject");
```

```
// Далее три строки с вариантами подключения к текстовому файлу
var File= fso.OpenTextFile("C:\\Inetpub\\wwwroot\\test\\test.txt",1);
// var File= fso.OpenTextFile("W:\\test.txt",1);
// var File= fso.OpenTextFile("\\\\192.168.1.2\\test\\test.txt",1);

document.myForm.S1.value=   File1.ReadAll()  +"\r"+"\n";
File1.Close();
}

function Load()
{
var Netwk = new ActiveXObject("WScript.Network");
// Подключение сетевого диска. Замените IP-адрес и имя каталога
Netwk.MapNetworkDrive("W:", "\\\\192.168.1.2\\test", "true",
"Administrator", "OFFOFF");
// WshNetwork.RemoveNetworkDrive("W:", "true", "true");
}

// -->
</script>

</head>
<body bgcolor=lightblue onload=Load()>
<form name="myForm">
<textarea rows="8" name="S1" cols="47"></textarea> 
</form>

<form name="F2">
  <p><input type="text" name="T1" value="" size="63">
<input type="button" name="button1"
value="Записать" onClick="first()"></p>
</form>

<p><input type="button" name="button2" value="Очистить"
onClick="Second()"><input type="button"
name="button3" value="Обновить" onClick="Third()"></p>

</body>
</html>
```

Во время загрузки страницы автоматически подключается сетевой диск с текстовым файлом. Для получения текста ответов необходимо нажимать кнопку **Обновить**. При этом все содержание файла сообщений копируется в текстовое окно. Клиентский вариант страницы универсален. Сетевой диск можно подключить и на локальном компьютере.

Конечно, это лишь игрушка. Но она работает, и на ее основе можно создать много полезных дополнений к сетевым инструментам.

Чтобы уменьшить число ошибок при повторении этого примера, вы можете скопировать его код со страницы по адресу в Интернете **http://www.okobox.narod.ru/LavrICQ/PlayICQ.htm**.

Видеокамера в сети

Все быстрее движение прогресса, все стремительнее в обычную жизнь проникают новые технологии. Портативная видеокамера еще недавно могла радовать только состоятельного человека, а малогабаритные видеокамеры, подключаемые к компьютеру, входили в состав дорогих систем видеонаблюдения, устанавливаемых в организациях для обеспечения охраны или спецслужбами для получения важной информации. Конечно, космические аппараты тоже снабжались подобными приборами. Теперь Web-камера доступна практически каждому владельцу компьютера. Ассортимент этих устройств может удовлетворить запросы практически любого уровня, как по цене, так и по возможностям. Решив приобрести Web-камеру, мы заказали ее в интернет-магазине. Малогабаритная камера Genius Slim 320 стала нашим выбором благодаря доступности и приемлемой цене. "Зачем Web-камера в локальной сети?" — спросите вы.

Учитывая, что наша сеть имеет выход в Интернет, применение ей можно найти весьма разнообразное.

- Наблюдение за помещением серверной.
- Передача видео- и аудиоинформации, как по локальной сети для ее пользователей, так и через Интернет для посетителей вашего сайта.
- Организация виртуальных встреч с сотрудниками удаленных участков сети.
- Оперативное создание учебных материалов для пользователей компьютеров в вашей сети.

Перечень можно продолжать и далее, но мы ограничимся этим списком.

В стандартной поставке вместе с Web-камерой предлагается программное обеспечение, которое может быть применено, но в основном для ознакомления с возможностями этого устройства. Для настоящей работы с Web-

камерой лучше найти более удобные и полезные программы. Таких программ разработано уже довольно много, и нам приглянулись два интересных продукта.

Один из них — ConquerCam фирмы ConquerWare из Копенгагена. По адресу **http://www.theill.com/conquercam/** можно скачать полнофункциональную тридцатидневную версию программы. Программа не обновлялась с 2004 года, но, вероятно, это связано с продуманностью и законченностью данного продукта. С ConquerCam доступны следующие действия.

- Захват изображения с Web-камеры.
- Индикация изменений в изображении.
- Передача изображения на FTP-сервер или в Интернет прямо с вашего компьютера (режим работы в качестве Web-сервера).
- Наложение на изображение даты и любых дополнительных изображений по вашему желанию.

Практически все необходимые параметры легко настраиваются под потребности пользователя.

Второй продукт — Кодировщик Windows Media 9 Series, разработанный в Microsoft, свободно распространяемый. Его можно найти по адресу

http://www.microsoft.com/windows/windowsmedia/ru/9series/encoder/default.aspx.

Эта программа позволяет передавать не статические изображения, сменяемые с заданными интервалами, а настоящее видео, сопровождаемое звуком. Сигнал от Web-камеры и микрофона (или другого источника звуки) кодируется так, что видеоинформация может передаваться даже по медленным модемным каналам связи. При этом передача может быть как on-line, так и в виде предварительной записи в файл, который может быть помещен на Web-странице и просмотрен при ее посещении.

Освоение программ доступно любому пользователю ПК. Далее рассмотрим только возможные применения этих программ. Представив себе цели, вы всегда решите задачи, которые необходимы для достижения целей.

Интеллектуальные развлечения

Когда-то, до появления телевидения, существовал такой вид досуга, как домашний театр. К праздникам или семейным торжествам домашняя труппа готовила представление, для участия в котором приглашались соседи и знакомые. В день премьеры приглашались соседи, знакомые, родственники, и в случае удачного представления постановка становилась темой для обсуждения на продолжительное время. В определенной мере семейные театры соревновались между собой. Здоровая интеллектуальная конкуренция застав-

ляла думать, расширять кругозор, познавать, постигать основы риторики, знакомиться с литературой и историей.

Позднее появилось телевидение. Практически сразу стали говорить о том, что телевизор разобщает людей. В свободное время люди перестали стремиться к встречам и беседам. Им было достаточно включить вечером телевизор, ставший электронным окном в мир и собеседником. В наше время телевизор объединился с другой бытовой техникой, превратившись в домашний кинотеатр, восхищающий качеством изображения и звука, позволяющий просматривать не только телевизионные передачи и видеофильмы с кассет и дисков, но и Web-страницы.

Правда, Web-страницы можно смотреть и на обычном ПК (собственно, как и телепередачи и видеофильмы). То есть современная техника, становящаяся все более доступной, позволяет включать ее в компьютерные сети. Если есть возможность просматривать Web-страницы, то кто-то эти страницы делает. Обладатель обычного персонального компьютера в наше время в состоянии создать Web-страницу, сложность которой будет зависеть от фантазии создателя.

Любой современный персональный компьютер позволяет организовать Web-сервер. Если этот сервер включен в локальную сеть, то просматривать его страницы сможет любой пользователь этой сети.

Компьютерные сети уже давно стали средой общения единомышленников посредством электронной почты, чатов, различных программ мгновенной передачи сообщений. Многие пользователи компьютеров создают персональные страницы в Интернете, используя бесплатные или платные площадки для хостинга или размещая страницы на своих серверах, имеющих постоянное подключение к Интернету.

Таким образом, к настоящему моменту компьютерные сети становятся средой живого общения не только соседей и родственников, но единомышленников, которые могут находиться на расстоянии многих километров друг от друга.

Web-камера позволяет поднять уровень общения еще на один уровень выше. Прямая трансляция живого видео или записи, подготовленной в домашней студии, может стать предметом интереса и коллективного обсуждения многими пользователями сети.

Программы ConquerCam и Кодировщик Windows Media 9 Series могут стать отправной точкой в техническом обеспечении ваших домашних студий, позволяющих транслировать видеопрограммы в сеть.

Если в сети есть общедоступный сайт, то на нем можно помещать объявления о программе трансляций.

Если учесть, что трафик внутри локальной сети (в том числе в домовых, районных, городских) не тарифицируется или не оплачивается, то вы полу-

чаете возможность как транслировать, так и просматривать видеопрограммы достаточно высокого качества (чем выше качество, тем большего объема трафик требуется для передачи видеоинформации).

Каждый желающий может стать режиссером, оператором, сценаристом, актером, композитором, писателем при создании произведений для публикации в сети.

Технические подробности

Говорить о создании Web-сервера мы сейчас не будем. Об этом много сказано на страницах в Интернете и просто в справке Windows. Сейчас поговорим только о том, как включить в Web-страницу видеоинформацию, как настроить передачу этой информации в Интернет. С программой ConquerCam вы сможете разобраться самостоятельно. Да она и не позволяет передавать в Интернет динамическое изображение. Только статические картинки, хотя и обновляемые при нажатии кнопки **Обновить** в браузере Internet Explorer, доступны при использовании этой программы. Совсем другое дело — Кодировщик Windows Media 9 Series. С помощью этой бесплатной программы вы можете передавать на свою страницу в Интернете видеоинформацию в реальном масштабе времени. От момента реально происходящего события до его изображения на странице пройдет всего несколько секунд. Они необходимы программе для преобразования сигнала от Web-камеры в видеопоток, который может воспроизвести Windows Media Player. Желательно иметь Media Player версии 9 или 10.

Кодировщик Windows Media 9 Series позволяет не только организовать трансляцию видео с Web-камеры, но и записать видеосюжет предварительно в файл с расширением wmv. И этот файл также может быть воспроизведен на Web-странице.

В качестве начальных условий зададим адрес вашего Web-сервера в Интернете или в локальной сети, а также его существование.

Создание Web-страницы в данном случае удобно начинать в офисном приложении Microsoft FrontPage 2003. Страница может быть уже создана, тогда с помощью Microsoft FrontPage 2003 потребуется добавить несколько элементов, которые позволят получить видеоизображение на ней.

Рассмотрим последовательность действий, необходимых для создания Web-страницы с видеоизображением.

1. Откройте Microsoft FrontPage 2003.
2. На пустом белом поле страницы кликните правой кнопкой мыши и выберите **Свойства страницы**.
3. Задайте необходимый цвет фона, шрифта и другие параметры по желанию.

4. В главном меню программы выберите **Таблица | Вставить | Таблица**.
5. Вставьте таблицу из трех строк и трех столбцов, остальные параметры таблицы выберите по своему вкусу.
6. Выберите ячейку, в которой должно быть видеоизображение. В нашем примере используем ячейку 2×2. В своей странице можете выбрать и другую ячейку.
7. Кликните левой кнопкой мыши на выбранной ячейке.
8. В главном меню программы выберите **Вставка | Веб-компонент**, а в открывшейся форме **Дополнительные элементы | Элемент ActiveX**.
9. Нажмите кнопку **Далее**.
10. В открывшемся списке найдите **Windows Media Player** и нажмите кнопку **Готово**. Ячейка увеличится до размеров окна Windows Media Player, имеющего в данном случае минимальный размер.
11. Теперь кликните правой кнопкой на вставленном элементе (он занимает всю ячейку) и выберите **Свойства элемента управления ActiveX**.
12. В открывшемся окне на вкладке **Общие** необходимо указать имя файла или адрес вашего сервера, передающего видеоизображение, а также порт, используемый для этого (в примере используется порт 3333). Адрес сервера может не совпадать с адресом сервера, на котором размещена сама страница. Можно указать адрес **http://Localhost:3333**, если вы хотите проверить работу страницы на локальном компьютере.

Примечание

Если предполагается, что страница будет помещена на сервер, где будет находиться и Кодировщик Windows Media 9 Series, то следует учесть, что на одном компьютере будут работать два сервера. Один основной (для отображения страниц сервера), его адрес и порт будут указываться в адресной строке браузера. Другой сервер дополнительный (для трансляции видеопотока). Его адрес должен быть указан в свойствах элемента ActiveX. На моем домашнем сервере это выглядит так: адрес в строке браузера **http://192.168.1.50:9080/proba_video.htm**, а в свойствах элемента ActiveX — **http://192.168.1.50:3333**.

Остальные параметры можно устанавливать по своему желанию.

13. Сохраните страницу, как Proba_video.htm в каталог Web-сервера.
14. Проверьте, что при открытии на странице виден Windows Media Player в виде небольшой панели управления и черного экрана. Закройте пока страницу.

Теперь запустите программу Кодировщик Windows Media 9 Series (надеюсь, что вы уже скачали ее, и увидели, что она имеет русский интерфейс). Само собой разумеется, что Web-камера у вас уже есть, драйверы установлены, камера подключена к компьютеру.

Здесь потребуется выполнить следующие действия:

1. Нажмите кнопку **Новый сеанс**.
2. В открывшемся окне **Новый сеанс** на вкладке **Мастера** выберите значок **Живая трансляция** и кликните по нему дважды левой кнопкой мыши.
3. Появится окно с возможностью выбора устройств, применяемых в сеансе. Должно быть видно наименование типа Web-камеры в поле **Видео**, а в поле **Звук** — звуковое устройство по умолчанию. Если вы устанавливали настройки аудиопараметров компьютера самостоятельно, то, возможно, придется и здесь самостоятельно выбрать необходимое значение из выпадающего списка.
4. Нажимите кнопку **Далее**.
5. В следующем окне мастера нового сеанса следует выбрать опцию **Получать от кодировщика**. Это значит, что ваша страница будет сама подключаться к кодировщику.
6. На следующем экране указываем выбранный порт (3333). Если у вас есть сомнения в том, что на вашем компьютере этот порт свободен, можно воспользоваться кнопкой **Найти свободный порт**. В этом случае потребуется смена значения порта и в свойствах элемента ActiveX на Web-странице.
7. На следующем экране выберите необходимую скорость в соответствующем поле. Выбор зависит от канала связи вашего сервера с Интернетом и канала применяемого пользователями Интернета, которые должны посещать вашу страницу. Для локальной сети можно выбирать более высокие значения, а для просмотра видео через модемное подключение лучше выбрать минимальную скорость. Можно отметить два варианта сразу, у пользователя скорость будет выбрана автоматически.
8. Если на следующем экране отметить **Сохранить копию потока вещания** и указать файл, в который поток будет сохранен, во время прямой трансляции будет создана копия сеанса в виде файла, который вы сможете воспроизводить по запросу пользователей. Это требует дополнительных настроек, но в них после установки прямого вещания вы сможете разобраться самостоятельно.
9. Далее будет предложено выбрать файлы для вступления, антракта и финала или производить кодирование только с выбранных устройств. Позднее вы можете поэкспериментировать с заранее записанными файлами, которые можно использовать для передачи информации в начале видеосеанса, во время перерыва или в конце его. Для простоты выбираем кодирование только с выбранных устройств и нажимаем **Далее**.
10. На следующем экране можно по желанию ввести информацию о заголовке, авторе и т. п. Снова нажимаем **Далее**, а затем — **Готово**.

Все. При подключенной камере вы увидите два окна. Окно **Ввод** содержит изображение, передаваемое камерой. Нажав кнопку **Запуск кодирования**, вы получите изображение и в окне **Вывод**. Это значит, что передача началась. Запускаем пробную Web-страницу, ожидаем несколько секунд и видим изображение, передаваемое камерой (рис. 13.19).



Рис. 13.19. Окно браузера с только что созданной страницей

Теперь, поэкспериментировав с камерой и программами, чтобы добиться желаемого вами результата, вы можете поместить страницу на доступный другим пользователям сервер, настроив его соответственно на получение изображения с сервера, где установлен Кодировщик Windows Media 9 Series.

Еще немного усилий, и вы сможете организовать телестудию в вашей сети!

В примере мы не рассматривали организацию звукового сопровождения "телепередач". Но в этом направлении никаких трудностей не встречается. Следует лишь учесть, что не обязательно использовать один микрофон. Можно через микшер подключить и несколько микрофонов, и другие источники звука.



Приложение

Справочные сведения

Работая в локальной сети, выходя в Интернет, настраивая маршрутизацию и другие сервисы сети, вы постоянно будете сталкиваться 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 DHCP-, WINS- и DNS-серверов помогает организовать адреса сети и привязать их к понятным именам. Но сами IP-адреса не могут быть произвольно назначены компьютерам или другим устройствам, работающим в сети. Для уверенного ориентирования 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 этим свойством будет намного легче, если вникнуть в его 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

TCP/IP-протоколы 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 рассылает 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, и каждому классу 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 указания адреса сети, на остальных местах должен располагаться адрес компьютера. Приведены также применяемые диапазоны адресов для каждого класса и зарезервированные для особых случаев адреса, не применяемые в Интернете.

Структура адреса становится более понятной, если адрес записать в двоичном коде. Например, маска 255.255.255.0 в двоичном коде выглядит так: 11111111.11111111.11111111.0. Все места, 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 "C", и адрес компьютера выражен единицей. Чем выше класс сети, тем больше адресов сети может существовать, и тем меньше компьютеров может находиться в такой сети. Каждый компьютер в сети имеет свой уникальный адрес, назначенный администратором или полученный автоматически. Именно такие адреса понимает 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. 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 254 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

Таблица П2 *(продолжение)*

Маска подсети 255.255.255.248 /29 (11111111.11111111.11111111.11111000)			
32 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
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
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

Таблица П2 *(окончание)*

Маска подсети 255.255.255.252 /30 (11111111.11111111.11111111.11111100)			
64 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
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
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

Связь между расширением маски подсети, двоичной записью маски и побайтовой записью для 32-разрядных адресов показана в табл. П3. 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-во	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
/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

Таблица П3 *(окончание)*

Расш.	Маска подсети в двоичном представлении	Побайтовое представление	Кол-во	Класс
/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 к десятичному виду (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 русскоязычных и англоязычных наименований объектов системы

В зависимости от версии ОС, установленных пакетов обновлений, вариантов русификации, а также от некоторых других причин имена объектов и названия окон и меню могут встречаться и на русском, и на английском языке. В табл. П4 приведен список соответствий некоторых русских и английских наименований, которые могут быть приведены в окнах и меню по-английски, несмотря на то, что ОС русифицирована.

Таблица П4. *Некоторые английские наименования*

Английское наименование	Русское наименование
Action	Действие
Active Directory	Служба каталогов

Таблица П4 *(окончание)*

Английское наименование	Русское наименование
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 никогда не имеют русского имени, а другие наименования не всегда являются точным переводом английского варианта.

Таблица П5. *Английские и русские наименования служб*

	Английское наименование	Русское наименование
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

***Таблица П5** (продолжение)*

	Английское наименование	Русское наименование
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
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

Таблица П5 *(продолжение)*

	Английское наименование	**Русское наименование**
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 медиаустройства
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)
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

Таблица П5 *(продолжение)*

	Английское наименование	**Русское наименование**
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)

***Таблица П5** (окончание)*

	Английское наименование	Русское наименование
71	Windows Installer	Windows Installer
72	Windows Management Instrumentation	Инструментарий управления Windows
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 описывается в окне **Службы** и тоже может быть на английском. Если это так, 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), который достаточно часто применяется 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 достаточно, 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, можно воспользоваться и портами из приведенного списка, если нет программ, которые их занимают. 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.

Аббревиатуры, сокращения и определения

Литература о компьютерных сетях изобилует терминами и сокращениями, которые не всегда понятны начинающим пользователям ПК и начинающим системным администраторам. Часть таких терминов и сокращений описана далее.

Беспроводная сеть

Это сеть, построенная на основе беспроводных сетевых адаптеров и концентраторов. Среди множества изделий различных фирм обращают на себя

внимание концентраторы фирмы Intel. Intel PRO/Wireless 2011 LAN Access Point — точка доступа для связи удаленного компьютера с локальной сетью — может применяться и как повторитель (repeater) для увеличения максимального расстояния при подключении. Intel PRO/Wireless 2011 LAN PC Card — беспроводный сетевой адаптер для компьютеров.

Строить сеть полностью на основе таких устройств нерационально. В отдельных случаях они позволяют обеспечить доступ пользователям, не имеющим возможности подключиться к сети с помощью кабеля.

Витая пара

Кабели на основе витой пары находят широкое применение в сетях передачи данных. Для кабеля на основе витых пар используются медные проводники диаметром 0,64—0,51 мм. В качестве материала изоляции обычно применяются полиэтилен, полипропилен, тефлон, вспененный полиэтилен. Неэкранированная витая пара представляет собой от 1 до 100 пар медных изолированных проводников, скрученных парами с согласованными шагами для уменьшения взаимного влияния. Наиболее распространены двух- и четырехпарные конструкции. Цветовая комбинация проводников фиксирована: один из проводников в паре имеет белый цвет с метками цвета второго одноцветного проводника этой пары — синего, оранжевого, зеленого или коричневого. Конструктивно все кабели делятся на экранированные и неэкранированные. Экранированные конструкции более защищены от помех и имеют лучшие показатели переходного затухания, но их применение требует специальных разъемов и правильной схемы заземления, поэтому в нашей стране большее распространение получили неэкранированные кабели. Наиболее распространен серый цвет кабеля, однако производятся кабели всех цветов, как правило, пастельных тонов. В случае наружной прокладки используется светостойкий полиэтилен (черного цвета). Все кабели маркируются по оболочке примерно следующим образом: фирма-производитель — марка изделия — тип изделия (4×2×0,52 — четырехпарный кабель с диаметром проводника), далее кодируются дата производства (1002 — октябрь 2002) и отметка метровой длины (иногда футы). Кроме того, на кабеле могут быть указаны материал оболочки, система сертификации и т. д.

Драйвер (driver)

Небольшая компьютерная программа для работы с конкретным периферийным устройством, таким как, например, сетевая плата или принтер.

Интерфейс

См. Interface.

Коаксиальный кабель

Представляет собой два соосных гибких металлических цилиндра, разделенных диэлектриком. Название произошло от латинских: **co** — совместно и **axis** — ось. Применяется для передачи высокочастотных сигналов. Для организации компьютерных сетей используется ограниченно. Кабель на основе витой пары вытесняет коаксиальный кабель в области сетестроения, ввиду большего удобства применения. В отдельных случаях может быть оправдано использование толстого коаксиального кабеля для связи удаленных на расстояние 180 м и более участков сети.

Коммутатор (switch)

Как и концентратор, позволяет объединить несколько компьютеров, подключив их к одному серверу. В отличие от устаревших теперь концентраторов (hub), коммутатор позволяет пересылать пакеты между несколькими сегментами сети, не загружая остальную сеть. Он является обучающимся устройством. Коммутатор анализирует адрес назначения в заголовке пакета и, сверившись с адресной таблицей, тут же (время задержки около 30—40 мкс) направляет этот пакет в соответствующий порт. Таким образом, его заголовок уже передается через выходной порт, хотя пакет еще целиком не прошел через входной.

Компьютерная сеть

Компьютерная сеть — это компьютеры, соединенные между собой средствами передачи информации. Эти средства достаточно разнообразны и применяются для решения возникающих на практике проблем. Их, тем не менее, можно разделить на программные средства, сетевое оборудование и кабельные системы.

В простейшем случае все компьютеры подсоединяются к одному и тому же коаксиальному кабелю и, тем самым, оказываются соединенными друг с другом. Но чаще используется более совершенная технология, в которой все компьютеры подсоединяются к специальному устройству, называемому концентратором, а для подключения применяется витая пара. В этом случае на каждом рабочем месте оборудуются розетки для подключения компьютера, а в центре, где будет установлен концентратор, — коммутационная па-

нель. Эта же самая кабельная система может использоваться для подключения телефонов к офисной АТС. Расстояние от концентратора до рабочего места ограничено. Оно не может быть больше 100 м. Если есть необходимость подключить к сети достаточно удаленные рабочие места, то используется оптоволоконный кабель. Такой кабель позволяет подключить рабочее место, удаленное на 2000 м. Но стоимость подобного соединения существенно выше. Различные модификации концентраторов обеспечивают обычно объединение от 4 до 24 компьютеров. Если на ваших компьютерах установлена операционная система Windows, то все необходимые программные средства для одноранговой сети у вас уже есть и их необходимо только задействовать, изменив конфигурацию операционной системы. Для более эффективной реализации работы в сети следует использовать специализированный компьютер — сервер, который применяется только для обеспечения работы в сети. Он отличается от обычных компьютеров тем, что при его проектировании предприняты специальные меры для повышения его надежности, расширяемости и безопасности. И это понятно, т. к. на нем чаще всего размещается жизненно важная для компании информация и от его работоспособности может зависеть работоспособность всей компании. На сервер устанавливаются специальные программные средства, которые в состоянии эффективно обслуживать многочисленные запросы, поступающие с остальных компьютеров сети.

Коннектор

Распространенное название электрических разъемов, применяемых для соединения кабельных коммуникаций с оборудованием. Для соединения компьютеров и сетевого оборудования кабелем "витая пара" обычно применяют коннекторы RJ-45.

Концентратор (хаб, Hub)

Устройство, которое "разветвляет" сеть на витой паре. Любая информация, пришедшая на один из его портов, через небольшое время отсылается через все остальные порты. Соответственно все порты хаба двунаправленные. Количество портов концентратора от 4 до 32.

Маршрутизатор (router)

Маршрутизатор распознает адрес получателя и перенаправляет по нему пакет. Для этих целей возможно применение отдельного компьютера с не-

сколькими сетевыми адаптерами. Маршрутизатор можно использовать для связи различных сетей. Внутри одной сети применяются коммутаторы.

Модем

Сокращение от "модуляция/демодуляция". Модем преобразует последовательные цифровые (двоичные) данные, поступающие от оконечного устройства, в форму, пригодную для передачи по аналоговой телефонной линии. Второй модем (на приемном конце) выполняет обратное преобразование аналогового сигнала в цифровые данные, принимаемые другим устройством (получателем).

Одноранговая сеть

Сеть, в которой нет выделенных серверов, а все компьютеры, подключенные к сети, делят между собой свои же ресурсы.

ОС (операционная система)

Встречается также жаргонный термин "Ось". Основной набор системного программного обеспечения, обеспечивающий работу компьютера и сети, предоставляющий часто и пользовательский интерфейс для взаимодействия пользователей с аппаратным и программным обеспечением. Существует множество ОС различного назначения, разработанных как отечественными, так и зарубежными компаниями и отдельными программистами.

Пакет

Информация в локальной сети передается блоками одинаковой длины — пакетами, в заголовках которых содержатся адреса отправителя и получателя. В IP-пакетах соответственно это IP-адреса, а в IPX-пакетах это Ethernet-адреса.

ПО (программное обеспечение, программы)

Обычно алгоритм в виде последовательности инструкций процессору. Для создания используются языки программирования. В большинстве случаев программы работают в среде операционных систем и предназначены для выполнения прикладных задач (вычислений), не связанных собственно с работой компьютера.

Порт

В широком смысле — место связи, точка подключения, "дверь" для входа на сервер или другое устройство. Существуют как физические порты (COM — последовательные, LPT — параллельные и другие), так и программные, определяющие диапазон памяти процессора, который используется для подключения. Например, интернет-соединения используют порты 80 (HTTP), 21 (FTP) и др. Применение того или иного номера порта обусловлено лишь стандартами и договоренностями, необходимыми для равномерного распределения нагрузки на память компьютера и позволяющими работать максимальному числу процессов в одно время.

Протокол

Правила и язык общения компьютеров сети между собой. Наиболее популярные протоколы: NetBEUI (расширенный NetBIOS), IPX/SPX, TCP/IP. NetBEUI — устаревающий протокол, пригодный для маленькой сети, которая состоит из одного сегмента.

IPX/SPX — протокол для NetWare, его поддерживают все версии NetWare. У него есть подробности в виде типа кадра Ethernet (тип фрейма). Для того чтобы компьютеры в одной IPX-сети видели друг друга, они все должны работать на одинаковом типе кадра.

TCP/IP — интернет-протокол, ему посвящены целые книги. Сложный протокол, в домашней сети его имеет смысл использовать при наличии систем UNIX, маршрутизатора и/или выхода в Интернет, а также при работе с приложениями, работающими с этим протоколом.

Разрешение имени в адрес

Действие, выполняемое DNS-сервером или другим сервером имен для определения соответствия сетевого имени IP-адресу объекта сети, имеющего это имя. Наиболее часто выполняется DNS-серверами в локальных сетях и в Интернете.

"Расшаренный диск"

Очень распространенное жаргонное выражение, ставшее обычным на Web-страницах пользователей и администраторов сетей и означающее диск общего доступа (Shared disk) или область на диске, открытые для доступа другим объектам сети. От английского *share* — разделять. "Шарить диски" — открывать диски для сетевого доступа, или подключать чужие диски, предоставленные для доступа.

Сегмент сети

Это часть сети, в которой все компьютеры "видят" друг друга напрямую. Любая сеть состоит как минимум из одного сегмента. Сеть, состоящая из нескольких сегментов, имеет в своем составе более сложное сетевое оборудование, как-то: маршрутизатор, мост, коммутатор.

Сервер

1. 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.
2. Главный компьютер, содержащий централизованные данные и управляющий получением этих данных другими компьютерами. Обычно такой компьютер всегда включен и за ним практически никто не работает, ему даже монитор не очень нужен. На сервере выполняется сетевая операционная система — как правило, это Novell NetWare 3.*x*, 4.*x*, 5.*x*, Windows NT/2000 Server, UNIX (Linux, FreeBSD) и др.
3. В технологии "клиент-сервер": главная программа, управляющая работой подчиненных программ-клиентов.

Сервер удаленного доступа

Программное средство, обеспечивающее доступ к компьютеру для пользователей, находящихся вне локальной сети.

Сетевая плата

См. сетевой адаптер.

Сетевой адаптер (сетевая карта/сетевая плата)

Устройство внутри компьютера (может быть встроенным в материнскую плату), позволяющее соединить этот компьютер с компьютерной сетью. Обычно применяются адаптеры для кабельных сетей, но могут применяться и беспроводные адаптеры. Выпускаются сетевые адаптеры многими производителями, среди них: 3com, Intel, DEC, AMD, Cabletron и др. Самая попу-

лярная сетевая карта — так называемая NE2000. Сетевые платы выпускаются в ISA-16 и PCI-вариантах, с разъемами BNC и/или UTP (TP), а иногда и с разъемом AUI. Каждая плата имеет уникальный адрес из 6 байт, например, 1E:34:00:00:FF:12, который называется ETHERNET-адрес или MAC-адрес. По этому адресу каждый сетевой адаптер однозначно идентифицируется сервером, что позволяет повысить безопасность сети.

Сетевой кабель

Коаксиальный кабель с волновым сопротивлением 50 Ом или кабель "витая пара". В настоящее время коаксиальный кабель применяется реже витой пары. Это связано с тем, что локальная сеть на основе витой пары имеет больше возможностей для расширения и модификации.

AD (Active Directory)

Термин Active Directory используется как для обозначения каталога с информацией о пользователях, компьютерах и других объектах сети, так и для обозначения службы каталога — комплекса программ, обеспечивающих доступ к этой информации. Active Directory поддерживает систему имен DNS, а имена в формате NetBIOS использует только для совместимости со старыми операционными системами. В Windows XP вообще прекращена поддержка NetBIOS (хотя и может быть еще установлена). При наличии множества связанных серверов Active Directory позволяет хранить свою базу данных в распределенном виде, и осуществлять автоматическую синхронизацию данных на всех серверах, входящих в домены Active Directory. Домены могут объединяться в деревья и леса. Часто применяется сокращенное обозначение — AD.

AUI (Access Unit Interface)

Интерфейс устройств доступа; интерфейс подключаемых устройств. N-контактный кабельный интерфейс штекерного типа, используемый в магистральных соединениях.

Auto-sensing 10/100 Mbps (автоматическое распознавание скорости передачи данных 10/100 Мбит/с)

Средство, позволяющее коммутаторам и концентраторам автоматически распознавать и настраивать скорость передачи данных по кабелю (называемое также *автосогласованием*). Интеллектуальные средства авторaспозна-

вания способны, кроме того, определять качество канала и автоматически выбирать максимальную скорость передачи.

BNS

Кабельный интерфейс для соединения коаксиального кабеля в магистральных сетях.

Bridge (мост)

Комбинация аппаратного и программного обеспечения, соединяющая две локальных сети и позволяющая осуществлять коммуникации между их станциями. Мосты функционируют на канальном (втором) уровне эталонной модели OSI (Open Systems Interconnection, модель взаимодействия открытых систем).

Bridge/Router (мост/маршрутизатор)

Устройство, функционирующее как мост, как маршрутизатор или как оба этих устройства одновременно.

Broadcast (широковещательная рассылка)

Передача сообщений всем адресатам сети.

Broadcast Domain (домен широковещательной рассылки)

Совокупность всех устройств, которые будут получать кадры широковещательной рассылки с любого устройства данной группы. Домены широковещательной рассылки, как правило, ограничиваются маршрутизаторами.

Broadcast Storm ("лавина" широковещательных пакетов)

Одновременная широковещательная рассылка пакетов несколькими отправителями, обычно поглощающая значительную часть доступной полосы пропускания сети и способная вызвать тайм-ауты.

DFS (Distributed File System)

Распределенная файловая система. Файлы в этой системе реально могут находиться в любом месте сети, но для пользователя они организованы в виртуальную структуру каталогов.

DHCP (Dynamic Host Configuration Protocol)

1. Протокол TCP/IP, автоматизирующий присвоение IP-адресов компьютерам (хостам), а также соответствующая служба. Для работы службы выделяются специальные серверы.
2. Служба динамического выделения сетевых адресов. Позволяет не загружать администратора сети проблемами распределения адресов, работает автоматически.

DNS (Domain Name System)

1. Служба имен Интернета, применяемая также в системах Microsoft Windows 2000 и Microsoft Windows 2003. Для работы службы выделяются специальные серверы.
2. Символьный идентификатор — имя, например, SERV.FIRMA.RU. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или Telnet.
3. Распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

DOS ODI и DOS NDIS

Сетевые драйверы, поддерживающие большинство ОС, в том числе Novell NetWare, Microsoft 9*x*, Microsoft Windows for Workgroups, Microsoft LAN Manager, Banyan VINES, Artisoft LANtasic, IBM LAN Server, HP LAN Manager и многие другие.

EFS (Encrypting File System)

Шифрующая файловая система, применяемая в современных операционных системах, которая позволяет прозрачно для пользователя шифровать файлы, используемые им. При этом для других пользователей эти файлы недоступны. Является надстройкой над файловой системой NTFS 5.0.

Ethernet

Самый распространенный стандарт компьютерных сетей. Имеет несколько модификаций и вариантов, которые совместимы друг с другом. Конкретные реализации обозначаются как 802.3 10Base-T — обычные локальные сети, 802.11b — радиосети, существуют и другие варианты.

Fast Ethernet

Широко распространенный протокол локальных вычислительных сетей, поддерживающий скорости передачи данных 10 и 100 Мбит/с.

FTP (File Transfer Protocol)

Протокол передачи данных в сети. Применяется для передачи файлов.

Gigabit Ethernet

Протокол передачи данных на скорости 1 Гбит/с и более (расширение спецификации IEEE 802.3 Ethernet). Протокол совместим с другими Ethernet-протоколами.

Hub

См. концентратор.

HTML

Язык гипертекстовой разметки. Средство создания страниц для публикации в Интернете и последующего просмотра с помощью браузера. HTML-страницы могут применяться и для обмена информацией в локальной сети, а также для хранения информации в виде HTML-файлов.

Interface

1. Способ и средство взаимодействия пользователя с программой.
2. Физическое устройство, соединяющее две системы или два устройства.
3. Стандарт (такой как RS-232-C), специфицирующий взаимодействие систем.

ISDN (Integrated Service Digital Network)

Международный стандарт передачи голоса, видеоинформации и данных по цифровым телефонным линиям.

LAN (Local Area Network)

Локальная компьютерная (вычислительная) сеть. Русское сокращение — ЛВС.

LINKLOCAL

Диапазон сетевых адресов, применяемых в локальных компьютерных сетях и не используемых в глобальных сетях.

MAC-адрес

Аппаратный адрес сетевого устройства. Не может повторяться, обеспечивает идентификацию сетевого устройства независимо от назначаемого адреса или имени.

MUI (Multilingual User Interface)

Многоязычный интерфейс пользователя. Установка MUI позволяет, имея нелокализованную версию ОС, получить интерфейс на национальном языке.

NetBEUI (NetBIOS Enhanced User Interface)

Сетевой протокол.

Это протокол, дополняющий спецификацию интерфейса NetBIOS, используемую сетевой операционной системой. NetBEUI формализует кадр транспортного уровня, не стандартизованный в NetBIOS. Он не соответствует какому-то конкретному уровню модели OSI, а охватывает транспортный уровень, сетевой уровень и подуровень LLC канального уровня. NetBEUI

взаимодействует напрямую с NDIS уровня MAC. Таким образом, это немаршрутизируемый протокол. Данный протокол понимает обычные буквенно-цифровые имена и отвечает за сеансы передачи данных между узлами сети, в нашем случае между компьютерами. Применяется только в локальных сетях, он упрощает работу с сетевыми адресами, позволяя использовать понятные имена компьютеров, которые могут быть связаны с именем пользователя или назначением компьютера в сети, что существенно облегчает навигацию в сети, поиск необходимого адреса и связь с ним. Новые версии операционных систем Windows прекратили поддержку протокола NetBEUI, но для временной совместимости со старыми компьютерами дистрибутивный диск Windows XP содержит этот протокол в качестве дополнения, которое можно установить.

Proxy Server (Proxy-сервер)

Это система, находящаяся между исполняемыми приложениями (такими как Internet Explorer) и соединением с Интернетом. Она перехватывает запросы к серверу, пытаясь выполнить их самостоятельно. Такой способ увеличивает быстродействие за счет отсечения повторных запросов одной и той же информации из Интернета. Proxy Server может кэшировать загружаемые из Интернета страницы (файлы). Если кто-то еще обращается к странице или файлу, ранее уже кем-либо запрошенным, Proxy Server выдает их из своего кэша. Это значительно быстрее, чем снова загружать страницу (файл) из Интернета. Proxy-серверы также могут выступать в качестве сетевого экрана, фильтруя IP-трафик по порту или IP-адресу.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Современный сетевой протокол.

TCP/IP-протоколы 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 рассылает по заранее определенному цифровому адресу в виде кадра информации — пакета, в который вложен пакет, созданный по TCP-протоколу. 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.

Telnet

Это один из старейших протоколов Интернета. Он появился в 1969 г. в ARPANET (сеть государственной организации The Advanced Research Projects Agency — бюро проектов передовых исследований. Теперь организация называется DARPA). Имя этого протокола является сокращением от названия telecommunications network protocol (сетевой коммуникационный протокол). Его описание находится в спецификации RFC 854. Этот протокол позволяет подсоединиться к удаленному компьютеру, находящемуся в сети, и работать с ним как будто бы вы работаете непосредственно на этом удаленном компьютере, т. е. в режиме терминала. Ваши возможности ограничены уровнем доступа, который задан для вас администратором удаленной системы.

В поставку Windows входит одноименная программа, которую вы можете запустить из меню **Пуск | Выполнить**.

Throughput (производительность, пропускная способность)

Общий объем корректно переданной (или обработанной) информации в заданный период времени. Выражается в битах в секунду или в пакетах в секунду.

UTP (неэкранированная витая пара)

Это самый популярный тип кабеля, используемый для соединения настольных систем и рабочих групп. *См. витая пара.*

Virtual LAN (VLAN, виртуальная локальная сеть)

Виртуальная локальная сеть (VLAN) состоит из связанной группы пользователей, которые могут осуществлять коммуникации непосредственно друг с другом и получать широковещательную информацию от других пользователей. При этом входящие в группу пользователи необязательно должны находиться в одном месте. В сетевой инфраструктуре, основанной на многопортовых коммутаторах и концентраторах, все рабочие станции могут взаимодействовать непосредственно друг с другом и получать друг от друга широковещательные пакеты. В такой сети виртуальные локальные сети (VLAN) применяются для управления трафиком, обеспечения защиты и для контроля широковещательной рассылки.

XML (Extensible Markup Language, расширенный язык разметки)

Язык стал стандартным с 1998 г. Напоминает язык разметки HTML, но применяется для структурированной записи больших объемов информации. В файлах XML могут сохраняться настройки оборудования, как у маршрутизатора D-Link 500T, например. Можно, один раз настроив одно устройство, передать файл для автоматизированной однотипной настройки большого числа этих устройств. Возможно и применение совместно с HTML-документами, для передачи на Web-страницы данных, которые будут отображаться, но храниться могут на другом сервере, где их можно оперативно обновлять.

WAN (Wide Area Network, территориально-распределенная сеть)

Сеть, охватывающая область, превышающую по размеру район или город.

WINS (Windows Internet Name Service)

Служба определения адресов, преобразующая имена компьютеров в сети (NetBIOS) в адреса IP.

Если вы используете NetBIOS поверх TCP/IP, необходимо запустить WINS для определения корректных IP-адресов.

10BASE2 (тонкий коаксиальный кабель)

Спецификация IEEE 802.3 сетей Ethernet на тонком коаксиальном кабеле.

10BASE5 (толстый коаксиальный кабель)

Спецификация IEEE 802.3 сетей Ethernet на толстом коаксиальном кабеле.

10BASE-FL (оптоволоконный кабель 10 Мбит/с)

Часть спецификации IEEE 10BASE-F, охватывающая сети Ethernet на оптоволоконном кабеле. Она совместима со спецификацией FOIRL (Fiber Optic Inter Repeater Link, волоконно-оптическая связь между повторителями (репитерами)).

100BASE-FX (оптоволоконный кабель 100 Мбит/с)

Реализация сети Ethernet на оптоволоконном кабеле, обеспечивающая скорость передачи данных 100 Мбит/с.

10BASE-T (витая пара 10 Мбит/с)

Спецификация IEEE 802.3 сетей Ethernet на неэкранированной витой паре (UTP).

100BASE-T (Fast Ethernet)

Технология 100 Мбит/с, основанная на методе доступа Ethernet/CD и использующая кабель "витая пара".

Вопросы и ответы

Вероятно, часть вопросов, которые приведены далее, совпадут с вашими; если нет, то пишите автору (гостевая книга на **www.okobox.narod.ru**).

Вопрос 1

Какие настройки сети и программы требуются для организации сети на двух компьютерах и выхода обоих в Интернет через один модем, установленный на первом компьютере?

Ответ

Windows, начиная с версии Windows 98 SE, позволяет осуществить это без применения дополнительного программного обеспечения. Необходимо установить для сетевого адаптера протоколы TCP/IP и NetBEUI. В параметрах протокола TCP/IP установить переключатель **IP-адрес получать автоматически**. На одном компьютере, том, на котором установлен модем, настроить соединение и общий доступ к подключению Интернета.

Вопрос 2

В моем офисе компьютер подключен к Интернету. Могу ли я использовать это подключение к Интернету из дома?

Ответ

При наличии второй телефонной линии можно установить два модема на офисный компьютер, контроллер удаленного доступа, адаптер виртуальной

частной сети. Адаптер виртуальной частной сети — это компонент Windows. Контроллеров удаленного доступа должно получиться два (по одному на модем).

После этих дополнений компьютер сможет одновременно использовать два модема. При недостатке внешних портов для подключения модемов один из них или оба могут быть внутренними.

Может случиться так, что после установки двух модемов вызываемый модем не будет отвечать на звонки. В этом случае необходимо в строку инициализации модема вписать: `ATS0=1`. Для этого надо открыть **Панель управления | Система | Устройства | Модемы | <Ваш модем> | Свойства | Дополнительно**.

Настройки сервера удаленного доступа остаются по умолчанию. IP-адрес назначается автоматически (192.168.55.2 на стороне клиента и 192.168.55.1 на стороне сервера), но на всякий случай установите пароль для доступа к серверу.

Следует иметь в виду, что скорость соединения будет существенно зависеть от качества связи с офисным компьютером. При отсутствии второй телефонной линии дешевле подключить к Интернету домашний компьютер.

Вопрос 3

Можно ли использовать программу Telnet для удаленного администрирования Windows 2000?

Ответ

Да, можно. Windows 2000 Professional, как и Windows 2000 Server, имеет встроенный Telnet-сервер. Если у вас под рукой Telnet-клиент, а у сервера есть постоянный IP-адрес, вы можете открыть окно командной строки на сервере откуда угодно, из любой точки земного шара. По умолчанию запуск Telnet-сервера отключен из-за очевидной угрозы безопасности. Чтобы запустить эту службу, воспользуйтесь командой `Net start telnet`.

Если нужно, чтобы сервер стартовал автоматически при запуске системы, следует установить режим запуска **Авто**, для этого необходимо открыть **Панель управления | Администрирование | Службы | Telnet**. После запуска сервера ваш компьютер готов обслуживать клиентские запросы к TCP-порту 23. По умолчанию сервер пытается аутентифицировать клиента по схеме NT LAN Manager (NTLM), что позволяет регистрироваться автоматически. Для удаленного доступа из-за пределов локальной сети это неудобно; чтобы сменить режим аутентификации, сначала нужно запустить утилиту администрирования сервера Telnet-командой `tlntadmn`.

В появившемся меню выберите пункт **Отобразить/изменить параметры реестра**, а в следующем меню — пункт **NTLM**. По умолчанию значение этого параметра реестра равно 2, что соответствует аутентификации средствами NTLM. Если изменить это значение на 1, сервер сначала попробует аутен-

тифицировать клиента по NTLM, а если не получится, запросит имя пользователя и пароль. Значение 0 отменяет попытку аутентификации клиента с помощью NTLM.

Теперь, когда процесс конфигурации сервера завершен, он доступен отовсюду, даже с компьютера под управлением UNIX. Стоит только набрать команду:

```
telnet <имя или IP – адрес сервера>
```

И все!

Примечание

Если установка Windows 2000 проводилась, как обновление Windows 98, то служба Telnet может функционировать неправильно. Надо также иметь в виду, что доступ к компьютеру может получить и злоумышленник (даже через Интернет, если компьютер подключен к нему), поскольку системы Windows не имеют средств ограничения доступа по данному протоколу.

Вопрос 4

Компьютер под управлением Windows XP не видит в сети рабочие станции с Windows 95 и DOS. Как это исправить?

Ответ

Протокол TCP/IP совершенствуется, и некоторые функции новых редакций этого протокола не поддерживаются старыми операционными системами. В сложившейся ситуации может помочь старый протокол NetBEUI. Достаточно установить на все компьютеры протокол NetBEUI (для Windows XP устанавливается отдельно с дистрибутивного диска). Применение только протокола TCP/IP не позволит компьютеру с Windows XP использовать файлы и принтеры рабочих станций DOS. Но рабочие станции DOS смогут использовать ресурсы компьютеров с Windows XP и Windows 2000.

Вопрос 5

До перехода с NetWare на Windows 2000 Server не возникало проблем при печати из прикладных программ на принтере, подключенном к рабочей станции DOS. Теперь эта печать идет чрезвычайно медленно. Что делать?

Ответ

Если нет возможности установить более новый компьютер или подключить принтер к серверу, увеличьте оперативную память одной из рабочих станций DOS до 8 Мбайт. Затем установите на нее Windows 95. Прикладные DOS-программы будут работать не хуже, а печать будет идти быстро с любых компьютеров.

Вопрос 6

Почему не виден принтер в сетевом окружении?

Ответ

Причин может быть несколько.

- ❒ Для принтера не установлен общий доступ.
- ❒ Общий доступ установлен, но пользователь, под именем которого вы вошли в сеть, не имеет прав доступа к принтеру.
- ❒ Принтер не поддерживает сетевое использование (встречается редко).
- ❒ Неправильно установлен принтер.
- ❒ При установке принтера использовался неподходящий драйвер.
- ❒ Не включен компьютер, к которому подключен принтер.
- ❒ Не исправен или не подсоединен сетевой кабель компьютера, к которому подключен принтер.

Вопрос 7

Почему не все компьютеры сети видны в сетевом окружении?

Ответ

Причин может быть несколько.

- ❒ Не все компьютеры включены.
- ❒ Не на всех компьютерах есть ресурсы с общим доступом.
- ❒ Не на всех компьютерах выполнен вход в сеть.
- ❒ Возможно, что следует подождать несколько минут, если компьютеры только что подключились к сети.
- ❒ Не все компьютеры используют одни и те же сетевые протоколы.
- ❒ Не у всех компьютеров исправен сетевой кабель.

Вопрос 8

Почему на некоторых компьютерах операции выполняются очень медленно?

Ответ

Причин может быть несколько.

- ❒ Возможно, применяется сетевой кабель слишком низкой категории, следует заменить кабель.
- ❒ Слишком длинный кабель от хаба до компьютера (более 100 м). Можно разрезать кабель в удобном для этого месте и установить в разрыв допол-

нительный хаб в качестве повторителя (усилителя) сигналов, передаваемых по сети.

- Если вы перешли с хабов 10 Мбит на коммутаторы 10/100 Мбит, а кабели оставили старые, настройте коммутаторы на работу с пониженной скоростью.
- Проверьте обжим сетевых разъемов и подключение кабелей к розеткам. Плохой контакт может вызвать нарушения в работе сети, и даже потерю данных (при работе с базами данных).
- Если дефект зависит от времени суток, возможно, что сервер работает с перегрузкой.

Вопрос 9

Не удается зарегистрироваться в сети, но имя пользователя и пароль верны.

Ответ

Причин может быть несколько.

- Потеряна связь с сервером (нарушения в кабельной системе).
- Включена клавиша <CapsLock>.
- Пароль изменен пользователем, имеющим права администратора.
- Если на сервере установлено более одной сетевой карты, то исключите протокол NetBEUI с проблемных компьютеров или отключите лишние сетевые адаптеры на сервере.

Вопрос 10

Почему после замены сетевой карты компьютер не входит в сеть и даже "зависает"?

Ответ

Следует после включения компьютера подождать несколько минут, а иногда около часа. Регистрационные данные компьютера на сервере привязаны к MAC-адресу сетевой платы, а он изменился. Вход в сеть может быть произведен, когда прекратятся попытки сервера найти в сети старую сетевую карту, зарегистрированную сервером вместе с именем компьютера.

Вопрос 11

Как проверить качество связи компьютера с сервером?

Ответ

Достаточно использовать команду `ping` из командной строки, введя в качестве параметра IP-адрес сервера. Если время ответа менее 10 мкс, то все

нормально. Если время ответа исчисляется десятками и сотнями микросекунд, да еще нестабильно, — ищите причины в неисправности кабельной системы или несоответствии параметров кабеля параметрам нового оборудования.

Вопрос 12

Проложены новые кабели и установлено новое сетевое оборудование, но качество связи очень низкое. Почему?

Ответ

Вполне возможно, что на одном или нескольких участков сетевой кабель проходит вблизи кабеля высокого напряжения. Необходимо проложить сетевой кабель не ближе 50 см от силового.

Вопрос 13

Почему при подключении сетевого кабеля в разъем сетевой платы не загораются ее индикаторы?

Ответ

Скорее всего, поврежден кабель. Но, возможно, что второй конец кабеля не вставлен в розетку.

Вопрос 14

Сетевой диск подключается при входе в систему, но если нет доступа к компьютеру, на котором расположены данные, пользователи машинально отключают возможность подключения диска при следующей загрузке. Как избежать этого?

Ответ

Очень просто, достаточно создать BAT-файл со следующим содержимым:

```
net use Буква_диска: \\Имя_компьютера\Имя_каталога
```

Поместите ярлык этого файла в папку Автозагрузка. При каждой загрузке компьютер будет пытаться установить соединение с сетевым ресурсом. Возможно и применение сценариев входа в сеть, если сеть не одноранговая.

Вопрос 15

Мне приходится часто подключать и отключать сетевые диски, можно ли упростить эту процедуру?

Ответ

Как и в предыдущем случае, создайте несколько BAT-файлов со строками, содержащими команды для подключений, и используйте их для подключения необходимого набора сетевых дисков.

Вопрос 16

Как упростить установку и модификацию приложений в сети?

Ответ

Проще всего на одном из компьютеров установить виртуальный CD-ROM. Программы такого назначения часто распространяются с новыми компьютерами, но можно их найти и в сети Интернет. Создайте несколько виртуальных дисков и скопируйте на них дистрибутивные диски. Настройте общий доступ к виртуальным дискам. Теперь, подключая такой диск в качестве сетевого на любой рабочей станции, вы можете устанавливать и модифицировать программное обеспечение на этих рабочих станциях. Причем подключаться к такому виртуальному диску можно с нескольких рабочих станций одновременно.

Вопрос 17

Компьютеры для нашей сети в целях экономии средств приобретаются без приводов CD-ROM. Существует ли возможность подключить компьютер к сети до установки Windows, для последующей установки операционной системы и программного обеспечения?

Ответ

Существует. Проще всего это реализуется на современных компьютерах с поддержкой различных режимов работы USB-портов из BIOS. Приобретите один Flash Drive. Сделайте его загрузочным и установите на него Microsoft Network Client version 3.0 for MS-DOS. Если вы приобретаете одинаковые сетевые адаптеры для всех компьютеров, то проблем не будет совсем, иначе вам потребуется дополнительно настраивать Microsoft Network Client version 3.0 for MS-DOS для работы с каждым компьютером.

Вопрос 18

До недавнего времени наша сеть работала без сбоев, в системных журналах все ошибки были объяснимы. Но теперь не реже одного раза в час на сервере, через который наша сеть имеет выход в Интернет, стала появляться ошибка, говорящая о том, что не удалось определить имя компьютера. При этом у пользователей сети проблем не возникает.

Ответ

Вероятнее всего, у вашего домена есть имя, совпадающее с именем другого домена, зарегистрированного в Интернете. Существуют три пути для решения этой проблемы.

1. Переименовать домен. Средствами операционной системы Windows 2000 Server это сделать невозможно. Придется переустановить AD, перерегистрировать компьютеры и пользователей сети. Имя домена в локальной сети лучше выбирать так, чтобы обеспечить наверняка отсутствие двойника в Интернете. Для этого выберите не существующую в Интернете зону, например ".dom" или ".loc".
2. Выход в Интернет осуществлять через компьютер (сервер), не входящий в ваш домен. Но в этом случае возможно появление других проблем. Одна из них — отдельная, не связанная с AD, авторизация пользователей на этом сервере (если необходимо).
3. Зарегистрировать имя своего нового домена в Интернете. При этом придется выполнить все процедуры, как и в п. 1. Имя домена в этом случае должно быть допустимым в Интернете.

Предметный указатель

8

802.11b 545, 546
802.11g 544, 545, 546, 549

A

Active Directory 73, 76, 79, 145, 200, 201, 202, 233, 329, 330, 331—337, 341, 342, 346, 348—352, 355, 360, 455, 461, 470, 478, 487
ADSL 148, 165, 167, 169, 264, 267, 280, 289, 290—297, 303, 327, 543, 549, 561

B

BBS 5
BIOS 617
Bridge 149, 165

C

Chkdsk 534

D

DFS 78
DHCP 50, 229, 234, 385, 386, 392, 500, 510, 518, 520, 536, 583, 592, 602, 605
DHCP-сервер 159, 302, 303, 307, 309—314, 318—321, 328, 385
Dial-up 241, 250
DNS 37, 39, 583, 592, 596, 601, 603, 605
dnsmgmt 316, 317
DNS-сервер 157, 159, 162, 168, 169, 268, 302, 303, 304, 312—318, 333, 367, 380, 381, 411, 412
DOS 107, 257, 492—499, 505, 509—512, 517, 518, 523, 524
Dynamic DNS 172, 175, 560

E

EFS 78
EIA 17
Ethernet 19, 20
ext3 74

F

Fast Esernet 21
FAT12 70
FAT16 70
FAT32 70, 74, 333
FIDO 5
Firewall/router 245
Flash Drive 617
Forwarding 245
FTP 595, 596, 601, 605, 606
FTP-клиент 505
FTP-сервер 505

H

HAB 42
HTA 480, 481, 486
HTTP 596, 601
HTTP-протокол 172

I

ICMP 187, 398, 401
ICQ 559, 572
IGMP 373, 375
IP-адрес 27, 37, 38, 39, 40, 45, 47, 48, 50, 53, 138, 139, 140, 141, 150, 157, 159, 167, 168, 172, 173, 175, 583, 605, 611, 612, 615
IP-фильтр 242 246
ISA 106, 107
ISDN 17
ISO 17

J

JScript 441—449, 453

L

Linux 55, 74, 75, 76, 77, 260
LMHOSTS 312, 321, 322
Log-файл 245

M

MAC 34, 608
MAC-адрес 392
Microsoft Network Client 499, 509, 511, 512, 517
MSBLAST 195

N

NAT 79, 170, 173, 200, 201, 262, 265, 269, 271, 293—297, 367, 371, 375, 377, 381, 401
NDIS 34, 608
NetBEUI 34, 146, 147, 607
NetBIOS 34
NetBIOS-имена 312, 318, 333
NNTP 596
NTFS 58, 70, 71, 74, 78, 333

O

OpenVPN 393—407, 412
OSI 17

P

PCI 106, 107, 111, 112
Ping 144, 145, 172, 180, 183, 187, 189, 228, 229
POP3 79, 596
POP3-сервер 302
PrimalScript 452, 453, 486

R

RADMIN 172, 175, 176, 241—252, 534, 535, 540
Rasdial 176
RJ-45 40, 41, 114, 123
Route 189, 190, 191, 192
Router 149
RS232 17

S

SMTP 79, 595, 596
SMTP-сервер 302
Splitter 165
Spyware 196
SuperScan 230
Switch 42

T

TCP 14
TCP/IP 20, 25, 39, 242, 243, 245, 583, 608
Telnet 242, 245, 423, 438, 439—441, 446, 448, 450, 451, 532— 536, 542, 594—596, 605, 609, 612
TFTP 596
Time 595, 596
Token Ring 23

U

UPS 112
USB 544—549, 552, 553, 617
UTP 109

V

VBScript 456
VMware Workstation 136
VNC 172
VPN 51, 151—154, 161, 393—399, 403—407, 544, 546, 596

W

Web 79
WebHop 172, 175, 560
Web-камера 576, 580
Web-сервер 302, 313, 314, 558, 559
Wi-Fi 545
Windows 2000 55, 56, 71, 77
Windows 2000 Server 198—202, 223, 231, 239, 253, 261
Windows 98 55, 60, 69, 70, 71, 73, 134, 145, 146, 189, 198
Windows Server 2000 231
Windows Server 2003 77—80, 83, 145, 146, 182
Windows XP 55—59, 63—80, 135—137, 141—147, 150, 151, 182, 190
WINS 39, 229, 234, 235, 501, 509, 510, 511, 520, 521, 583, 610
WINS-сервер 302, 318, 319, 322
Wireles 553—556

X

XML 75, 565, 571

А

Апплет 63, 65
Архивирование 427

Б

Беспроводная сеть 543
Беспроводный адаптер 544, 545
Брандмауэр 142, 144, 182, 184, 266, 367, 368, 375, 377, 401, 406

В

Виртуальная частная сеть 72
Виртуальный:
  адаптер 151
  компьютер 136
Вирус 195
Витая пара 18, 22, 23, 41, 123
Волоконно-оптический кабель 22
Время входа 352
Вызов по требованию 159

Д

Дистанционное управление рабочим столом 379

И

ИБП 415—420
Имена NetBios 39
Инернет-подключение к удаленному рабочему столу 357—359
Интернет 16, 25, 27, 35, 40—46, 51, 52, 103, 115, 118, 244

Интернет-сервер 367, 380, 402
Источник бесперебойного питания 42, 92, 111, 112, 118, 415

К

Категория 5 41
Клиент для сетей Microsoft 145
Коаксиальный кабель 18, 22
Коллизия 20
Коммутатор 21, 41, 42, 45, 48, 145
Концентратор 21, 42, 45

Л

Локальные политики домена 338

М

Маршрутизатор 41, 42, 47, 48, 149, 189, 190, 199, 245, 371, 375, 380, 385, 544, 546, 549, 550, 552
Маршрутизация 368, 369
Маршрутизация и удаленный доступ 369, 403
Маска 27, 584
Мастер настройки сервера 263, 268—272, 315
Мастер создания области 303—306
Метрика 191
МККТТ 17, 18
Модем 39, 44, 46, 48, 241, 243, 250, 557, 612
  ADSL 47
  DSL 41
  аналоговый 41, 544
Монтаж 114, 117
Мост 149, 165

Н

Нуль-модемный кабель 254

О

Одноранговая сеть 46
Основной шлюз 157

П

Параметры безопасности 153, 338
Перекрестный кабель 40, 41, 45, 89
Подключение к удаленному рабочему столу 324
Политика паролей 338
Политики учетных записей 338
Почтовый сервер 274, 276, 280
Принтер 46
Профиль служб терминалов 346, 348

Р

Резервирование 307
Резервное копирование 427
Роль сервера 331

С

Сервер 16, 36—39, 43, 46, 49—51, 260
Сервер терминалов 323, 328
Серверная 97
Сетевое подключение 137
Сетевой:
  адаптер 91
  фильтр 42, 91
Служба доступа к файлам и принтерам 145
Сохраненные запросы 341
Сплитер 165
Статическое сопоставление 322
Структурная схема 108
Сценарии входа 536

Т

Таблица маршрутизации 190
Техническое задание 115, 116
Трафик 529, 530, 532

У

Удаленное администрирование 612
Удаленный доступ к рабочему столу 326
Управление компьютером 414, 436, 438, 439, 455
Учетные записи 337, 340, 341, 344, 347, 348, 352, 354

Ф

Файл Hosts 38, 39
Физический:
адрес 145
сетевой адаптер 151
Фильтры входа 389

Х

Хаб 21, 42

Ш

Шлюз 46
Интернета 165



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.
MandrakeSoft Mandrakelinux. Полное руководство пользователя	528 с.
Mandriva Linux: полное руководство пользователя	544 с.
Актершев С. Задачи на максимум и минимум	199 с.
Андрианов В., Соколов А. Автомобильные охранные системы. Справочное пособие	272 с.
Бернс С. Фотомагия Photoshop. Трюки и эффекты. Полноцветное издание	448 с.
Богданов-Катьков Н. Струйные принтеры для дома и офиса	224 с.
Боков В. Физика магнетиков. Учебное пособие для вузов	129 с.
Боресков А. Разработка и отладка шейдеров	496 с.
Брайант Р., О'Халарон Д. Компьютерные системы: архитектура и программирование	1104 с.
Брэй Б. Микропроцессоры Intel: 8086/8088, 80186/80188, 80286, 80386, 80486, Pentium, Pentium Pro Processor, Pentium II, Pentium III, Pentium 4.Архитектура, программирование и интерфейсы. Шестое издание	1328 с.
Бурлаков М. В. Путеводитель по Adobe Photoshop CS 2	688 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.
Данилов П. The Bat! 3. Практическая работа	288 с.
Джазайери М. и др. Основы инженерии программного обеспечения. 2-е изд., пер. с англ.	832 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.
Калашников О. Ассамблер? Это просто! Учимся программировать	384 с.
Калиновский А. Ваша домашняя страничка в Интернете. Homepage, или просто "хомяк"	224 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.
Кертен Р. Введение в QNX Neutrino 2. Руководство для разработчиков приложений реального времени	400 с.
Климов А. Занимательное программирование на Visual Basic .NET	528 с.
Климов А., Чеботарев И. Windows. Народные советы	400 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.
Кулагин Б. 3ds max 8: Актуальное моделирование, визуализация и анимация	496 с.
Кулагин Б., Морозов Д. 3ds max 6 и character studio 4. Анимация персонажей	224 с.
Культин Н. Visual Basic. Освой на примерах (+CD-ROM)	288 с.
Культин Н. Visual Basic. Освой самостоятельно	480 с.
Макаров Б. и др. Избранные задачи по вещественному анализу, 2-е изд.	624 с.
Малыхина М. Базы данных: основы, проектирование, использование	512 с.
Мачник Э. Фотообман в Photoshop	272 с.
Михайлов С., Черков А., Цветков И. 1С:Бухгалтерия 7.7. Решение типичных проблем пользователя	272 с.
Морозова О. Построй свой супер-сайт за 21 день!	224 с.
Новиков Б., Домбровская Г. Настройка приложений баз данных	210 с.
Очков В. Mathcad 12 для студентов и инженеров	464 с.
Палмер М., Синклер Р. Проектирование и внедрение компьютерных сетей. Учебный курс, 2-е изд.	240 с.
Пахомов Б. C++ и Borland C++ Builder для начинающих	640 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.
Потопахин В. Turbo Pascal. Решение сложных задач	208 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.
Рыжиков Ю. Работа над диссертацией по техническим наукам	
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. Knoppix — это Linux без проблем	336 с.
Соломенчук В. Железо ПК 2005	480 с.
Соломенчук В. Железо ПК 2006	448 с.
Столлингс В. Компьютерные сети, протоколы и технологии Интернета	650 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.
Фленов М. Linux глазами хакера	550 с.
Фленов М. PHP глазами хакера	304 с.
Фленов М. Компьютер глазами хакера	336 с.
Фрей Д. AutoCAD и AutoCAD LT для начинающих	680 с.
Частиков А. Архитекторы компьютерного мира	384 с.
Чечельницкий А. Десятипальцевый набор на клавиатуре	48 с.
Шапорев Д. Visual FoxPro. Уроки программирования	480 с.
Щёлоков В. Новые правила приватизации земельных участков и строений. Справочник землепользователя	192 с.
Яцюк О. Основы графического дизайна на базе компьютерных технологий (+CD-ROM)	270 с.

www.bhv.ru

Старовойтов А.

Сеть на Linux: проектирование, прокладка, эксплуатация

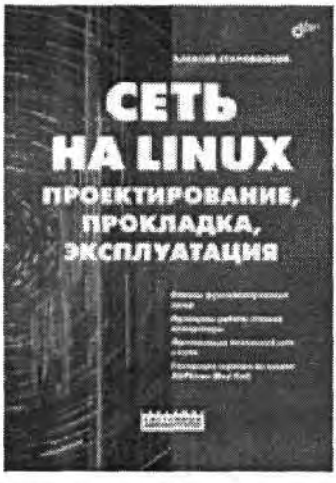
Серия «Системный администратор»

Магазин "Новая техническая книга"

СПб., Измайловский пр., д. 29, тел.: (812) 251-41-10

Отдел оптовых поставок

E-mail: opt@bhv.spb.su



Рассмотрены практические вопросы по прокладке сети, организации сервера (Apache, Samba, DNS, DHCP) на основе операционной системы Linux и интеграции этого сервера в сетях Windows. Большое внимание уделено повседневной эксплуатации сети. Излагаются основы функционирования сетей и сетевой аппаратуры. Даются практические рекомендации по проектированию и прокладке сетей, проверке и поиску неисправностей. Приводится пример построения локальной сети небольшой фирмы и методика поиска неисправностей без использования специального оборудования. Рассмотрены вопросы антивирусной защиты сервера. Описанная технология может быть использована не только при прокладке и сопровождении сети небольшой фирмы на основе Linux-сервера, но и для организации домашних сетей.

Старовойтов Алексей Анатольевич, окончил Московский энергетический институт по специальности «Промышленная электроника». После окончания института работал в области проектирования и прокладки малых локальных сетей. С 2000 года начал увлекаться Linux-системами, как одним из средств организации серверов локальных сетей. Хобби быстро стало профессиональным занятием, и в настоящее время автор продолжает работу в области организации локальных сетей, отдавая предпочтение Linux-системам для организации сервера, дает консультации по вопросам использования Linux в качестве сервера для небольших сетей.

Магазин-салон
"НОВАЯ ТЕХНИЧЕСКАЯ КНИГА"

190005, Санкт-Петербург, Измайловский пр., 29

В магазине представлена литература по

компьютерным технологиям

радиотехнике и электронике

физике и математике

экономике

медицине

и др.

Низкие цены
Прямые поставки от издательств
Ежедневное пополнение ассортимента
Подарки и скидки покупателям

Магазин работает с 10.00 до 20.00
без обеденного перерыва
выходной день – воскресенье

Тел.: (812)251-41-10, e-mail: trade@techkniga.com