

Александр Поляк-Брагинский

# ЛОКАЛЬНАЯ СЕТЬ

САМОЕ  
НЕОБХОДИМОЕ

2-е издание

Санкт-Петербург

«БХВ-Петербург»

2011

УДК 681.3.06  
ББК 32.973.202  
П54

**Поляк-Брагинский А. В.**

П54 Локальная сеть. Самое необходимое. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2011. — 576 с.: ил.

ISBN 978-5-9775-0636-6

Книга представляет собой практическое руководство по созданию локальной вычислительной сети для дома или небольшого офиса. Обсуждаются вопросы маршрутизации, удаленного администрирования и управления, настройки почтового сервера, совместного использования ресурсов. Представлено описание программ для передачи текстовой видео- и аудиоинформации, контроля трафика, удаленного управления и администрирования. Описано применение виртуальных технологий, позволяющих удешевить сеть, получить максимум функциональности при минимальных затратах. Рассмотрены вопросы объединения в одной сети компьютеров с разнородными операционными системами, имеющими на сегодняшний день достаточно широкое распространение, включая работу с операционными системами Windows и Linux. Описаны проблемы согласования в одной сети старых и новых компьютеров, а также организации доступа в сеть извне и защиты ее от несанкционированных действий.

Во втором издании добавлено описание полезных программ и средств администратора, увеличено число практических примеров, рассмотрены современные сетевые технологии.

*Для опытных пользователей и начинающих администраторов*

УДК 681.3.06  
ББК 32.973.202

**Группа подготовки издания:**

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Григорий Добин</i>
Редактор	<i>Юрий Рожко</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.11.10.

Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 46,44.

Тираж 1500 экз. Заказ №

"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию № 77.99.60.953.Д.005770.05.09 от 26.05.2009 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 978-5-9775-0636-6

© Поляк-Брагинский А. В., 2010  
© Оформление, издательство "БХВ-Петербург", 2010

# Оглавление

<b>Введение.....</b>	<b>9</b>
Благодарности .....	10
Для кого эта книга .....	11
О чем эта книга .....	11
Как читать эту книгу.....	11
Во втором издании.....	12
<b>ЧАСТЬ I. СОЗДАНИЕ ПРОСТЕЙШЕЙ СЕТИ.....</b>	<b>13</b>
<b>Глава 1. Два компьютера, соединенные кабелем, — это уже сеть.....</b>	<b>15</b>
Передача файлов с компьютера на компьютер .....	15
Связь ПК-ПК через LPT-порты .....	16
Связь ПК-ПК через сетевые адаптеры .....	18
IP-адреса .....	18
Расширения масок подсети .....	21
Подсоединение компьютеров .....	26
Сетевые настройки компьютера под управлением ОС Windows XP.....	27
Сетевые настройки компьютера под управлением ОС Windows Vista .....	36
Сетевые настройки компьютера под управлением ОС Linux .....	42
Настраиваем общий доступ к файлам и папкам в Windows Vista.....	48
Пример создания каталога общего доступа в Windows Vista.....	49
Настраиваем общий доступ к файлам и папкам в Linux.....	53
Особенности сетевого доступа к файлам из Linux к Windows Vista.....	57
Соединяем компьютеры без кабеля.....	58
Оборудование .....	58
Организация сети .....	62
Соединяем компьютеры посредством Bluetooth.....	70
Настройка Bluetooth.....	71
Windows 7 в сети.....	74
Соединяем компьютеры через Интернет .....	75
<b>Глава 2. Создаем одноранговую сеть.....</b>	<b>77</b>
Настраиваем сетевое подключение .....	77
Сетевое подключение в одноранговой сети .....	78

Настройка сервера Samba в Linux .....	82
Подключаем общий принтер .....	86
Общий принтер в Windows Vista .....	86
Общий принтер в Linux .....	90
Подключаем сеть к Интернету.....	93
Настройка в старых версиях Windows .....	94
Настройка компьютера общего доступа к Интернету .....	94
Настройка остальных компьютеров сети.....	95
Настройка в Windows Vista и Linux.....	98
<b>Глава 3. Защищаем сеть .....</b>	<b>130</b>
Брандмауэр .....	130
Брандмауэр Windows .....	131
Файрвол в Mandriva Linux .....	135
Брандмауэр для Windows Comodo.....	137
И снова Firestarter.....	140
Антивирус.....	142
Avast!.....	143
AnVir Task Manager .....	145
<b>ЧАСТЬ II. НЕОБЫЧНЫЕ РЕШЕНИЯ В СЕТИ .....</b>	<b>147</b>
<b>Глава 4. Соединяем удаленные компьютеры .....</b>	<b>149</b>
Соединяем удаленные компьютеры через модем .....	149
Соединяем компьютеры под управлением Windows Vista.....	149
Связь двух компьютеров через модем в Windows XP .....	154
Соединяем компьютеры под управлением Windows 98.....	157
Компьютер — телефон — компьютер .....	158
Комментарии.....	161
Микрофильтры и сплиттеры .....	161
Шлюз для доступа в Интернет .....	161
DNS .....	162
IP-адреса .....	162
Соединяем компьютеры через Интернет .....	163
OpenVPN.....	164
Hamachi .....	167
NeoRouter.....	169
NeoRouter Configuration Explorer.....	170
<b>Глава 5. Маршрутизация .....</b>	<b>175</b>
Сетевой мост .....	175
Настраиваем маршрутизацию в Windows XP.....	180
Указываем маршруты .....	180
Делаем маршрутизатор из Windows XP .....	182
Настраиваем маршрутизацию в Linux Mint.....	185
Применяем аппаратные маршрутизаторы и модемы.....	187
Настраиваем связь по выделенной линии.....	187
Настраиваем доступ через Интернет .....	193
Ссылки .....	197

<b>Глава 6. Используем старый компьютер в сети .....</b>	<b>198</b>
Компьютер под DOS в вашей сети .....	198
Установка операционной системы MS-DOS 7.1 .....	199
Установка Microsoft Network Client version 3.0 for MS-DOS .....	203
Настройки DHSP и WINS на сервере Windows 2000 Server.....	208
Linux .....	210
Файловая система.....	210
Работа в сети Windows.....	211
Некоторые замечания .....	214
<b>ЧАСТЬ III. СРЕДСТВА ВОССТАНОВЛЕНИЯ И ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ СЕТИ .....</b>	<b>217</b>
<b>Глава 7. Хранение данных, восстановление системы .....</b>	<b>219</b>
Резервирование и архивирование данных .....	219
Acronis True Image — резервное копирование всей системы .....	220
Средства Windows.....	225
Используем консоль восстановления .....	226
Консоль восстановления в загрузочном меню .....	226
Основные команды Консоли восстановления .....	227
Сохраняем важные данные .....	230
Копирование данных в сетевой каталог .....	230
<b>Глава 8. Обеспечиваем бесперебойное питание.....</b>	<b>236</b>
Бесперебойное питание для двух серверов.....	236
Существующие решения .....	237
<b>ЧАСТЬ IV. СЕТЕВЫЕ СЕРВЕРЫ .....</b>	<b>245</b>
<b>Глава 9. Выбираем операционную систему.....</b>	<b>247</b>
Операционная система для сервера.....	247
Установка операционной системы на сервер .....	250
Итак, начнем установку.....	253
Источники бесперебойного питания .....	260
Планирование общих ресурсов и прав пользователей.....	262
Пример создания нового пользователя и нового ресурса .....	266
Другие возможности управления правами пользователей .....	269
Windows Server 2003.....	270
Варианты работы выделенного сервера.....	273
Как работает сервер приложений? .....	273
Настройка сервера после установки.....	274
Настройка служб терминалов .....	277
Операционная система для рабочей станции .....	284
Еще немного информации об ОС .....	285
<b>Глава 10. Выбираем файловую систему .....</b>	<b>287</b>
Сравнительная характеристика NTFS и FAT32 .....	288
NTFS.....	288
FAT32.....	288
Некоторые выводы.....	289

Теперь немного о файловых системах для Linux .....	289
Parted Magic .....	290
<b>Глава 11. Устанавливаем виртуальный компьютер.....</b>	<b>293</b>
Что можно установить? .....	294
Установка Microsoft Virtual Server 2005 R2 .....	295
Используем VMware Player .....	300
VMware Server .....	302
Замечания по установке VMware Server и VMware Player под Linux .....	302
Соблюдаем лицензии .....	307
Virtual Appliances .....	308
Виртуальные технологии в нашей сети .....	309
Два компьютера в одном .....	310
Запуск виртуальной машины по сети .....	318
Задачи для виртуальной машины .....	323
Установка Oracle VirtualBox .....	325
<b>Глава 12. Настраиваем файловый сервер.....</b>	<b>335</b>
Каким должен быть файловый сервер? .....	335
Настройка сервера .....	337
Настраиваем файловый сервер под Linux .....	342
<b>Глава 13. Настраиваем FTP-сервер.....</b>	<b>346</b>
Клиент FTP .....	349
TFTP-сервер .....	351
<b>Глава 14. Настраиваем Web-сервер .....</b>	<b>353</b>
Web-сервер средствами ОС .....	353
Простой Web-сервер другими средствами .....	357
<b>Глава 15. Настраиваем DHCP-сервер.....</b>	<b>359</b>
DHCP-сервер Windows Server 2003 .....	359
Установка .....	360
Резервирование IP-адреса на DHCP-сервере .....	364
Дополнительные настройки .....	366
Простой DHCP-сервер на базе Linux Ubuntu .....	368
<b>Глава 16. Настраиваем WINS-сервер.....</b>	<b>370</b>
WINS-сервер Windows Server 2003 .....	370
Пример локальной сети с WINS-сервером .....	372
<b>Глава 17. Настраиваем DNS-сервер .....</b>	<b>375</b>
Зачем DNS-сервер в сети .....	375
DNS-сервер Windows Server 2003 .....	377
<b>Глава 18. Настраиваем media-сервер.....</b>	<b>382</b>
Кодировщик Windows Media 9 Series .....	382
VLC Media Player — трансляция по сети .....	386
Передача .....	387
Прием .....	391
Ссылки .....	393

<b>Глава 19. Настраиваем почтовый сервер .....</b>	<b>394</b>
Почтовый сервер в Windows Server 2003.....	394
Управление почтовым сервером.....	397
Web-интерфейс.....	398
Courier Mail Server .....	402
Ссылки .....	423
<b>ЧАСТЬ V. ПРЕОБРАЗОВАНИЕ ОДНОРАНГОВОЙ СЕТИ В ИЕРАРХИЧЕСКУЮ .....</b>	<b>425</b>
<b>Глава 20. Организация доменной сети .....</b>	<b>427</b>
Active Directory.....	427
Что же такое AD? .....	427
Установка AD.....	428
Политики .....	435
Добавление пользователей.....	437
Сетевой профиль .....	443
Регистрация компьютеров.....	443
Регистрация других объектов .....	444
Изменение свойств объектов .....	445
О безопасности.....	447
<b>ЧАСТЬ VI. ОСОБЫЕ ПРИЕМЫ АДМИНИСТРИРОВАНИЯ.....</b>	<b>449</b>
<b>Глава 21. Средства автоматизации .....</b>	<b>451</b>
Применяем сценарии .....	451
Общие сведения .....	451
Редактор PrimalScript.....	453
Программы в формате HTA.....	456
Ссылки .....	461
Сценарии в Linux .....	461
<b>Глава 22. Средства удаленного управления и администрирования .....</b>	<b>465</b>
Управляем локально .....	465
Осуществляем удаленное администрирование .....	469
Решаем задачи администрирования по e-mail .....	470
Удаленный доступ к рабочему столу рабочей станции через Интернет.....	477
Настраиваем рабочую станцию с выделенным IP-адресом.....	477
Устанавливаем подключение к рабочему столу.....	479
Вариант 1 .....	479
Вариант 2 .....	480
Рекомендации .....	480
Настраиваем рабочую станцию с динамическим IP-адресом .....	482
Доступ к удаленному рабочему столу Linux .....	483
Подключение к компьютеру с помощью LogMeIn .....	487
<b>Глава 23. Подсчитываем трафик.....</b>	<b>491</b>
Возможности программы BWMeter .....	491
Настраиваем программу.....	492
Ссылки .....	496

<b>ПРИЛОЖЕНИЯ .....</b>	<b>497</b>
<b>Приложение 1. Общение через домашнюю сеть и Интернет .....</b>	<b>499</b>
Средства связи.....	499
Факс в Windows.....	500
Факс в Linux.....	504
Электронная почта в Windows .....	505
Электронная почта в Linux.....	508
Программы обмена мгновенными сообщениями, голосом и видео в Windows .....	510
Программы обмена мгновенными сообщениями, голосового и видеосообщения в Linux .....	514
Радио и телевидение в сети.....	517
Видеокамера в сети с компьютерами под Windows.....	517
Домашнее телевидение.....	519
VLC-медиаплеер .....	524
Ретрансляция радио и телевизионных передач .....	524
<b>Приложение 2. Советы начинающему администратору локальной сети .....</b>	<b>529</b>
Что должен знать администратор локальной сети? .....	529
Где можно получить необходимые программы? .....	530
Поиск информации в Интернете.....	530
<b>Приложение 3. Краткий словарь терминов и сокращений .....</b>	<b>532</b>
<b>Приложение 4. Справочные сведения .....</b>	<b>542</b>
Создание Web-страниц.....	542
Основа Web-страницы.....	542
Форматирование Web-страницы .....	543
Специальные символы.....	543
Ссылки .....	544
Графика на Web-странице.....	544
Управление цветом .....	545
Таблицы .....	545
Что такое служба каталогов? .....	546
Зачем нужна служба каталогов? .....	547
Active Directory.....	547
Основные понятия.....	548
Спецификации на допустимые расстояния кабеля в сети Ethernet.....	552
<b>Приложение 5. Наиболее используемые команды Linux.....</b>	<b>553</b>
<b>Предметный указатель .....</b>	<b>571</b>



# Введение

Что для вас кажется самым необходимым? Большинство считает, что это то, без чего нельзя обойтись. На самом деле, внимательно осмотревшись, вы обнаружите, что множество из кажущихся необходимыми вещей вокруг нас совсем не нужны. Человеку не так много надо, чтобы жить. Правда, для обеспечения такой жизни необходимо много работать, заниматься совсем не тем, чем хотелось бы, работать даже тогда, когда очень хочется отдохнуть.

Жизнь современного пользователя ПК, а тем более системного администратора, в значительной мере проходит в сети. Жизнь в сети тоже может быть аскетичной. Ничего лишнего, просто связь между компьютерами для решения каких-либо практических задач. Тем не менее обслуживание такой сети и ее пользователей, поддержание жизни в ней может быть весьма трудоемким. Особенно, если это сеть смешанная и ее узлы находятся на значительном расстоянии друг от друга.

Желая сделать свою жизнь более интересной, человек находит средства и приемы для упрощения выполнения множества рутинных ежедневных задач. Так же и в сети. Организовав сеть или начав работать в уже существующей сети, очень хочется переложить некоторые задачи на плечи вспомогательного программного обеспечения, освободив себе время для творческой работы или просто для отдыха.

Творчество — всегда присуще человеку. Поэзия это или земледелие, а творческий человек всегда вкладывает свою душу в любимое дело. Поэзия и земледелие, как и многие другие области человеческой деятельности, существуют очень давно. Но появляются новые и новые сферы применения творческого потенциала человека. Сначала это работы энтузиастов, и их работа не всегда понятна окружающему большинству. Постепенно это новое проникает в жизнь обычных людей и становится привычным, как земледелие.

Компьютерные сети стали обычным и распространенным явлением во всем цивилизованном мире. Творчески настроенные любители и профессионалы создают свои произведения и делятся своим опытом с себе подобными и просто интересующимися.

Один компьютер теперь не может существовать сам по себе, как муравей без муравейника. Все, что делается для компьютера, делается для сети. Даже дома в самых консервативных семьях появляются компьютеры, которые подключаются

к сети. Пользователям компьютеров все чаще требуется своя сеть, выполняющая именно их задачи. Затем возникает необходимость в объединении этих маленьких сетей, потом... Словом, творчество не имеет границ.

Когда-то и автор этой книги начал работу в небольшой локальной сети. Лень, присущая человеку, а особенно системным администраторам, и на этот раз стала двигателем прогресса. Работая существенно больше, чем было отведено графиком работы, автору удалось настолько освободить свое время и время своих сотрудников от рутинных задач, что руководство совершенно освободило его от должности системного администратора, переведя на должность заместителя директора. Но до настоящего времени локальная вычислительная сеть остается делом и увлечением, которое занимает почти все свободное время.

Теперь очень часто нет необходимости изобретать велосипед — сети существуют достаточно давно, чтобы накопился очень богатый опыт их эксплуатации.

Все же, есть немало вопросов, которые недостаточно освещены как в литературе, так и в Интернете. Новые операционные системы, причем не только от Microsoft, входят в жизнь обычных пользователей ПК. Они еще не стали общепринятыми и общепризнанными, но уже теснят привычные Windows на рабочих столах пользователей. Это заставляет задуматься и системных администраторов, особенно администраторов малых сетей, где чаще всего нет единого стандарта на применяемые рабочие станции и их ОС. Linux еще несколько лет назад была привилегией очень опытных пользователей, имеющих желание и способных разобраться во множестве конфигурационных файлов и скриптов, не используя графический интерфейс, теперь же эта ОС становится такой же доступной, как и Windows. Пришла пора обратить на Linux внимание, не бояться этой операционной системы, а изучать ее, включать в свои сети компьютеры под ее управлением.

В этой книге автор попытался собрать как свой опыт, так и опыт сетевого сообщества, который может быть полезен и вам при организации небольшой домашней или офисной сети. Насколько средства, описанные автором, покажутся вам необходимыми, зависит от многих условий и задач, поставленных перед сетью. В различные моменты времени, при решении конкретных задач, описанные в книге средства автору казались крайне необходимыми.

## Благодарности

Книга редко бывает продуктом индивидуальной работы. Конечно, материал книги выстрадан автором, но без содействия множества других людей книгу не увидят читатели.

Трудно перечислить всех поименно. Ведь даже разработчики операционных систем и вычислительной техники невольно содействовали появлению этой книги. Если бы не они, не о чем было бы писать. Моя благодарность им.

Друзья и семья, которые поддерживали в трудные минуты, тоже содействовали появлению этой книги.

Редакторы стоят на рубеже подготовки книги к печати. Им приходится причисывать текст, находить не совсем логичные с точки зрения читателя фразы, обна-

рживать случайные ошибки, иногда спорить с автором, добиваясь максимально возможной стройности произведения. Я благодарен этим людям за их терпение и профессионализм.

Читатели моих книг нередко задают вопросы, заставляют задуматься над еще не описанными проблемами, требующими решения у читателей. Я глубоко признателен всем, кто пишет мне, предлагает новые идеи, своими вопросами побуждает к дальнейшей работе над новыми книгами. Благодарю всех активных читателей и тех, кто просто купил и прочитал книгу. Приобретение книги — своего рода голосование за нее.

## **Для кого эта книга**

Книга предназначена для всех интересующихся созданием и эксплуатацией локальных сетей. Все, кто связал себя с этим интересным и полезным направлением деятельности, внес в большей или меньшей степени и свой вклад в общее дело. Иногда даже вопрос, заданный начинающим пользователем, становится импульсом к появлению новой идеи и новой разработки. Конечно, эти идеи и разработки не всегда публикуются в массовых печатных изданиях и транслируются по телевидению. Но разве в этом смысл жизни творческой личности? Достичь желаемого результата и поделиться с себе подобными. Даже материальная сторона вопроса уходит на задний план. Для тех, кто еще начинает, но уже решил связать свою жизнь с сетью, будь то маленькая квартирная сеть или сеть предприятия, и для тех, кто уже создал свою маленькую первую сеть и не хочет останавливаться на достигнутом результате, и предназначена эта книга.

## **О чем эта книга**

О локальной компьютерной сети, ее создании, работе в ней и ее администрировании. О приемах и средствах, облегчающих работу в сети, делающих сеть еще полезнее, а работу в ней интереснее. О том, что может оказаться необходимым в вашей работе в сети.

## **Как читать эту книгу**

Книга разбита на части и главы, которые рассказывают о создании простой сети, о средствах управления сетью, использовании виртуальных технологий в сети. Рассмотрены задачи, которые реально возникали при создании и эксплуатации небольшой сети. Поэтому, если вы начинающий пользователь или администратор маленькой локальной сети, прочитайте книгу последовательно от начала до конца. Тяжелой для понимания информации в ней почти нет. Прочитав книгу, вы, возможно, будете возвращаться к отдельным ее главам, решая конкретные сетевые задачи. Примеры, приведенные в книге, доступны для повторения. Все они были обязательно опробованы автором. Некоторые из них могут показаться поначалу сложными. Но постепенно, совершенствуя свою сеть, столкнувшись с задачами,

описанными в книге, вы обнаружите, что ранее казавшийся сложным материал оказался достаточно простым.

## Во втором издании

Во втором издании книги добавлены материалы по работе в операционной системе Linux и работе с аппаратными маршрутизаторами компании Allied Telesis. Linux становится все более популярной операционной системой и осваивать работу в ней начинающему системному администратору необходимо. Надо заметить, что Linux изначально разрабатывалась в качестве сетевой операционной системы. Чем больше вариантов решения задачи вы знаете, тем успешней будет решение вопросов, связанных с созданием и обслуживанием реальной сети. Аппаратные маршрутизаторы тоже завоевывают позиции в небольших сетях. Однажды настроенный маршрутизатор работает без зависаний и ошибок, не требует обслуживания, обновления операционной системы. Маршрутизаторы фирмы Allied Telesis дешевле устройств Cisco, и освоить работу с ними не так уж сложно.

*Глава 4* дополнилась информацией о программе NeoRouter, о которой автор узнал совсем недавно, но применив в своей практике, обнаружил, что программа — просто находка для начинающих администраторов, если им необходимо быстро настроить виртуальную сеть между несколькими компьютерами в Интернете.

К сожалению, по ряду причин автору пришлось отказаться от поддержки своего сайта. Тем не менее, читатели могут связаться с автором по электронной почте по следующему адресу: **tx-mm@mail.ru**.



# ЧАСТЬ I

## Создание простейшей сети

Эта часть посвящена описанию операций, необходимых для создания простейшей сети.

Теперь трудно удивить тем, что у вас дома два-три компьютера, все они имеют доступ в Интернет и каждый имеет доступ к каждому. Но, такие мини-сети существуют у пользователей ПК со стажем. Если же вы еще не достаточно уверенно владеете знаниями и умениями в области "сетестроения" — не беда! Начните с самого простого. Тем более что все сложное состоит из простых составляющих.



# ГЛАВА 1



## Два компьютера, соединенные кабелем, — это уже сеть

Любая современная операционная система содержит в своем составе средства для объединения персональных компьютеров в сеть. Способов такого объединения существует довольно много, и вам решать, какой из них применить. Правильная постановка задачи поможет выбрать наиболее рациональное решение. Спросите сами себя — чего я жду от своей сети? Даже два компьютера можно объединить в простейшую сеть несколькими способами. Каждый из этих способов имеет свои преимущества, недостатки и особенности. Поставив задачу, можно выбрать наименее затратный и наиболее доступный способ объединения компьютеров.

### Передача файлов с компьютера на компьютер

Это одна из самых простых и распространенных задач, которую можно решить, объединив компьютеры в сеть. На самом деле кажущиеся лаконичность и простота такой задачи весьма обманчивы. Советы, которые можно найти в литературе и в Интернете, описывают как очень простые варианты решения, так и связанные с глубоким знанием современных технологий передачи данных. Но нам нужно просто передать файлы. Чаще всего такая задача возникает при появлении второго компьютера. Есть, конечно, компактные средства для временного хранения и переноса данных, такие как *флэш-накопители* ("флэшки") или *флэш-карты*, широко применяемые в цифровых фотоаппаратах. Многие современные компьютеры снабжены встроенными адаптерами (*картридерами*) для использования этих средств. Есть и внешние адаптеры, которые можно подключать к компьютерам через USB или *PCMCIA-порты*. Но, если компьютеры находятся рядом, значительно удобнее иметь постоянное соединение между ними. В современных условиях удобнее всего такое соединение выполнять стандартными средствами, с применением обычных на сегодняшний день сетевых технологий. Но в отдельных случаях, когда сеть еще не создана, когда нет другого способа перенести необходимые файлы с компьютера на компьютер, можно применить простейший способ соединения, рассмотренный в следующем разделе.

## Связь ПК-ПК через LPT-порты

Надо сказать, что сетевые технологии применяются так давно, что кое-что уже стирается из памяти пользователей ПК. Уже трудно встретить компьютер под управлением DOS, и легко встретить человека, который даже не представляет себе это семейство операционных систем, некогда очень популярных у самых обычных пользователей персональных компьютеров. Но остались средства, которые разрабатывались для передачи информации между компьютерами под управлением DOS. В старых руководствах для начинающих пользователей ПК можно встретить подробное описание Norton Commander. Это файловый менеджер с широчайшими возможностями, без которых трудно было представить комфортную работу на старых машинах. В этот менеджер встроена возможность подключения к другим компьютерам, и не одна. Если вас заинтересует работа с этим шедевром прошлого, поищите старые самоучители для пользователей ПК. Здесь же мы рассмотрим другую программу связи между компьютерами — *Lap2Desk* (L2D.EXE). Честно говоря, теперь трудно найти ее в Интернете. Это действительно народное средство, передаваемое от пользователя к пользователю через Интернет. Таким же образом оно попало когда-то и ко мне. Исключительная простота программы и ее миниатюрность заслуживают внимания и в наше время. А в ситуациях, когда необходимо перенести файлы на компьютер без установленной операционной системы, программа может оказаться незаменимой.

Для осуществления связи между компьютерами через параллельные порты (LPT), которые чаще применяются для подключения принтеров, необходим *нуль-модемный кабель*, который можно купить или изготовить самостоятельно из обычного кабеля для LPT-портов, перепаяв проводники на одном из разъемов кабеля в соответствии с табл. 1.1. Разъемы имеют по 25 контактов, но перепаять следует только те, что указаны в таблице. Остальные проводники должны соединять контакты обоих разъемов с одинаковым номером.

**Таблица 1.1.** Распайка кабеля LPT

Разъем 1	Разъем 2
2	15
3	13
4	12
5	10
6	11
10	5
11	6
12	4
13	3
15	2



Изготовив или купив кабель, скачайте файлы программы Lap2Desk по адресу <http://antiqua.boom.ru/link/lap2deck.zip> или <http://nostalgym.net.ru/link/lap2deck.zip>. В архиве link.zip находятся следующие файлы:

- L2D.EXE
- L2DMAP.EXE
- example.BAT
- README.TXT

Распаковав архив в любой заранее созданный каталог и используя любой текстовый редактор, создайте в этом каталоге файлы LINKSLP.BAT и COM\_2.BAT для удобства работы с программой.

Файл LINKSLP.BAT содержит строки:

```
@echo off
l2d /lpt1
l2dmap.exe
```

Файл COM\_2.BAT содержит строки:

```
@echo off
mode com2:19200,n,8,1,p
l2d /com2
```

Скопируйте этот каталог на дискету или в раздел винчестера с файловой системой FAT или FAT32. На ту же дискету или в раздел винчестера запишите файлы файлового менеджера, например, Volkov Commander. Соедините компьютеры подготовленным кабелем.

#### **ПРИМЕЧАНИЕ**

Соединение компьютеров желательно выполнять при выключенных компьютерах.

Далее можно начинать работать с программой.

Загрузку компьютеров можно произвести с загрузочной дискеты, изготовленной в ОС Windows 98 средствами самой системы.

#### **ПРИМЕЧАНИЕ**

Если у вас нет загрузочной дискеты, то рекомендации по ее изготовлению можно получить по адресу <http://support.microsoft.com/kb/325879/>, подробную информацию по изготовлению других загрузочных устройств по адресу <http://www.multiboot.ru/xpboot.htm>.

После окончания загрузки обоих компьютеров вставьте в каждый из них по очереди дискету с файлами программы и файлового менеджера (возможно, что вы сочтете более удобным создать вторую копию дискеты).

Запустите на выполнение файл LINKSLPT.BAT (в этом файле записаны команды для начала работы с программой). Это действие следует выполнить на обеих машинах.

Выберите букву доступного для работы диска, на который будет отображаться диск второго компьютера (available for mapping), нажмите комбинации клавиш <M> и <Alt>+<X>. Программа позволяет выбрать, какой из дисков второго компьютера должен быть подключен под выбранной буквой.

Интерес возможно представляет и то, что программа может работать под управлением Windows 98, если запущена до запуска Windows (на начальном этапе загрузки). Файл L2DMAP.EXE из комплекта программы необходим только для визуального отображения функций программы и действий пользователя. Те, кто знаком с командной строкой DOS, сможет работать с программой и без графического интерфейса (GUI), работая с L2D.EXE из командной строки. Параметры для работы в командной строке можно узнать, выполнив команду L2D.EXE /?.

### **ЗАМЕЧАНИЕ**

Программа Lap2Desk применяется и для связи компьютеров через последовательные порты. При этом технология работы с ней не изменяется, но *потребуется кабель для COM-портов*.

К сожалению, на современных компьютерах воспользоваться этой программой сложно. Работает она под управлением DOS или Windows ранних версий, основанных на DOS (Windows 95/98), поэтому диски размером более 8 Гбайт и отформатированные в файловой системе NTFS она не увидит. Но если в вашем распоряжении оказалась пара старых компьютеров, ее вполне можно применить для передачи файлов между ними.

В старых операционных системах были штатные средства для организации подключения через LPT- или COM-порты. Можно найти программы для связи через USB-порты. Но для современных компьютеров актуальность таких способов связи между компьютерами низка. Опыт говорит, что при наличии сети они не могут дать каких-либо преимуществ по сравнению с обычным сетевым подключением. Но, кто знает, может быть, вам пригодится этот редкий метод организации простой сети между раритетными компьютерами. Но, даже если не пригодится, знать о нем надо. Если вам удастся поработать с таким соединением, вы сможете оценить современные сетевые технологии, прочувствовать дыхание истории... Далее мы не будем рассматривать устаревшие сетевые технологии. И приступим к созданию вполне современного сетевого соединения.

## **Связь ПК-ПК через сетевые адаптеры**

Этот способ соединения компьютеров по сравнению с рассмотренным в начале главы уже значительно ближе к тем, что применяются в настоящих *локальных вычислительных сетях* (ЛВС). Отличие состоит только в том, что в первом случае компьютеров может быть всего лишь два. Сеть же это два или более соединенных между собой компьютеров. Значит, наш случай соответствует созданию простейшей сети из двух компьютеров.

### **IP-адреса**

Сети, о которых далее будет идти речь, создаются по технологии Ethernet. Если вы хотите подробнее узнать об этой технологии, можно посетить страницу <http://ru.wikipedia.org/wiki/Ethernet>. Одна из особенностей этой технологии со-

стоит в том, что каждый узел сети, в том числе и компьютер, должен иметь свой IP-адрес, который представляет из себя 32-битное число для четвертой версии IP-протокола (*IPv4*) и 128-битное для шестой версии (*IPv6*). Ввиду того, что IPv6 еще не получил распространения у обычных пользователей ПК, мы будем рассматривать работу только с IPv4.

Стандарты IEEE 802.3u Fast Ethernet и IEEE 802.3z Gigabit Ethernet в настоящее время наиболее распространены в локальных сетях. Выполненные в соответствии с этими стандартами сети могут работать на скоростях 100 и 1000 Мбит/с соответственно. Для домашней сети вполне может быть достаточно и более низких скоростей передачи данных. Если ваш сетевой адаптер не новый и соответствует стандарту IEEE 802.3i, то скорость передачи данных будет составлять 10 Мбит/с, что нас вполне устроит.

Но в любом случае правила, по которым станет работать сеть, будут одни и те же. Сетевое оборудование при этом использует метод управления доступом — множественный доступ с контролем несущей и обнаружением коллизий (*CSMA/CD* — Carrier Sense Multiple Access with Collision Detection). Это значит, что все узлы сети, общаясь между собой, смогут "видеть" друг друга одновременно, а ошибки при передаче данных будут автоматически обнаруживаться и исправляться.

Все программы и устройства, работающие в сети, будут подчиняться семейству протоколов *TCP/IP* (Transmission Control Protocol/Internet Protocol — Протокол управления передачей/протокол Интернета). Этим протоколам (иначе правилам общения компьютеров в сети между собой) подчиняются в наше время все сети, имеющие выход в Интернет. Ведь мы не хотим оставаться в изоляции от большого сетевого сообщества! Значит, и наша создаваемая сеть должна работать по общим правилам. Представить суть работы этих правил проще всего, посмотрев на графическое представление работы TCP/IP (рис. 1.1).

Вся передаваемая по сети информация делится на *пакеты данных*, каждый из них учитывается, контролируется его доставка получателю. В случае ошибки при передаче пакета он передается повторно. 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).

Остается выяснить, каким образом компьютеры будут находить друг друга в сети? Для этого существует система IP-адресов.

Протокол IP пакеты информации 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 процедура выполняется в обратном порядке. Пакеты принимаются, сортируются и собираются в исходном сочетании. Цифровой, а вернее *IP-адрес*, представляет собой четырехбайтовую 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).

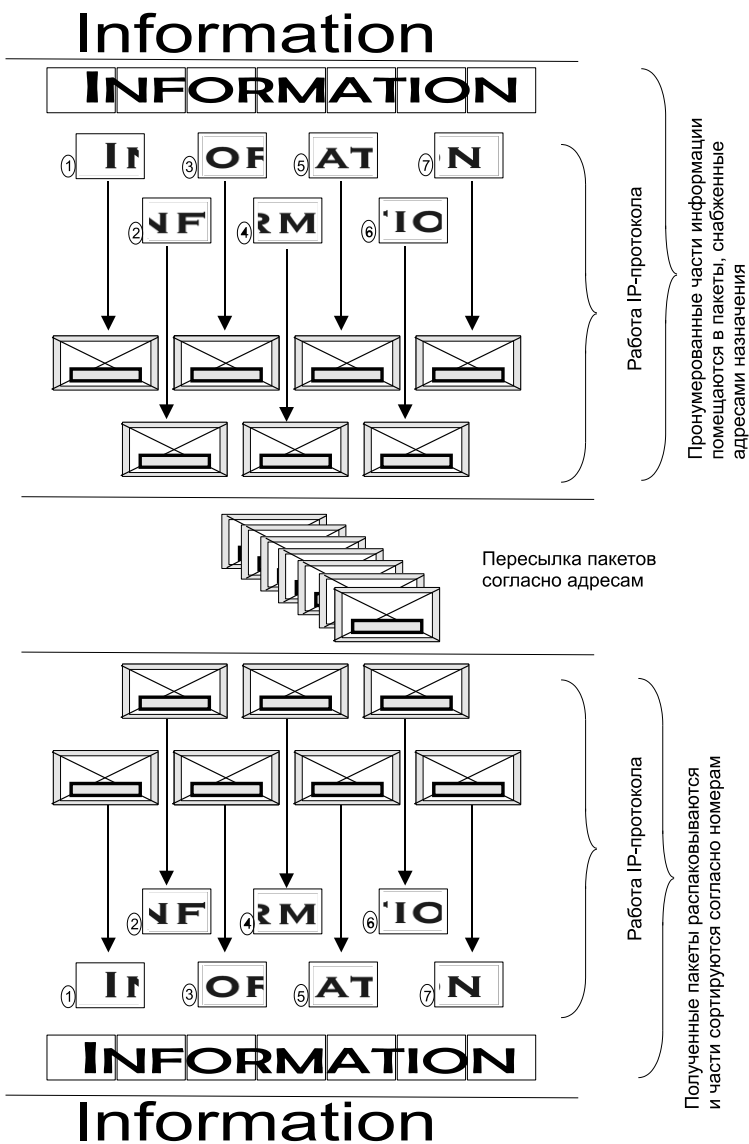


Рис. 1.1. Графическое представление работы TCP/IP

Таблица 1.2. Диапазоны адресов для классов сетей

Класс сети	Маска подсети	Диапазон адресов	Зарезервированные адреса
A	255.0.0.0	01.0.0.0—126.0.0.0	10.0.0.0 по 10.255.255.255 127.0.0.0 по 127.255.255.255
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

Маска подсети показывает 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 (резервированных) адресов.

Структура адреса становится более понятной при представлении его 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. Именно такие адреса будут присваиваться компьютерам нашей сети. В отдельных случаях компьютер или другое сетевое устройство может иметь не один адрес. Важно, чтобы соблюдалось правило уникальности адреса в сети. Появление двух устройств с одинаковым адресом вызовет ошибку в работе сети, и одно из устройств или сразу оба не смогут в ней работать. Современные операционные системы обнаруживают такие ситуации и сообщают пользователю о возникшей проблеме. При создании сети и подключении к Интернету на первых порах вызывает затруднение определение диапазона адресов по известной маске. Для того чтобы уверенно читать сетевые адреса и назначать их в своей сети, есть смысл подробнее рассмотреть расширения масок подсети.

## Расширения масок подсети

В отдельных случаях бывает удобно использовать значение *маски подсети* с расширением. Это позволяет логически выделять сети одного класса и коротко записывать сетевые адреса. Максимальное значение адреса сети в двоичном виде представлено непрерывным рядом единиц. Само *расширение* — это число двоичных единиц в значении маски подсети. Один из диапазонов, применяемый для локальных сетей с выходом в Интернет: с 192.168.0.0 по 192.168.255.0.

### ПРИМЕЧАНИЕ

Значения "0" и "255" в адресах узлов сети не применяются, поскольку соответствуют многоадресной рассылке пакетов. Если послать сообщение, адресованное узлу с адресом 192.168.0.255 (маска подсети 255.255.255.0), то сообщение получат все компьютеры сети.

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 64516 узлов. Для общего применения такие значения адресов не рекомендованы, но в закрытых сетях их можно использовать, как и адреса 10.0.0/24. Расширение (табл. 1.3), таким образом, позволяет более точно указать назначение адреса, независимо от принятых договоренностей о применении диапазонов адресов.

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

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)

<b>Маска подсети 255.255.255.248/29 (11111111.11111111.11111111.11111000)</b>			
<b>32 подсети</b>			
<b>Наименьший IP</b>	<b>Наибольший IP</b>	<b>Наименьший IP</b>	<b>Наибольший IP</b>
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

<b>Маска подсети 255.255.255.252/30 (11111111.11111111.11111111.11111100)</b>			
<b>64 подсети</b>			
<b>Наименьший IP</b>	<b>Наибольший IP</b>	<b>Наименьший IP</b>	<b>Наибольший IP</b>
x.x.x.0	x.x.x.3	x.x.x.128	x.x.x.131
x.x.x.4	x.x.x.7	x.x.x.132	x.x.x.135
x.x.x.8	x.x.x.11	x.x.x.136	x.x.x.139
x.x.x.12	x.x.x.15	x.x.x.140	x.x.x.143
x.x.x.16	x.x.x.19	x.x.x.144	x.x.x.147
x.x.x.20	x.x.x.23	x.x.x.148	x.x.x.151
x.x.x.24	x.x.x.27	x.x.x.152	x.x.x.155
x.x.x.28	x.x.x.31	x.x.x.156	x.x.x.159
x.x.x.32	x.x.x.35	x.x.x.160	x.x.x.163
x.x.x.36	x.x.x.39	x.x.x.164	x.x.x.167
x.x.x.40	x.x.x.43	x.x.x.168	x.x.x.171
x.x.x.44	x.x.x.47	x.x.x.172	x.x.x.175

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.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 показана связь между расширением маски подсети, двоичной записью маски и побайтовой записью для 32-разрядных адресов. Для каждого расширения указаны количество и класс сетей, которые могут быть созданы с применением данной маски.

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

Расш.	Маска подсети в двоичном представлении	Побайтовое представление	Число узлов	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



Таблица 1.4 (окончание)

Расш.	Маска подсети в двоичном представлении	Побайтовое представление	Число узлов	Класс
/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
/25	11111111.11111111.11111111.10000000	255.255.255.128		C
/26	11111111.11111111.11111111.11000000	255.255.255.192	1	C
/27	11111111.11111111.11111111.11100000	255.255.255.224	1	C
/28	11111111.11111111.11111111.11110000	255.255.255.240	1	C
/29	11111111.11111111.11111111.11111000	255.255.255.248	1	C
/30	11111111.11111111.11111111.11111100	255.255.255.252	1	C
/31	11111111.11111111.11111111.11111110	255.255.255.254	1	C
/32	11111111.11111111.11111111.11111111	255.255.255.255	0	—

Далее приведен пример преобразования двоичного значения 11000000 в десятичный вид (192).

$$\begin{aligned}
 11000000 \text{ Bin} &= 128*1 + 64*1 + 32*0 + 16*0 + 8*0 + 4*0 + 2*0 + 1*0 \\
 &= 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 \\
 &= 128 + 64 \\
 &= 192
 \end{aligned}$$

Для того чтобы во время работы с реальными компьютерами легче было разобратся с присвоением IP-адресов, еще раз обратимся к таблице (табл. 1.2). В поле **Зарезервированные адреса** указаны диапазоны IP-адресов, с которыми при создании локальной сети нам придется встречаться наиболее часто. Эти адреса не используются для узлов в Интернете. Некоторые адреса не используются и в локальных сетях. Локальный компьютер, имеющий возможность подключения к сети или уже подключенный, кроме сетевого IP-адреса имеет свой внутренний IP-адрес из диапазона с 127.0.0.0 по 127.255.255.255. Обычно это адрес 127.0.0.1. Вы всегда можете проверить возможность работы вашего компьютера в сети, выполнив из командной строки команду `ping 127.0.0.1`. Если в ответ на эту команду появляется информация об отправленных и полученных пакетах, то можно быть уверенным, что компьютер сможет работать в сети при условии правильно выполненных настроек.

Диапазон с 169.254.0.0 по 192.168.255.255 используется операционными системами Windows для автонастройки сетевых адаптеров. Если вы не предполагали использовать такие адреса, но обнаружили, что сетевой адаптер вашего компьютера имеет адрес из этого диапазона, следует искать проблему. Какого характера эта проблема сразу сказать трудно, но скорее всего вы допустили ошибку в настройках сети или было нарушено физическое подключение к сети.

Адреса с 192.168.0.0 по 192.168.255.0, с 172.16.0.0 по 172.31.0.0 и с 10.0.0.0 по 10.255.255.255 могут использоваться в локальных сетях. Именно для них они зарезервированы.

## Подсоединение компьютеров

Итак, есть два компьютера, есть два сетевых адаптера (в современных ПК часто встроены в материнскую плату), есть отрезок кабеля витой пары пятой категории (cat. 5 или 5e) необходимой длины, есть два коннектора (разъема) типа *RJ-45*.

Кроме перечисленного ранее потребуются обжимной инструмент для коннекторов RJ-45 или услуга по изготовлению обжатого кабеля (могут оказать в специализированных компьютерных магазинах).

Если вы решили обжимать кабель самостоятельно, то следует соблюдать некоторые правила. Есть всего два варианта распределения проводников кабеля по контактам разъемов (два варианта *разводки кабеля*). Можно придумать и другие варианты, но тогда при развитии и росте сети вы обязательно встретитесь с проблемами. Правильные варианты разводки показаны в табл. 1.5.

**Таблица 1.5.** Разводка витой пары

Стандарт EIA/TIA-568A	Стандарт EIA/TIA-568B	Номер контакта
Бело-зеленый	Бело-оранжевый	1
Зеленый	Оранжевый	2
Бело-оранжевый	Бело-зеленый	3
Синий	Синий	4

Таблица 1.5 (окончание)

Стандарт EIA/TIA-568A	Стандарт EIA/TIA-568B	Номер контакта
Бело-синий	Бело-синий	5
Оранжевый	Зеленый	6
Бело-коричневый	Бело-коричневый	7
Коричневый	Коричневый	8

Для того чтобы соединить два компьютера без использования дополнительных устройств, необходим так называемый *перекрестный кабель*. Для того чтобы изготовить такой кабель, достаточно обжать противоположные разъемы кабеля по разным вариантам стандарта EIA/TIA-568. Проводники стандартной витой пары всегда окрашены в цвета, указанные в таблице, это поможет вам не запутаться при обжиме.

Соединение компьютеров перекрестным кабелем может быть выполнено при расстоянии между компьютерами не более 100 м. Соединение компьютеров перекрестным кабелем не требует дополнительного оборудования, и все же автор рекомендовал бы выполнять соединение компьютеров через *коммутатор (switch)*. Например, очень распространены коммутаторы Comrex PS2208B, которые не требуют никакой настройки, работают полностью автоматически. Эти коммутаторы автоматически определяют вид подключения к портам. Таким образом, применив перекрестный кабель там, где требуется прямой, вы все равно получите работоспособное соединение. Но все же лучше применять кабели, соответствующие задачам подключений. Это упростит поиск неисправностей в сети, когда вы или те, кто будет разбираться в созданной вами сети, будут искать причины проблем. Применение коммутатора в простейшей сети требует использования двух обычных кабелей, у которых оба конца обжаты одинаково.

Коммутатор может быть расположен в любом месте между подключаемыми компьютерами, при этом расстояние между компьютерами может быть увеличено до 200 м. Наличие коммутатора позволит, настроив сеть из двух компьютеров, без труда подключить дополнительные компьютеры к уже созданной сети.

Подключив кабель к сетевым картам на обоих компьютерах, можно настроить сеть с помощью **Мастера настройки сети**, который присутствует как в Windows XP и во всех новых версиях Windows, так и в современных версиях Linux. Далее мы рассмотрим настройку вручную.

## Сетевые настройки компьютера под управлением ОС Windows XP

Эта операционная система постепенно уступает место Windows Vista и Windows 7. Но до сих пор компьютеры с ОС Windows XP можно приобрести, а у домашних пользователей и на предприятиях пока еще подавляющее большинство компьютеров под управлением этой ОС. Только появление Windows 7 ускорило процесс перехода с Windows XP на новую операционную систему, но процесс идет пока не столь быстро. Автору известна организация, где работают три сервера под

управлением Windows 2003 и более тридцати пользователей работают с Windows XP. Переход на новые системы пока не планируется ввиду его дороговизны. Однако надо учитывать, что официальная поддержка Windows XP планируется только до 2012 года.

1. Для начала, убедитесь, что учетная запись администратора и учетная запись обычного пользователя имеют пароли. Работая в сети без пароля, вы подвергнете компьютер опасности для непрошеного вторжения со стороны сети. А некоторые возможности сети вообще будут недоступны учетным записям пользователей без пароля.

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.

2. Откройте **Панель управления | Система** на вкладке **Имя компьютера** (рис. 1.2).

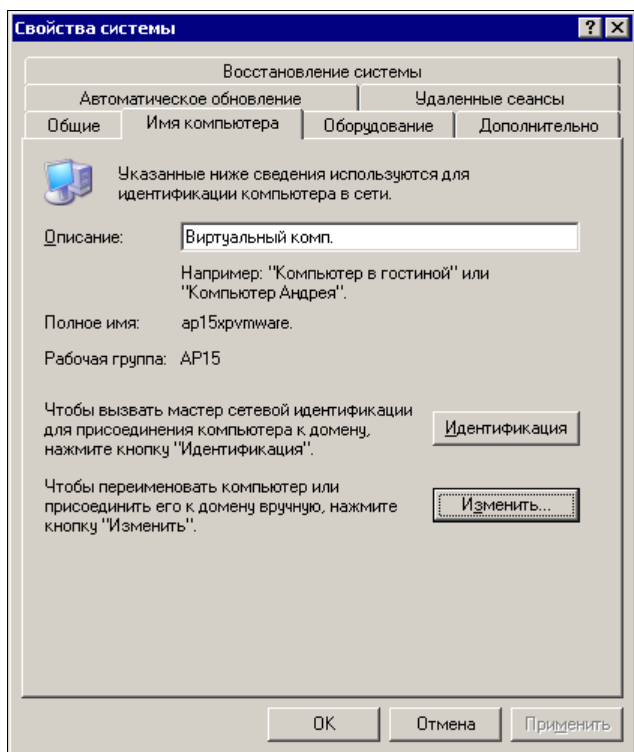


Рис. 1.2. Окно **Свойства системы**, вкладка **Имя компьютера**

3. Затем нажмите кнопку **Изменить**. Откроется окно **Изменение имени компьютера** (рис. 1.3).

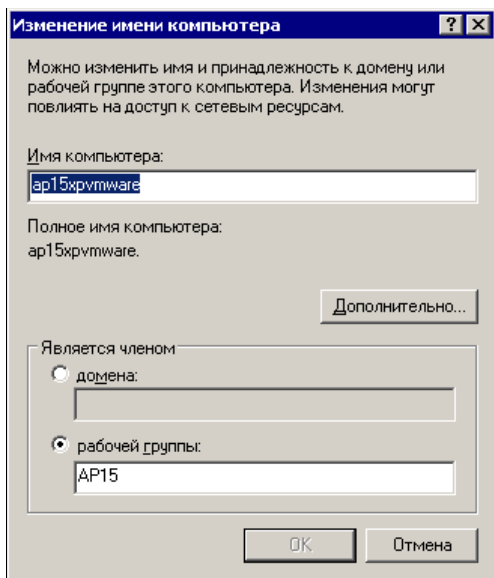


Рис. 1.3. Окно **Изменение имени компьютера**

4. В поле **Имя компьютера** необходимо ввести то имя, под которым ваш компьютер должен быть виден в сети, а в нижней части этого окна следует указать, что компьютер является членом рабочей группы, и указать имя этой рабочей группы. По умолчанию система предлагает имя WORKGROUP или MSHOME. Если вы предполагаете, 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. Следует учитывать, что имя компьютера тоже должно быть информативным.

То имя, которое вы видите на рисунке, например, говорит о принадлежности компьютера к рабочей группе ar15, 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](http://www.vmware.com/vmwarestore/newstore/wkst_eval_login.jsp)), вы можете получить ее пробную версию (объем файлов более 50 Мбайт).

Для сети не имеет значения — виртуальный компьютер подключается к ней или реальный. Все настройки для этих компьютеров идентичны. Только физически виртуальный компьютер подключен через адаптер своей хост-машины.

5. Теперь откройте **Панель управления | Сетевые подключения** (рис. 1.4).

В различных версиях Windows наименование подключения может быть представлено 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 наименование 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.

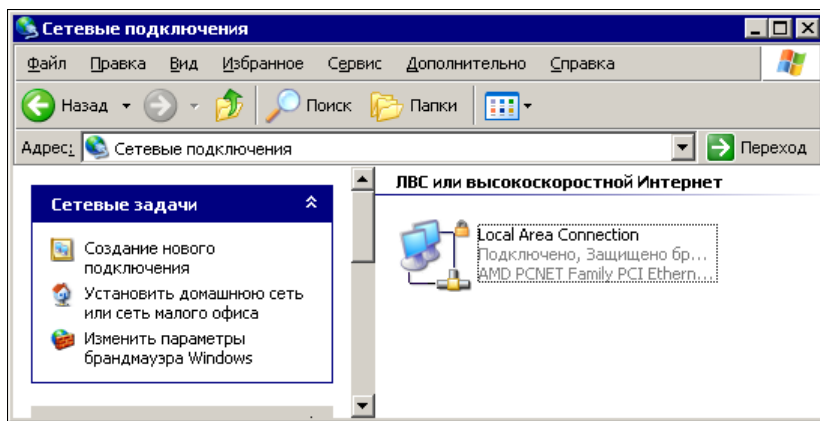


Рис. 1.4. Окно Сетевые подключения

6. Поэтому давайте переименуем наше сетевое подключение. Можно, как и в имени компьютера, применить осмысленные обозначения. Например, можно этому подключению дать имя LocalConn15.
7. Теперь, откройте свойства этого подключения (рис. 1.5).
8. На вкладке **Общие** из списка компонентов необходимо выбрать **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). После выбора они будут помечены галочками.
9. Кроме этого следует выбрать **Internet Protocol (TCP/IP)** (Протокол Интернета TCP/IP). Затем для этого пункта необходимо установить свойства, доступ к которым появляется после нажатия кнопки **Свойства** (рис. 1.6).

#### 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 рисунке. Операционная система сама будет назначать компьютеру IP-адрес. Вернитесь к окну **Сетевые подключения** и проверьте IP-адрес для подключения **LocalConn15**.

#### ПРИМЕЧАНИЕ

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

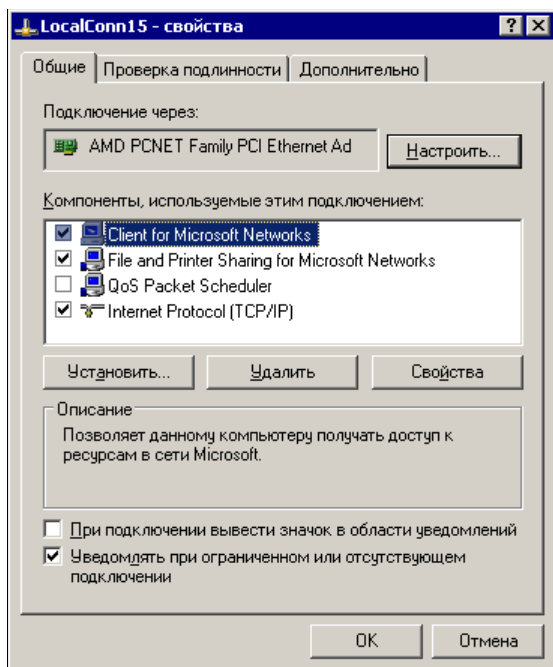


Рис. 1.5. Окно LocalConn15 — свойства

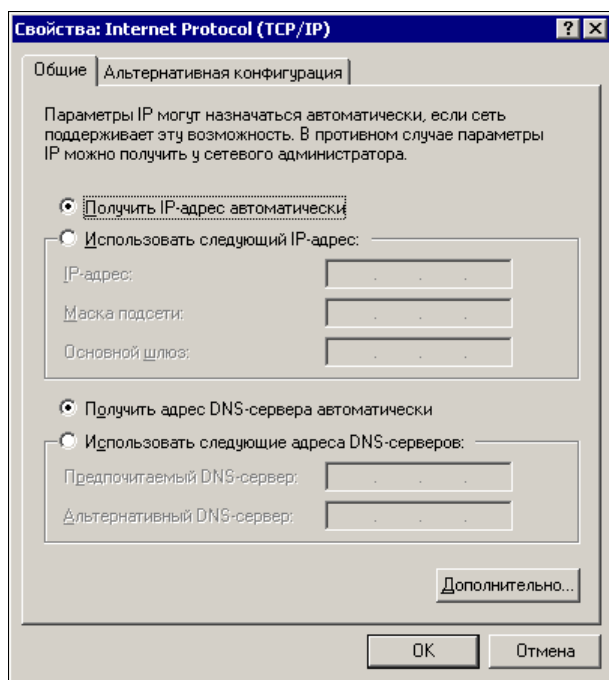


Рис. 1.6. Окно Свойства: Internet Protocol (TCP/IP)

- Для того чтобы проверить IP-адрес, присвоенный при подключении, можно открыть окно **Состояние LocalConn15** (рис. 1.7), выбрав в контекстном меню этого подключения пункт **Состояние**.

IP-адрес, который вы увидите в этом окне, может иметь различные значения, зависящие от того, в какую сеть вы включили компьютер. В любом случае, для первых компьютеров в сети (а мы сейчас настраиваем именно первый компьютер, 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.

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

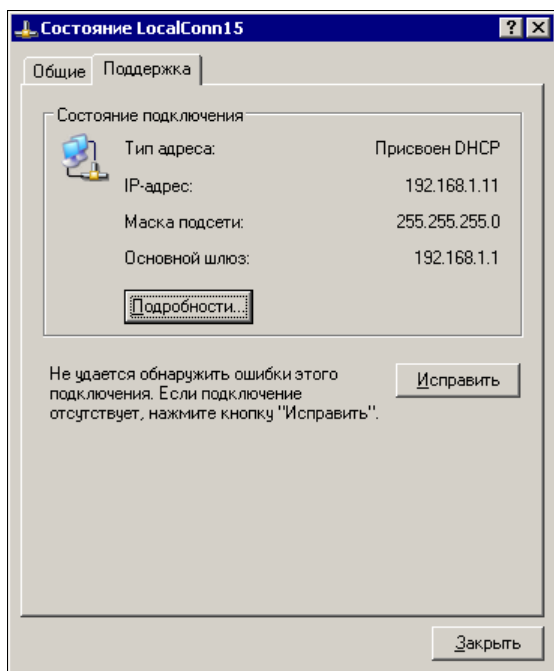


Рис. 1.7. Окно **Состояние LocalConn15**, вкладка **Поддержка**

- Для того чтобы самостоятельно назначить IP-адрес, в окне свойств подключения (см. рис. 1.6) выберите опцию **Использовать следующий IP-адрес** и в поле **IP-адрес** 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** (см. рис. 1.7) есть кнопка **Подробнее**. Среди сведений, которые открываются при нажатии на эту кнопку, 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. 1.8). На вкладке **Доступ** установите флажки **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.

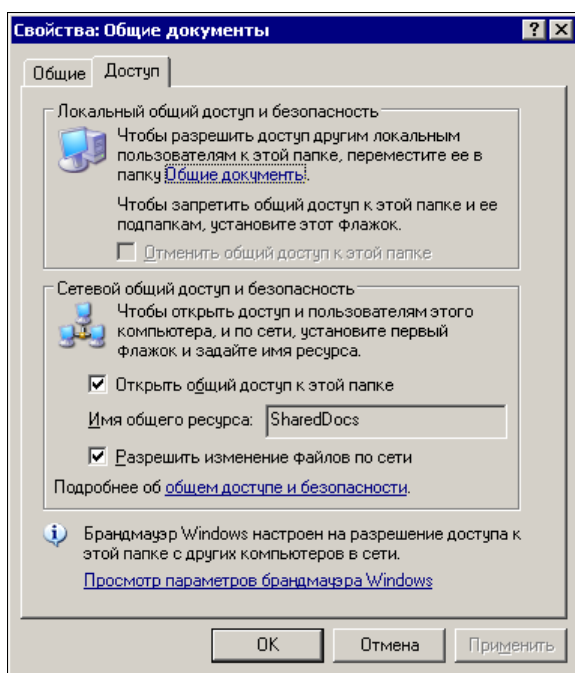


Рис. 1.8. Окно **Свойства: Общие документы**

- Теперь остается повторить все настройки на втором компьютере сети. Подключая второй компьютер, 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 в сетевом окружении оба компьютера (рис. 1.9).

- Откройте тот, что для вас удаленный. Вы увидите доступные по сети ресурсы этого компьютера (рис. 1.10).

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 подведено питание.

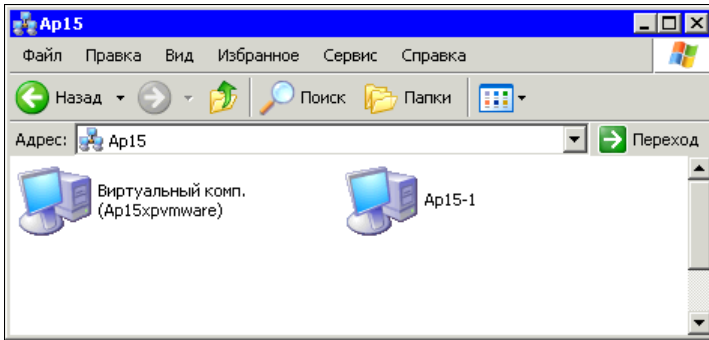


Рис. 1.9. Окно **Ap15** — сетевое окружение рабочей группы Ap15

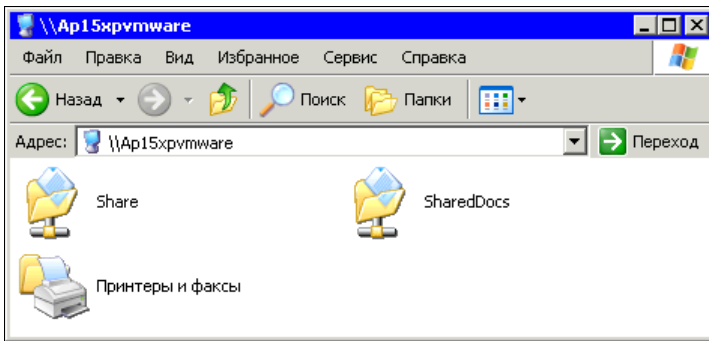


Рис. 1.10. Окно **\\Ap15xrvnware** — доступное по сети содержимое первого сетевого компьютера

## Если не заработало

Вполне возможно, что результат не получился. В чем может быть проблема? Схема нашей сети проста (рис. 1.11).

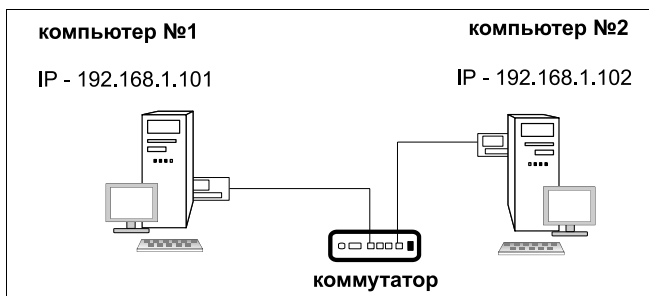


Рис. 1.11. Схема нашей сети

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

Настройки *брандмауэра* находятся в **Панель управления | Брандмауэр Windows** (рис. 1.12).

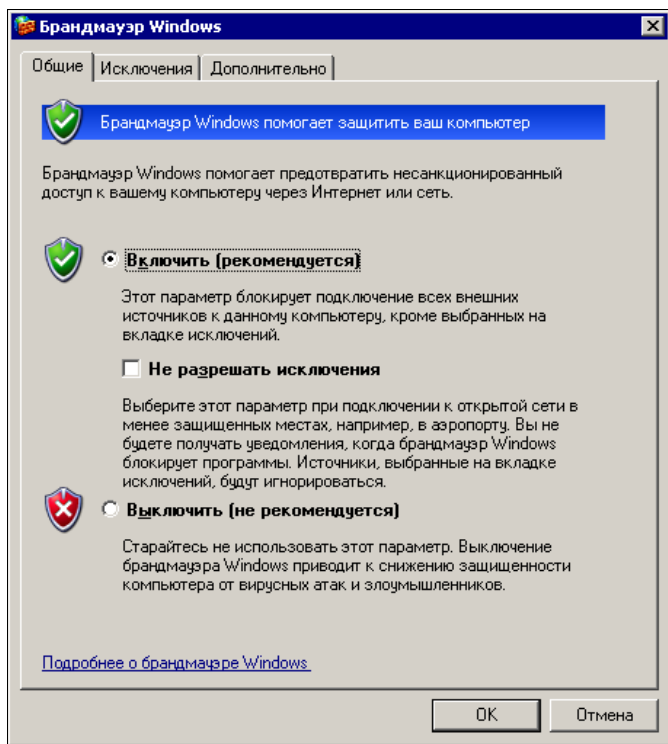


Рис. 1.12. Окно **Брандмауэр Windows**

Отключите брандмауэр, выбрав соответствующий переключатель, согласившись с тревожными предупреждениями операционной системы. Если сразу после этого все заработало, то на вкладке **Исключения** этого окна в списке программ и служб выберите **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 работаете с компьютером № 1. Результат выполнения команды должен быть подобен тому, что показан на рис. 1.13.

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

```

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

C:\Documents and Settings\Julia>ping 192.168.1.101

Обмен пакетами с 192.168.1.101 по 32 байт:

Ответ от 192.168.1.101: число байт=32 время=4мс TTL=128
Ответ от 192.168.1.101: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.101: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.101: число байт=32 время=4мс TTL=128

Статистика Ping для 192.168.1.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 4 мсек, Среднее = 2 мсек

C:\Documents and Settings\Julia>

```

Рис. 1.13. Окно командной строки, результат выполнения команды ping

Если ответ на команду ping по локальному адресу положительный, то проверяем состояние сетевого адаптера через диспетчер устройств. В диспетчере устройств для сетевых устройств не должно быть вопросов желтого цвета. Если есть такие вопросы, то переустанавливаем драйверы сетевого адаптера. Правильно установив верный драйвер, проверяем работу сети.

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

Если проблем с оборудованием не обнаружено, кабельную сеть заменяем временными, но заведомо исправными патчкордами.

#### ПРИМЕЧАНИЕ

*Патчкорд* — отрезок кабеля, с двух сторон обжатым разъемом RJ-45, служит для подключения конечного оборудования к сетевому оборудованию или абонентской розетке.

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 приступить к эксплуатации сети.

## Сетевые настройки компьютера под управлением ОС Windows Vista

Множество вариантов режимов работы компьютера в сети требуют каждый раз индивидуального подхода. Старайтесь вникать в суть производимых действий,

чтобы незначительно изменившиеся условия не могли сбить вас с толку и помешать выполнению требуемых операций.

Что же необходимо выполнить для того, чтобы компьютер под управлением ОС Windows Vista заработал в вашей сети?

### ПРИМЕЧАНИЕ

Описание настроек приведено для классического стиля меню **Пуск** ОС Windows. Если вы не знаете, как настроить вашу систему для классического стиля отображения меню **Пуск**, воспользуйтесь встроенной справкой.

1. Подключите компьютер к сети.
2. Нажмите кнопку **Пуск**.
3. Выберите **Настройка | Панель управления**.
4. В открывшемся окне **Панель управления** (рис. 1.14) найдите значок **Центр управления сетями и общим доступом** (на рисунке нижний ряд в центре).

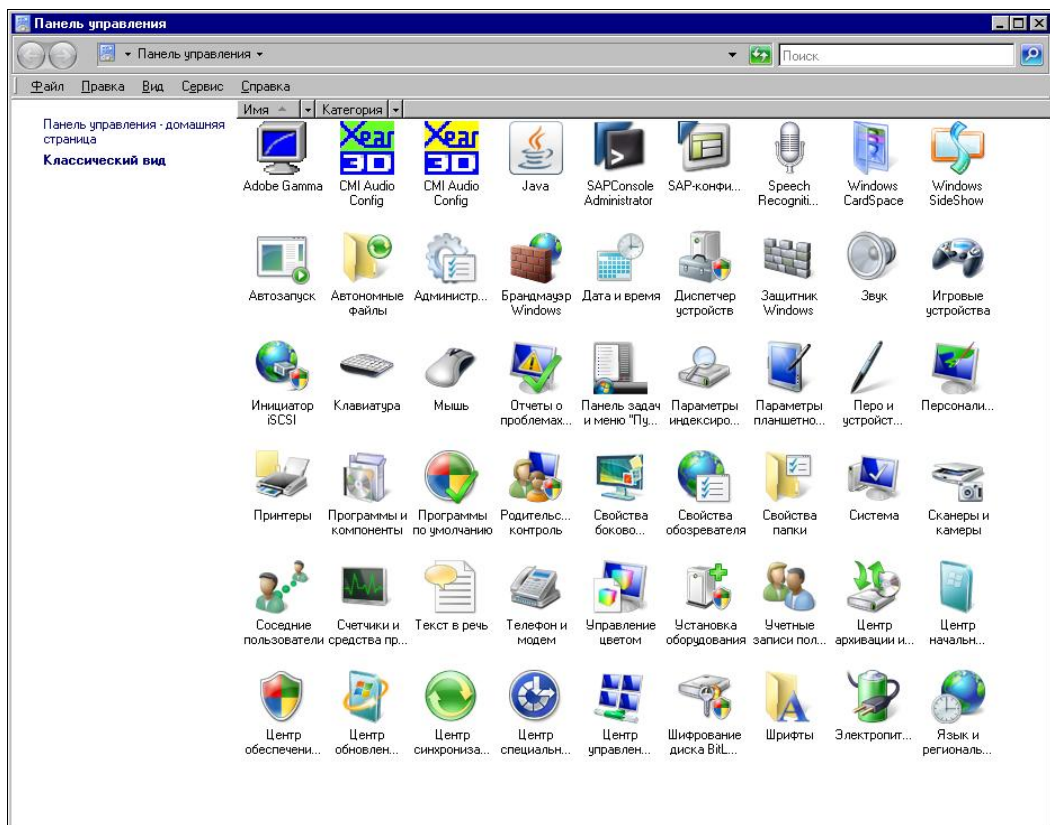


Рис. 1.14. Окно Панель управления

5. Двойным щелчком (если у вас не настроено иное поведение мыши) по этому значку откройте одноименное окно (рис. 1.15).

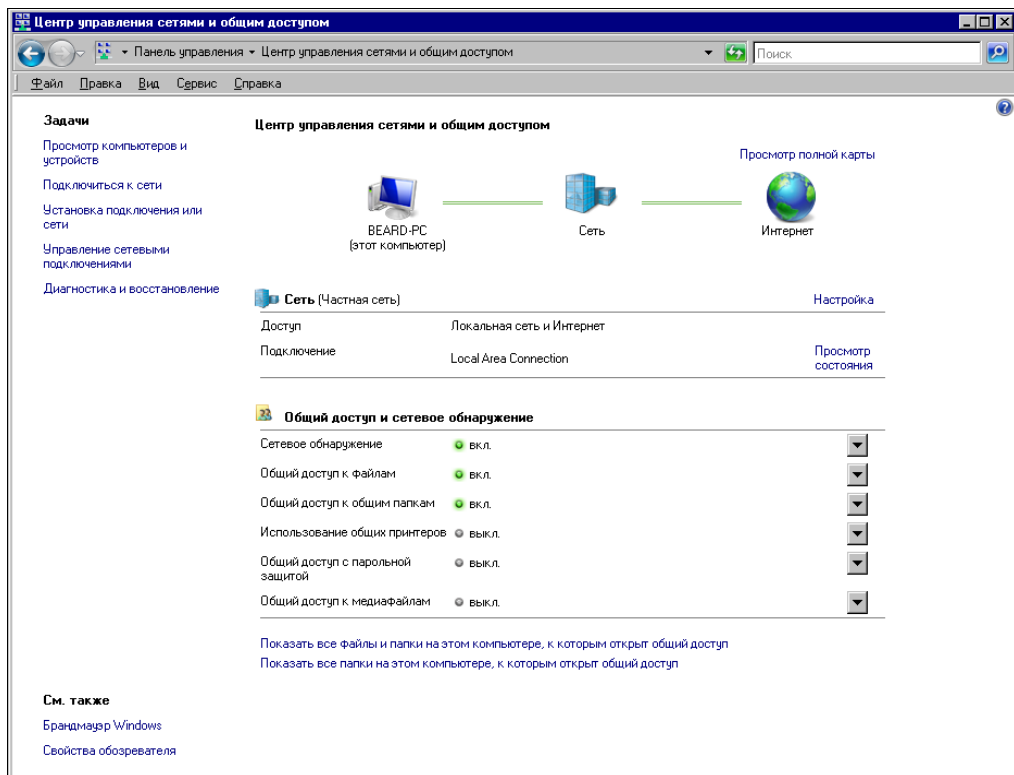


Рис. 1.15. Окно **Центр управления сетями и общим доступом**

6. Если компьютер еще ни разу не был подключен к сети, можно воспользоваться пунктом меню в левой части окна — **Подключиться к сети**. В других случаях выберите пункт **Управление сетевыми подключениями**.

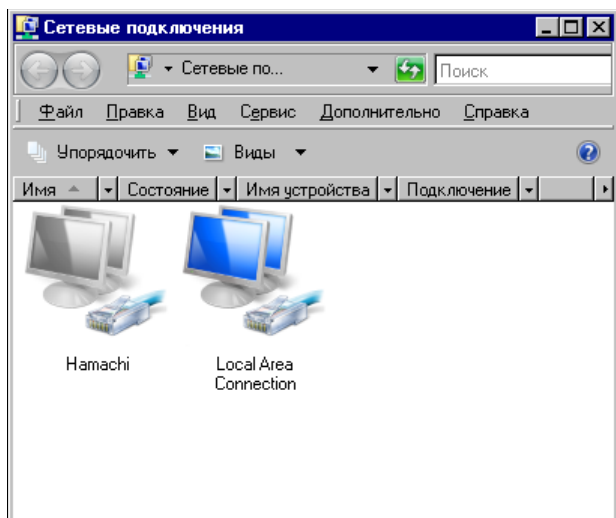
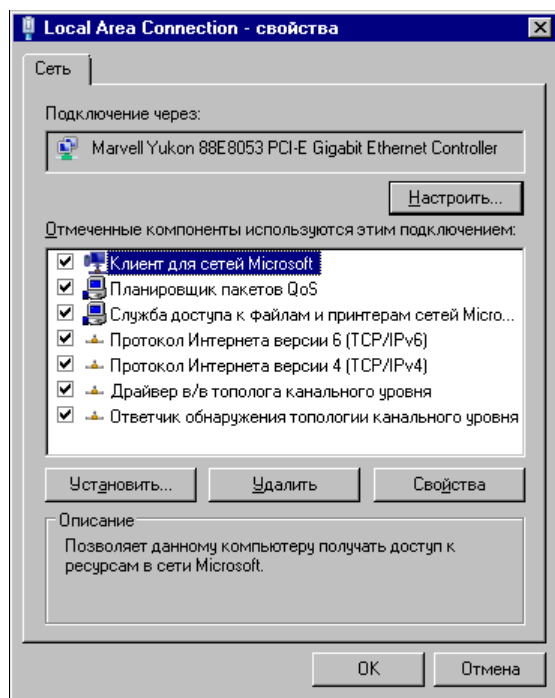
7. В открывшемся окне **Сетевые подключения** (рис. 1.16) вы увидите имеющиеся на данный момент сетевые подключения вашего компьютера. Найдите значок **Local Area Connection** (Подключение по локальной сети).

8. Щелкните по этому значку правой кнопкой мыши и в контекстном меню выберите пункт **Свойства**.

В верхней части открывшегося окна **Local Area Connection — свойства** (рис. 1.17) вы увидите имя вашего сетевого адаптера. Ниже находится перечень компонентов, которые можно настроить, открывая соответствующие окна кнопкой **Свойства** или **Установить**.

9. Откройте окно свойств компонента **Клиент для сетей Microsoft** кнопкой **Свойства**. В открывшемся окне **Свойства: Клиент для сетей Microsoft** (рис. 1.18) в выпадающем списке поля **Поставщик службы имен** выберите **Локатор Windows**.

Поскольку наша сеть не содержит серверов имен, которые необходимы в больших сетях, сама операционная система будет просматривать сеть и собирать информацию об именах, имеющихся в ней сетевых устройств.

Рис. 1.16. Окно **Сетевые подключения**Рис. 1.17. Окно **Local Area Connection — свойства**

10. Если вы не видите у себя компонент **Служба доступа к файлам и принтерам сетей Microsoft** (см. рис. 1.17), вставьте диск с дистрибутивом системы и, нажав кнопку **Установить**, установите эту службу. Настроек она не требует.
11. Перейдите к компоненту **Протокол Интернета версии 4 (TCP/IPv4)** (см. рис. 1.17). Нажмите кнопку **Свойства** (рис. 1.19).

На рисунке приведены параметры настройки для конкретной сети, в которой работает мой компьютер. Ваши настройки могут быть иными.

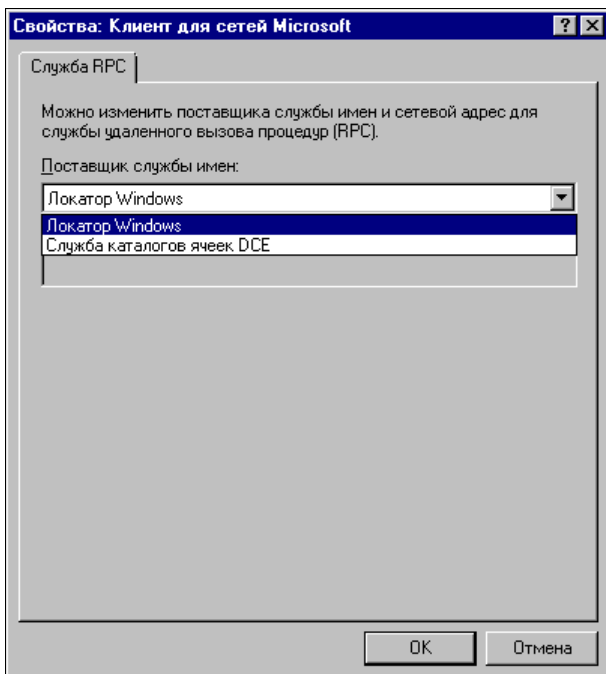


Рис. 1.18. Окно Свойства: Клиент для сетей Microsoft

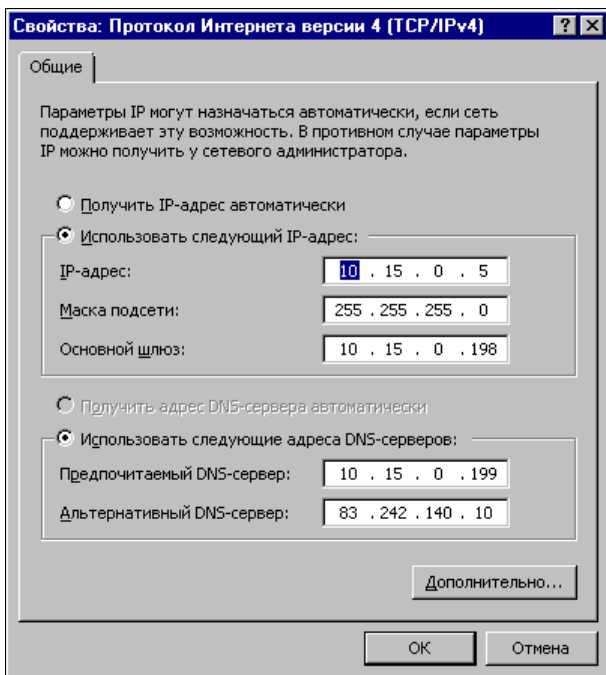


Рис. 1.19. Окно Свойства: Протокол Интернета версии 4 (TCP/IPv4)



Опишем основные варианты, с которыми вам, возможно, придется столкнуться. Во-первых, адреса DNS-серверов вам потребуются только для обеспечения возможности работы в Интернете. Провайдер должен предоставить вам эти адреса при подключении или они будут назначаться автоматически. Автоматическое получение адресов DNS-серверов возможно при автоматическом получении IP-адреса самого компьютера. В маленькой сети есть смысл использовать статические (назначенные вручную) IP-адреса. Вы можете использовать любые адреса из диапазона зарезервированных адресов сетей класса "С" (с 192.168.0.0 по 192.168.255.0) или из диапазона зарезервированных адресов сетей класса "А", кроме адресов с 127.0.0.0 по 127.255.255.255. При этом маска подсети будет назначаться в зависимости от числа компьютеров и других узлов в вашей сети. Предположим, что вы планируете приобрести пять компьютеров для всех членов семьи. Сами при этом предполагаете иметь три компьютера. Возможно, что вы будете использовать какой-нибудь маршрутизатор и другие сетевые устройства, для которых потребуются IP-адреса. Вероятно, что в любом случае вам будет достаточно 15 адресов. Посмотрев в таблицу (табл. 1.5), можно найти маску 255.255.255.240/28, применив которую можно создать 16 подсетей с 16-ю адресами в каждой. Если вы выбрали сеть класса "С", то диапазоны адресов в вашей сети могут быть следующими:

192.168.0.0—192.168.0.15, или 192.168.0.16—192.168.0.31, или 192.168.0.32—192.168.0.47 и т. д.

Для сети класса "А" это адреса 10.1.0.0—10.1.0.15, или 10.1.0.16—10.1.0.31, или 10.1.0.32—10.1.0.47 и т. д. Цифры во втором и третьем октете адреса могут быть иными, например, 10.123.123.X.

Если вам пока сложно выбрать необходимый диапазон адресов для вашей сети, то вам подойдет следующий вариант 192.168.0.0—192.168.0.255 с маской 255.255.255.0. В этой сети может быть 254 узла. Для домашней сети это много, но некоторые автоматические настройки сети Windows рассчитаны именно на этот диапазон. Как вариант, можно рекомендовать 192.168.0.0—192.168.0.15 с маской 255.255.255.240. Иногда выбор диапазона адресов для домашней сети зависит от применяемого оборудования для подключения к Интернету. Например ADSL<sup>1</sup>-модем D-Link 500T имеет собственный адрес 192.168.1.1, что вынуждает использовать диапазон 192.168.1.0—192.168.1.255 с маской 255.255.255.0 или 192.168.1.0—192.168.1.15 с маской 255.255.255.240. Эти диапазоны могут быть записаны с применением расширений масок как 192.168.1.0/24 и 192.168.1.0/28.

В любом случае не следует для компьютеров применять крайние значения диапазонов адресов. Начальный адрес диапазона это адрес сети, а конечный — адрес широковещательной рассылки.

Пока у вас всего два компьютера, не будет больших проблем при ошибочном выборе их адресов. Вы всегда сможете исправить ошибку достаточно оперативно. Поэтому смелее выбирайте приглянувшийся диапазон и назначайте адрес своему компьютеру. Адрес основного шлюза можно не указывать, если такового в вашей сети нет. Им может быть упомянутый выше ADSL-модем, например.

---

<sup>1</sup> ADSL — Asymmetrical Digital Subscriber Line — асимметричная цифровая абонентская линия.

## Сетевые настройки компьютера под управлением ОС Linux

В последнее время у пользователей ПК постоянно растет интерес к ОС Linux. Многие заинтересованно рассматривают уже установленную систему у своих товарищей, но не решаются установить ее у себя. Автор опробовал в своих сетях несколько известных дистрибутивов этой ОС. Можно отметить определенные отличия в них, но по большому счету работа с Linux в любой современной версии одинаково комфортна. Выбор дистрибутива в большой мере — дело вкуса, тем не менее, при его выборе следует обратить внимание на год его создания. Чем новее дистрибутив, тем больше вероятность, что в нем будут содержаться драйверы для нового оборудования, и большее число программ, не входящих в поставку, можно будет установить без проблем. Дистрибутивы могут быть совершенно бесплатными. Но в платных версиях Linux, как правило, содержатся более совершенные драйверы устройств и некоторые дополнительные возможности, такие, например, как бесплатная поддержка от разработчиков.

Установка системы не сложнее, чем установка Windows. Но есть некоторые особенности. Если на диске уже есть операционная система, программа установки будет задавать наводящие вопросы и может сама выбрать место для Linux, оставив возможность двойной загрузки. Но если вы никогда не устанавливали Linux, лучше провести первую установку на отдельный винчестер.

Настройка сети может быть выполнена еще на этапе установки системы.

В качестве примера рассмотрим одну из новейших версий Mandriva Linux 2008.

В данном примере предполагается, что уже существует локальная сеть Ethernet с шлюзом в Интернет.

1. На экране **Сводка** (рис. 1.20), который выводится во время установки на этапе настройки оборудования, нажимаем кнопку **Настройка** напротив строки **Сеть-ethernet**.
2. На следующем экране (рис. 1.21) выбираем Ethernet, нажимаем кнопку **Далее**, и на появившемся экране (рис. 1.22) выбираем настройку вручную, нажимаем **Далее** и вводим необходимые параметры сети и локального компьютера на экране (рис. 1.23).

Можно настроить сеть и после установки системы.

1. Для этого достаточно открыть **Система | Администрирование | Настройка компьютера | Сетевой центр**.
2. В открывшемся окне **Центр управления Mandriva Linux — Сетевой центр** нажмите кнопку **Настройка** под строкой используемого сетевого адаптера (их может быть больше одного). Откроется окно **Параметры сети**, в котором вы увидите поля для ввода уже знакомых параметров (рис. 1.24).
3. Для указания имени компьютера в окне **Центр управления Mandriva Linux** откройте **Имена узлов**, в открывшемся одноименном окне (рис. 1.25) введите его, нажав кнопку **Добавить**, или измените существующее имя, нажав кнопку **Изменить**.

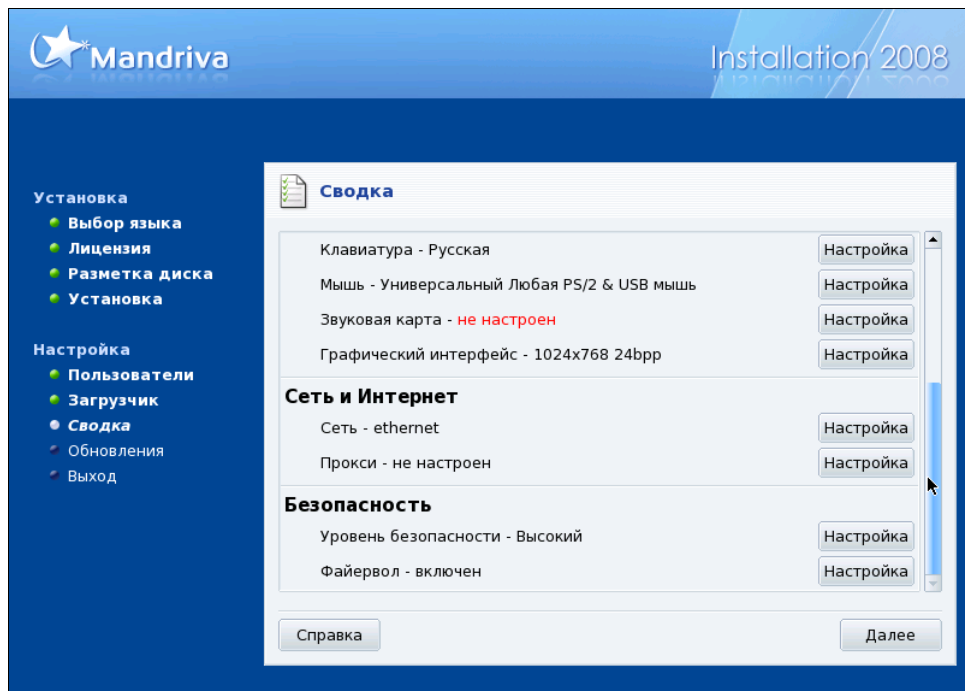


Рис. 1.20. Установка Linux, экран Сводка

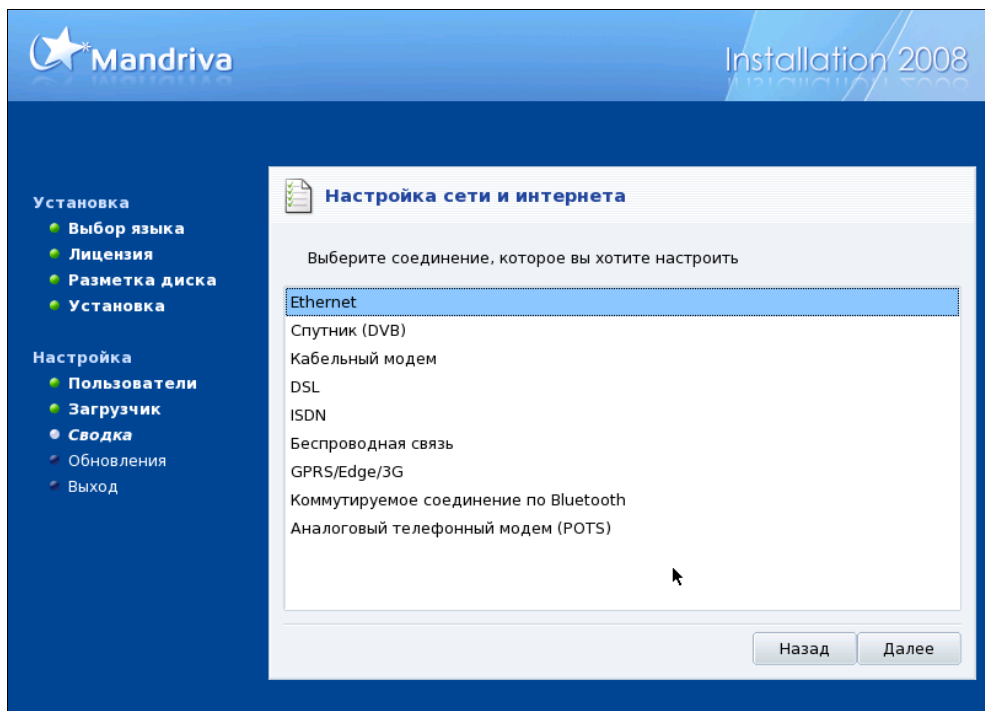


Рис. 1.21. Установка Linux, экран Настройка сети и интернета (выбор соединения)

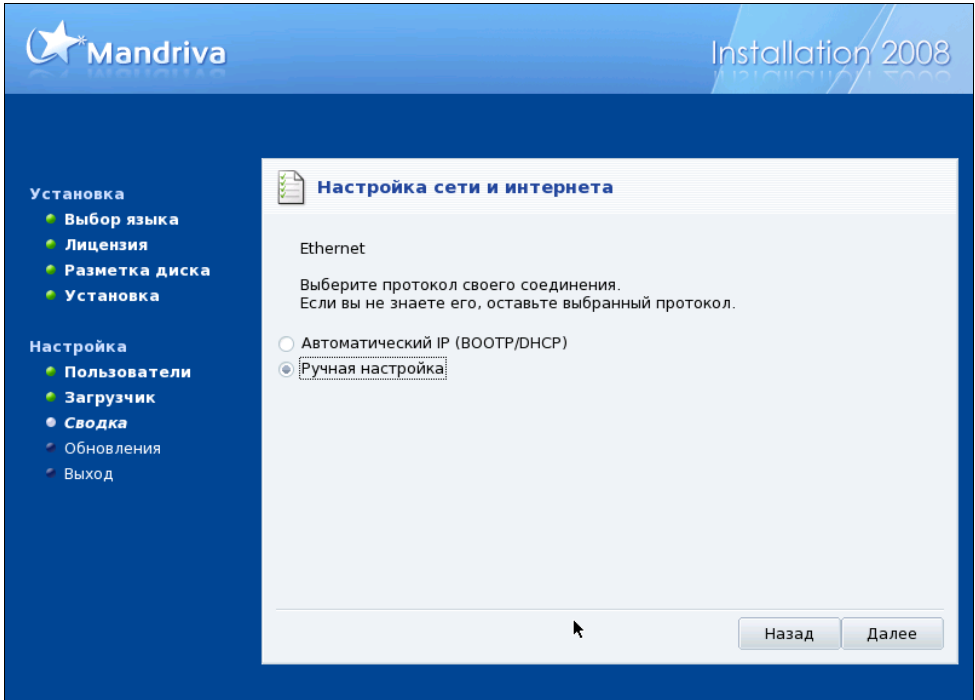


Рис. 1.22. Установка Linux, экран **Настройка сети и интернета** (Ethernet)

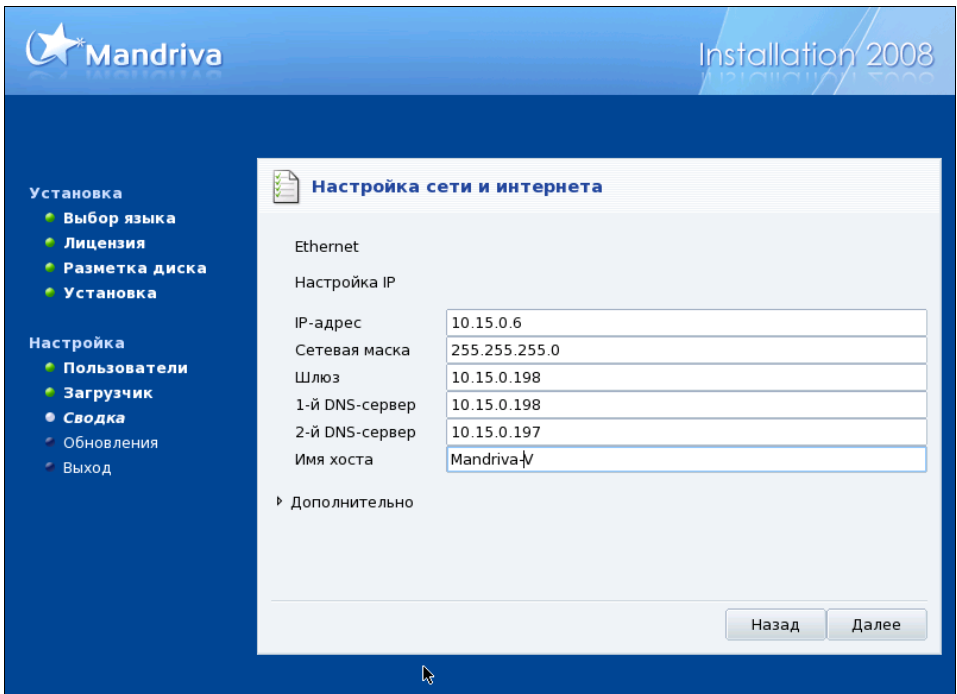


Рис. 1.23. Установка Linux, экран **Настройка сети и интернета** (Ethernet — Настройка IP)

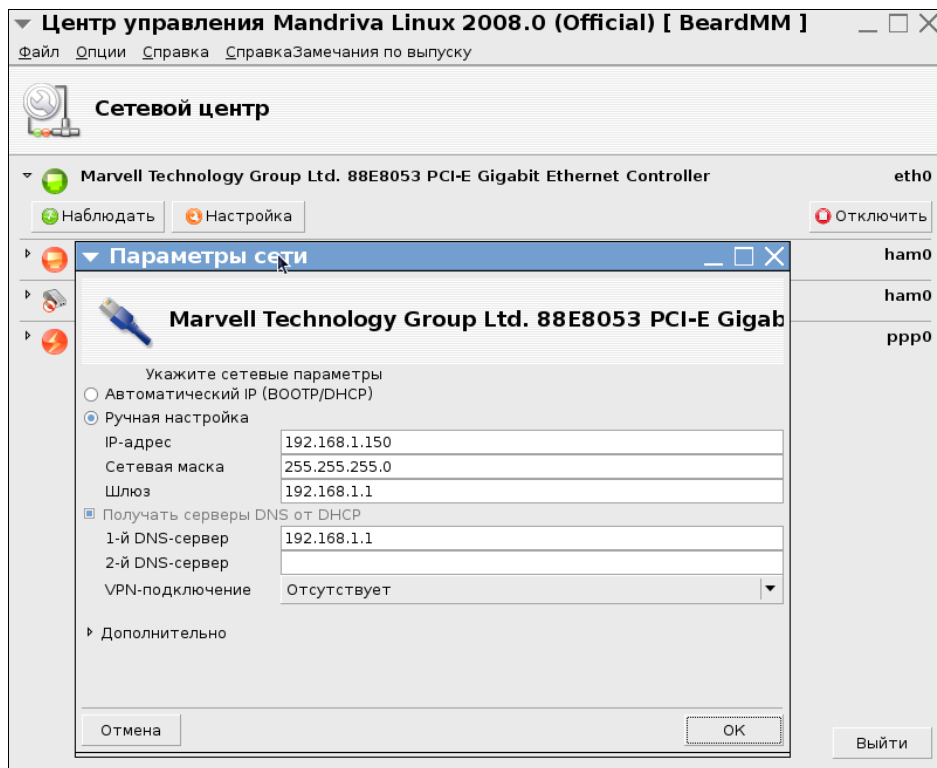


Рис. 1.24. Окна Центр управления Mandriva Linux — Сетевой центр и Параметры сети

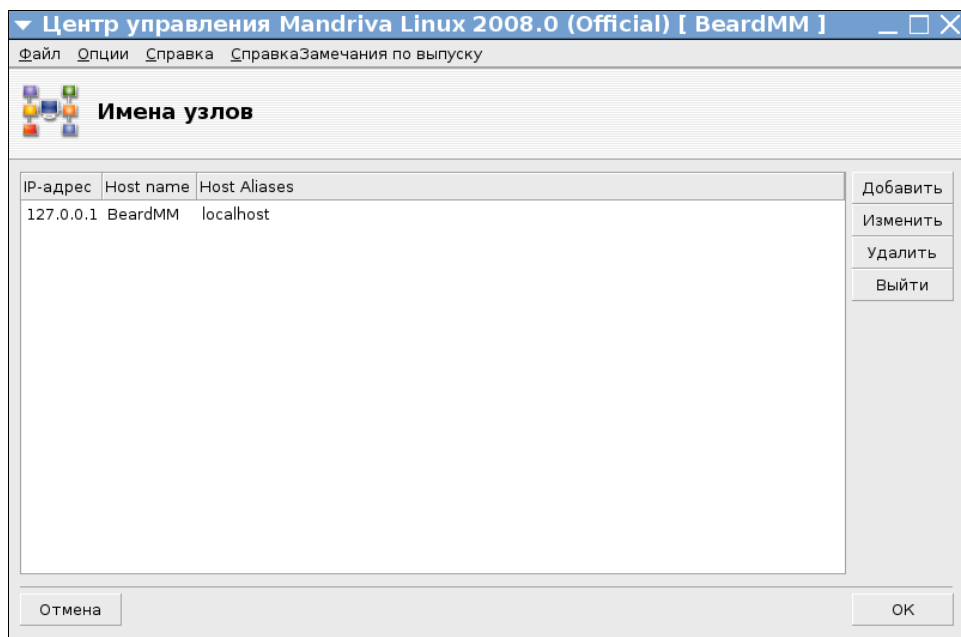


Рис. 1.25. Окно Центр управления Mandriva Linux — Имена узлов

Настройка рабочей станции под управлением другой версии Linux ASP Linux для работы в сети так же не сложна. Ознакомившись с несколькими версиями Linux, вы поймете, что работать можно в любой из них одинаково комфортно. Далее приведу процедуру настройки Linux ASP Linux.

1. Подключите компьютер к сети.
2. Нажмите кнопку **Система** (рис. 1.26).

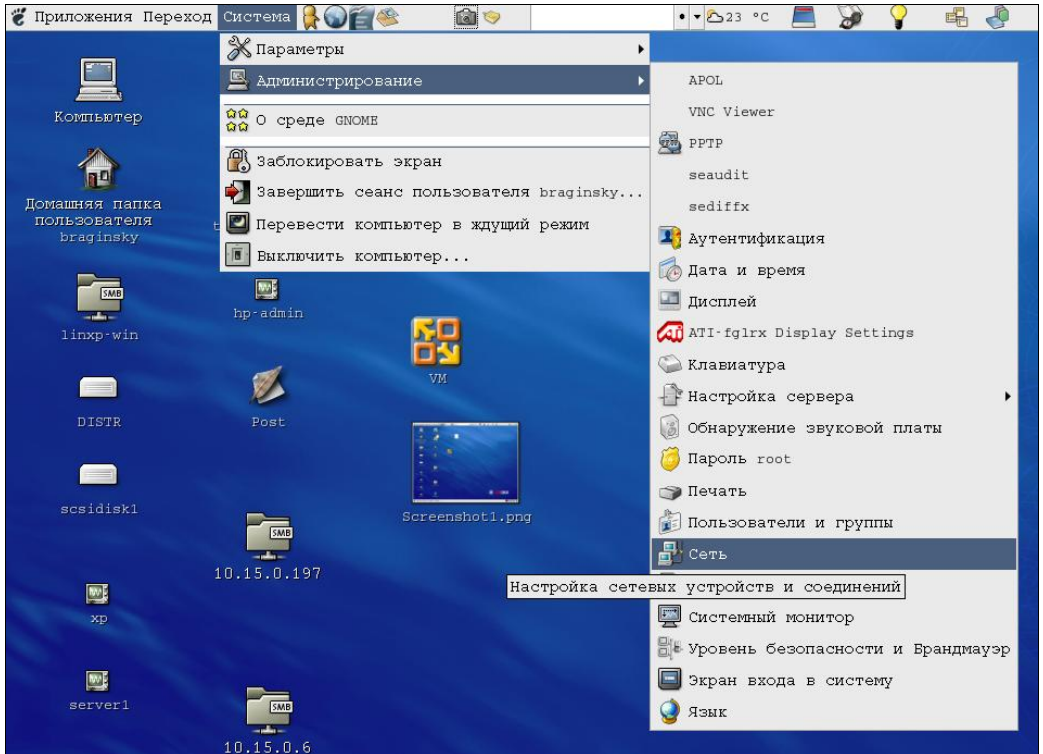


Рис. 1.26. Рабочий стол ASPLinux 11.2 (фрагмент) — выбор меню **Сеть**

3. Выберите **Администрирование | Сеть**.
4. В открывшемся окне **Запрос** (рис. 1.27) введите пароль администратора системы. Откроется окно **Настройка сети** (рис. 1.28).

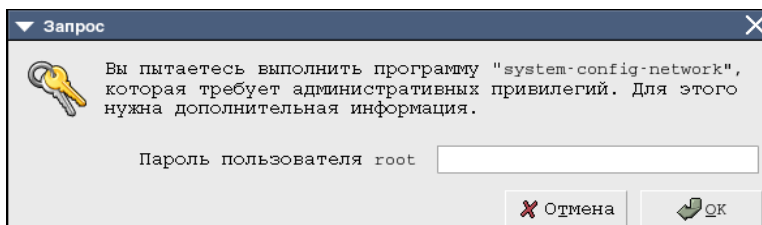


Рис. 1.27. Окно **Запрос** — ввод пароля администратора

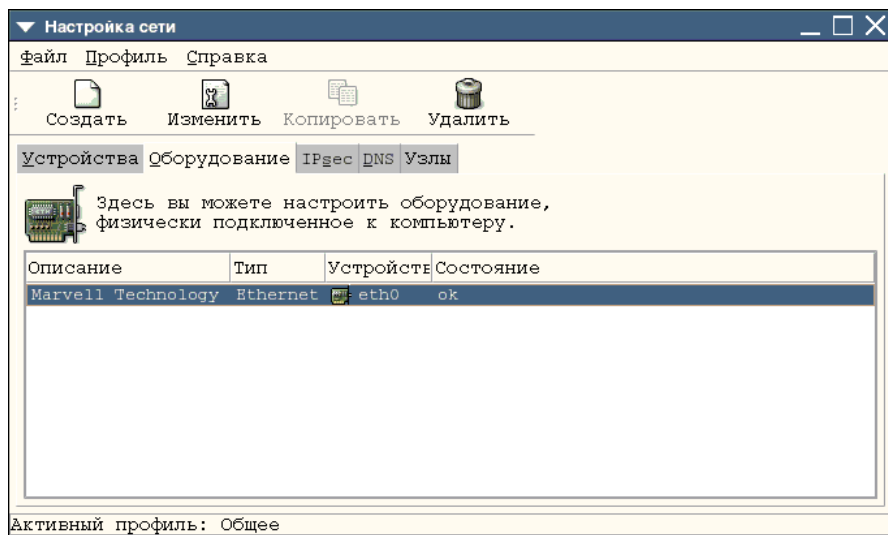


Рис. 1.28. Окно Настройка сети

5. На вкладке **Оборудование** этого окна вы должны увидеть ваш сетевой адаптер, который определен во время установки системы.
6. На вкладке **Устройства** этого окна с помощью кнопки **Создать** создайте новое устройство (аналог подключения в Windows), которое далее в окнах для ввода параметров будет именоваться как **Новое Соединение**. В них выберите тип соединения Ethernet и имя вашей сетевой карты.
7. Теперь в окне **Настройка сети** на вкладках **DNS** и **Узлы** укажите необходимые IP-адреса.
8. В свойствах подключения (кнопка **Изменить**) укажите IP-адрес рабочей станции, маску подсети и адрес основного шлюза, если это необходимо. Или оставьте вариант **Автоматически получить адрес IP при помощи dhcp**.
9. Согласитесь с предложением системы сохранить настройки.

Вы можете создать несколько соединений с различными параметрами для разных сетей. Это может быть полезно для ноутбуков. Аналогично Ethernet-соединению, вы можете настроить и модемное соединение. Если модем внешний, то не потребуются драйверы для него, но устройство необходимо создать, указав имя /dev/ttyS0, где S0 соответствует порту COM1.

Для подключения к сетевым каталогам достаточно в меню **Файл** любого локального каталога выбрать пункт **Соединиться с сервером** и указать в окне **Соединение с сервером** тип сервиса **Ресурс ОС Windows**, сетевое имя или IP-адрес компьютера. На рабочем столе будет создан значок сетевого каталога. В процессе создания сетевого каталога потребуется авторизация на удаленном компьютере.

Настроив свои компьютеры для работы в сети, вы сможете совместно использовать файлы. Для просмотра сохраненного видео, например, не потребуется делать копию фильма и переносить ее на другой компьютер. Достаточно открыть имею-

щийся файл из общего сетевого каталога, но при необходимости его можно скопировать. Однако рассмотрим все по порядку.

## Настраиваем общий доступ к файлам и папкам в Windows Vista

Для настройки общего доступа к файлам и папкам выполните следующее:

1. Откройте из **Панели управления** окно **Центр управления сетями и общим доступом**, в котором найдите задачу **Просмотр компьютеров и устройств**. Откроется окно **Сеть** (рис. 1.29).

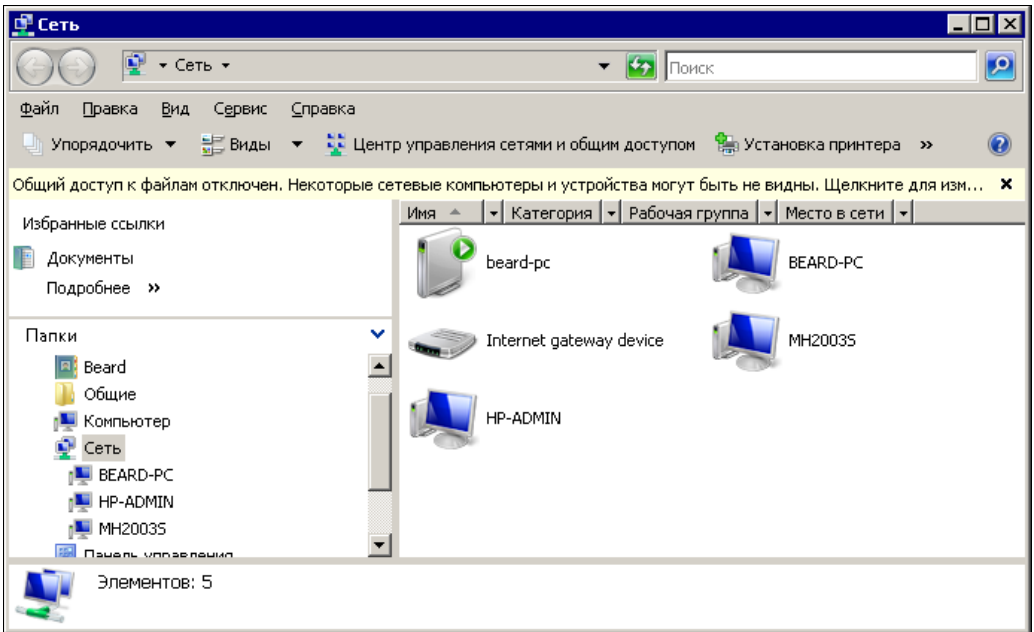


Рис. 1.29. Окно **Сеть**

В окне **Сеть** вы увидите устройства, обнаруженные системой в сети. При отсутствии общего доступа к файлам в верхней части окна вы увидите сообщение, которое предупреждает об отсутствии общего доступа к файлам и проблемах, связанных с этим.

2. Щелкнув это сообщение, вы увидите меню, содержащее три пункта, первый из которых предлагает включить сетевое обнаружение и общий доступ к файлам. Воспользуйтесь этим предложением. Придется, как обычно в ответственных случаях, подтвердить свое желание выполнить это действие, и общий доступ будет включен.
3. Теперь можно выбрать папки, которые вы хотели бы предоставить в общий доступ в сети. В свойствах выбранных папок можно назначить общий доступ к ним, установив необходимые разрешения для пользователей сети. Процедура не



сложная, но следует иметь в виду, что все пользователи одноранговой сети, которую мы создали, должны иметь учетные записи на каждом компьютере, к которому они хотят иметь доступ из сети. После настройки общего доступа в окне **Сеть** вы сможете открывать компьютеры, получая доступ к разрешенным папкам.

Управлять общим доступом к папкам можно и из окна **Центр управления сетями и общим доступом** из раздела **Общий доступ и сетевое обнаружение**, устанавливая необходимые параметры доступа, воспользовавшись кнопками со стрелками.

Когда общий доступ включен, можно добавлять папки и файлы, к которым обеспечивается общий доступ. Лучше для этого создать специальные папки, в которые вы будете помещать файлы, доступ к которым необходим по сети. Это исключит возможность доступа к вашим личным файлам, просмотр которых другими пользователями не желателен для вас. Учитывая, что каталоги и файлы могут быть доступны из различных операционных систем, имена им следует присваивать, используя латиницу. Кириллические имена файлов могут оказаться нечитаемыми при просмотре их по сети. Это связано с тем, что в различных операционных системах могут применяться разные кодовые страницы для системных шрифтов.

Следует также иметь в виду, что в Linux прописные и строчные символы в именах файлов и папок считаются разными символами. Если для Windows папки с именами "Share" и "share" неотличимы для системы, и в одном родительском каталоге нельзя создать две таких папки, то в Linux это возможно. То же и при поиске файлов и папок в сети. Windows найдет папку share, если в качестве параметра поиска будет задано имя Share, а Linux в аналогичной ситуации будет искать только имя Share.

## Пример создания каталога общего доступа в Windows Vista

В Windows Vista папки пользователя собраны в одном каталоге с именем этого пользователя. Именно в этом каталоге рекомендуется создавать любые новые папки. Обратите внимание на то, что если в Windows Vista имя учетной записи пользователя изменено после ее создания, в главном меню пункт для доступа к папке пользователя будет иметь новое имя, а сама папка — старое. Так, на компьютере автора продавцами была создана учетная запись с именем "I", которая впоследствии переименована в "Beard". Вы можете использовать любые имена для своих учетных записей, заменяя ими те, что использовал автор.

Создадим для учетной записи Beard каталог с общим доступом. Для этого выполним следующее:

1. Откроем папку пользователя **Пуск | Документы | Beard** (рис. 1.30).
2. Создадим вложенную папку Share, откроем окно ее свойств и перейдем на вкладку **Доступ** (рис. 1.31).

На этой вкладке можно увидеть две кнопки — **Общий доступ** и **Дополнительный доступ**.

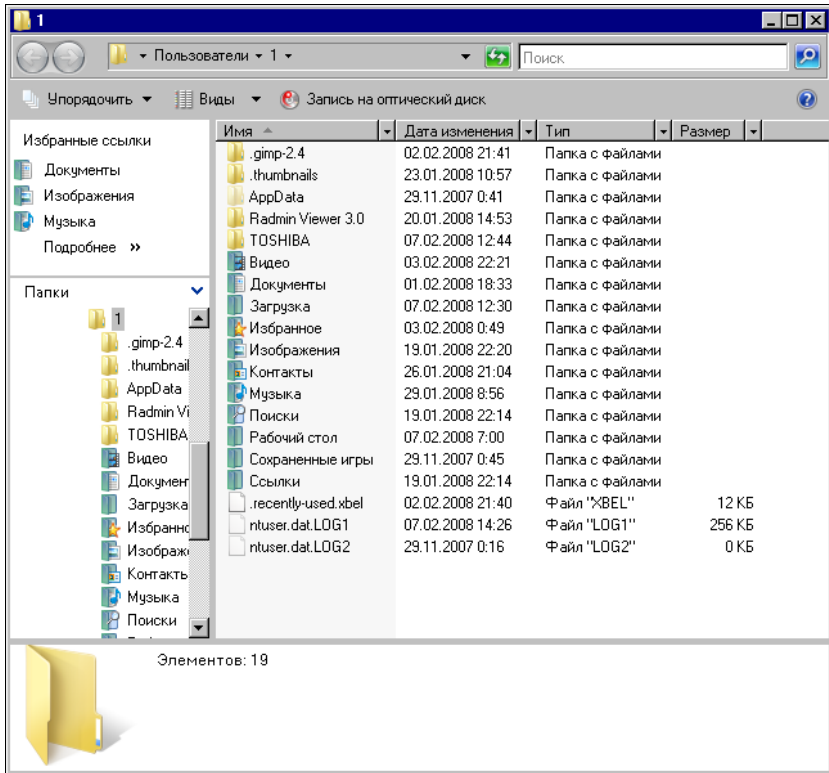


Рис. 1.30. Окно 1 (папка текущей учетной записи)

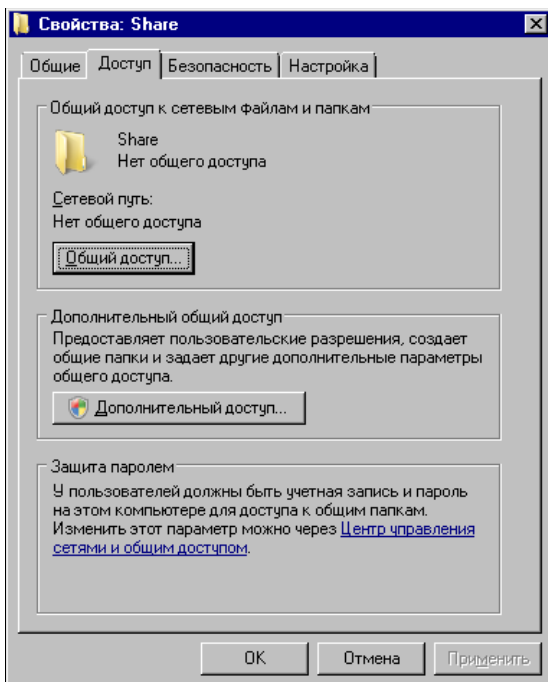


Рис. 1.31. Окно Свойства: Share, вкладка Доступ

3. Воспользуемся кнопкой **Общий доступ**. Откроется окно **Общий доступ к файлу**, в котором следует нажать кнопку **Доступ**. В течение нескольких секунд или минут система настроит возможность общего доступа к каталогу. При успешном завершении операции появляется соответствующее сообщение (рис. 1.32).

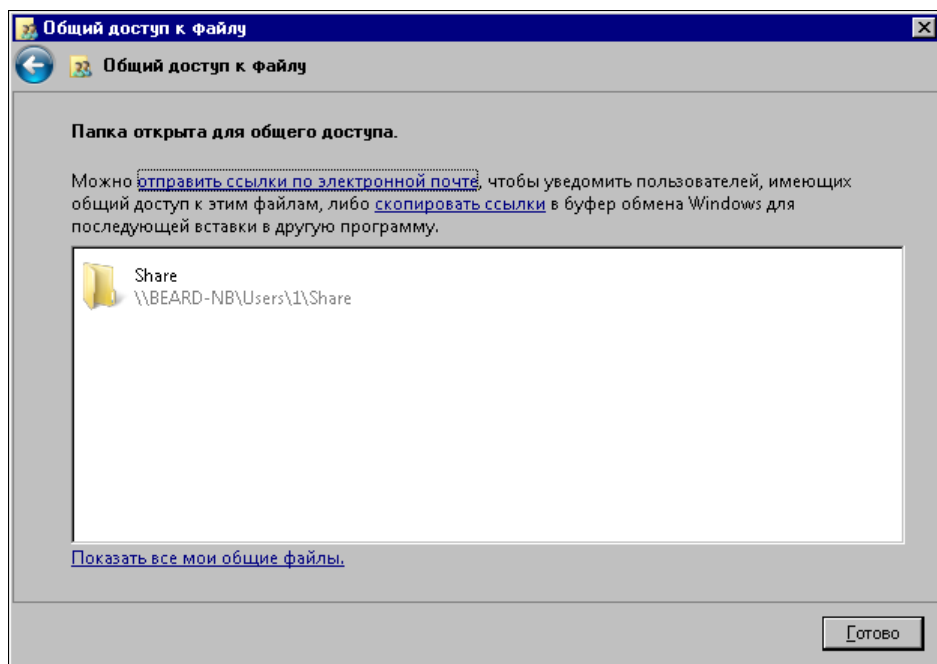


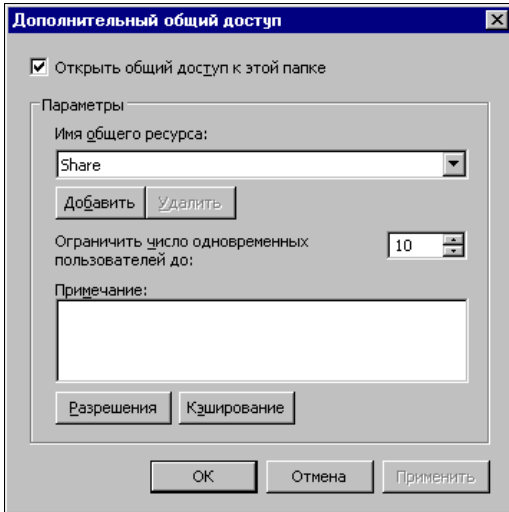
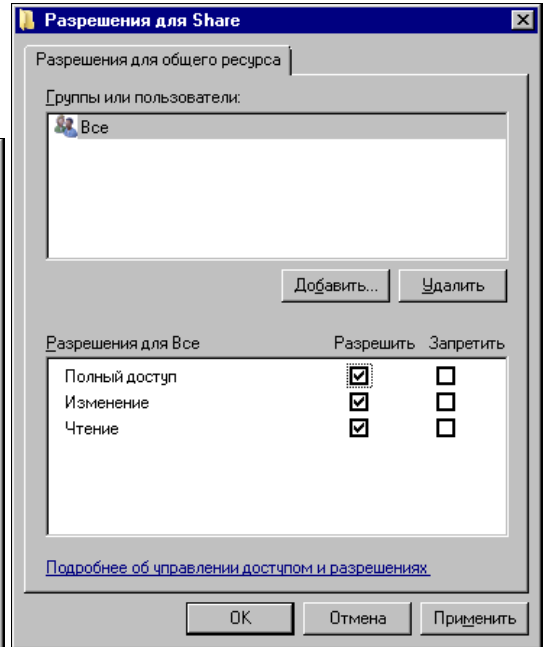
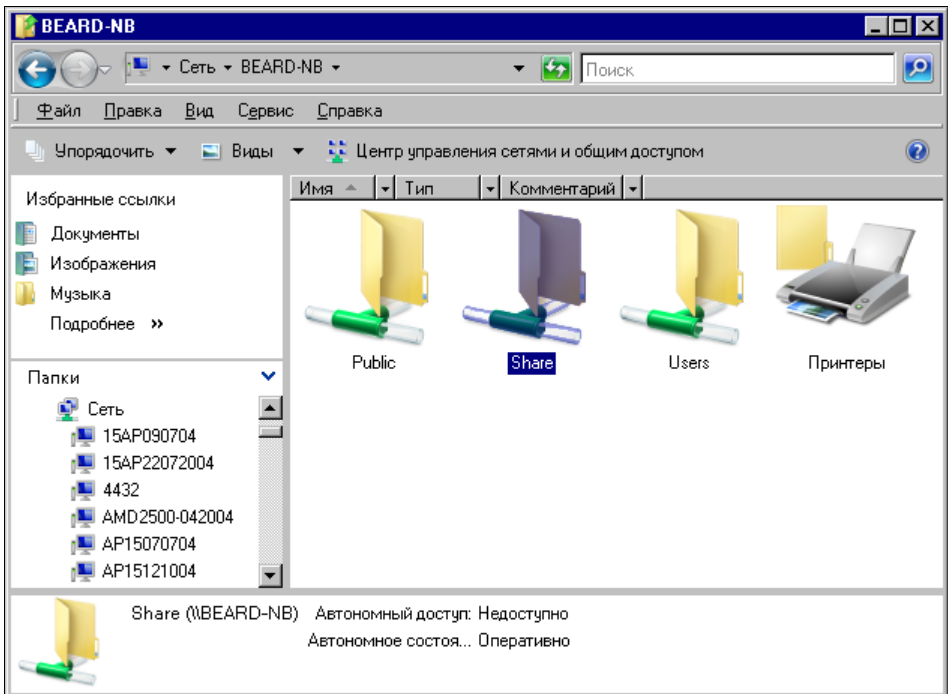
Рис. 1.32. Окно **Общий доступ к файлу** — сообщение об открытии общего доступа

4. Теперь воспользуемся кнопкой **Дополнительный доступ** (см. рис. 1.31). Нажав на нее, мы вызовем окно (рис. 1.33) **Дополнительный общий доступ**. Только что мы обеспечили доступ локальных пользователей к папке, теперь обеспечим доступ по сети. Нажмем кнопку **Разрешения**.
5. В открывшемся окне **Разрешения для Share** (рис. 1.34) укажем разрешения для пользователей, подключающихся к папке Share через сеть.

Теперь сетевые пользователи смогут подключиться к папке Share, найдя компьютер Beard-NB в сетевом окружении (рис. 1.35). Поиск компьютера в сети возможен и по его IP-адресу. Этот вариант может быть полезен при подключении из другой операционной системы, например из Linux (рис. 1.36).

Настроив общий доступ к файлам и папкам по сети, вы можете пользоваться сетевыми каталогами так же, как и локальными.

Напомню, что имя учетной записи на компьютере изменялось. Для доступа по сети необходимо указывать старое имя учетной записи, которое соответствует имени каталога пользователя в системе. В операционной системе Windows Vista Ultimate есть возможность полного переименования учетных записей через оснастку **Управление компьютером** (**Панель управления** | **Система и ее обслужива-**

Рис. 1.33. Окно **Дополнительный общий доступ**Рис. 1.34. Окно **Разрешения для Share**Рис. 1.35. Окно **BEARD-NB** (Общие ресурсы, видимые через сеть с другого компьютера)

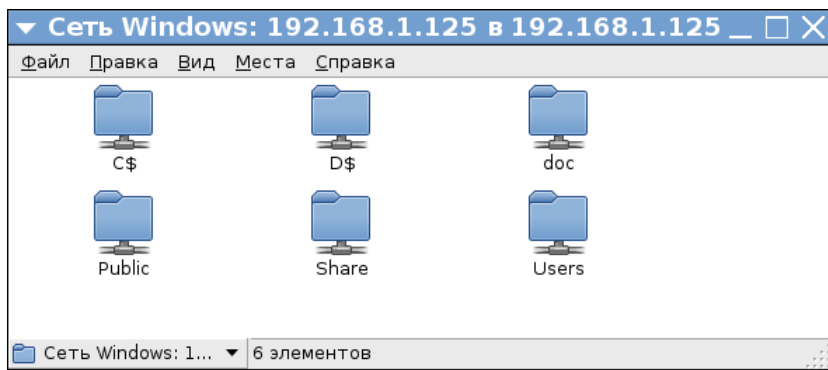


Рис. 1.36. Окно **Сеть Windows: 192.168.1.125** (доступные по сети ресурсы на компьютере с IP-адресом 192.168.1.125 при подключении из Linux)

ние | **Администрирование** | **Управление компьютером**). Если у вас установлена именно такая система, можете самостоятельно найти раздел **Локальные пользователи** в окне **Управление компьютером**. Переименование таким способом возможно, если вы вошли в систему под другой учетной записью.

## Настраиваем общий доступ к файлам и папкам в Linux

В операционной системе Linux для обеспечения доступа к файлам и папкам по сети применяется специальная служба — сервер Samba. Обычно она устанавливается по умолчанию. В отличие от Windows в Linux необходимо запускать эту службу после включения компьютера или перезагрузки, иначе доступ будет отключен. В различных версиях Linux доступ к настройкам Samba может быть выполнен разными путями. Например, в ASP Linux путь к настройкам сетевого доступа к файлам и папкам следующий: **Система** | **Администрирование** | **Настройка сервера Samba**, а в Mandriva Linux — **Система** | **Администрирование** | **Настройка компьютера** | **Сетевые службы** | **Настройка Samba**. Если сервер Samba не установлен, то система сообщит об этом и предложит установить его. Установка стандартных пакетов в Linux происходит автоматически, следует только согласиться с ее необходимостью. Интерфейс настройки в версиях Linux может несколько отличаться, но незначительно. Однажды настроив Samba в одной версии Linux, вы легко повторите настройки в любой другой. Рассмотрим настройку Samba в Mandriva Linux.

1. Итак, пройдите по указанному ранее пути и откройте окно **Центр управления Mandriva Linux 2008.0** (рис. 1.37). Прежде чем система допустит вас к настройкам компьютера, потребуется ввести пароль администратора, введите его.
2. В окне **Центр управления Mandriva Linux 2008.0** нажмите кнопку **Добавить**. Откроется окно **Добавить пользователя Samba** (рис. 1.38).
3. Выберите имя пользователя из числа имеющихся учетных записей в выпадающем одноименном списке. В окне **Центр управления Mandriva Linux 2008.0** на

вкладке **Пользователи Samba** (рис. 1.39) появится строка с именем учетной записи, имеющей права доступа.

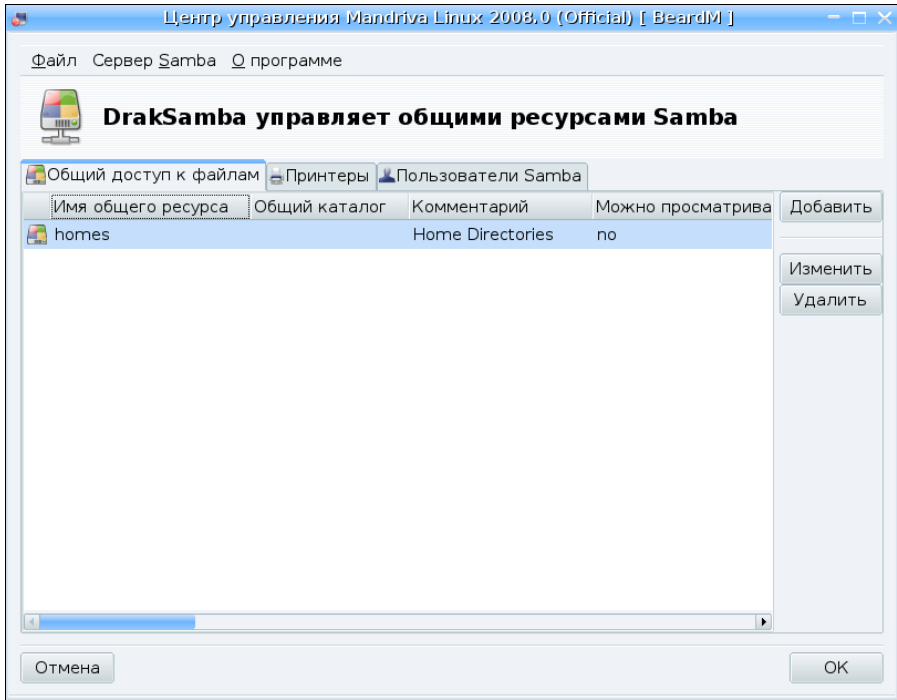


Рис. 1.37. Окно **Центр управления Mandriva Linux 2008.0**

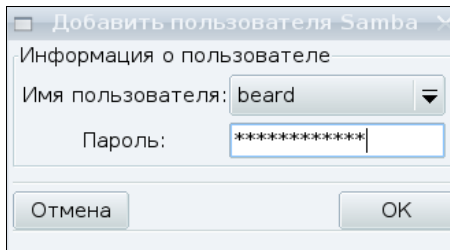


Рис. 1.38. Окно **Добавить пользователя Samba**

- В окне **Центр управления Mandriva Linux 2008.0** на вкладке **Общий каталог** нажмите кнопку **Добавить**, для добавления каталога общего доступа. Откроется окно **Выбор каталога** (рис. 1.40), в котором необходимо выбрать существующий или созданный предварительно каталог. Есть возможность создания каталога прямо из окна **Выбор каталога**. В примере выбирается каталог Share, который был создан в папке пользователя.

В окне **Центр управления Mandriva Linux 2008.0** на вкладке **Общий доступ к файлам** (рис. 1.41) появится строка с именем выбранного каталога. Теперь доступ к каталогу Share возможен с любой рабочей станции под управлением Windows

или Linux. На рисунке (рис. 1.42) приведено окно с доступными ресурсами компьютера под управлением Linux, открытого в сети с компьютера под управлением Windows Vista.

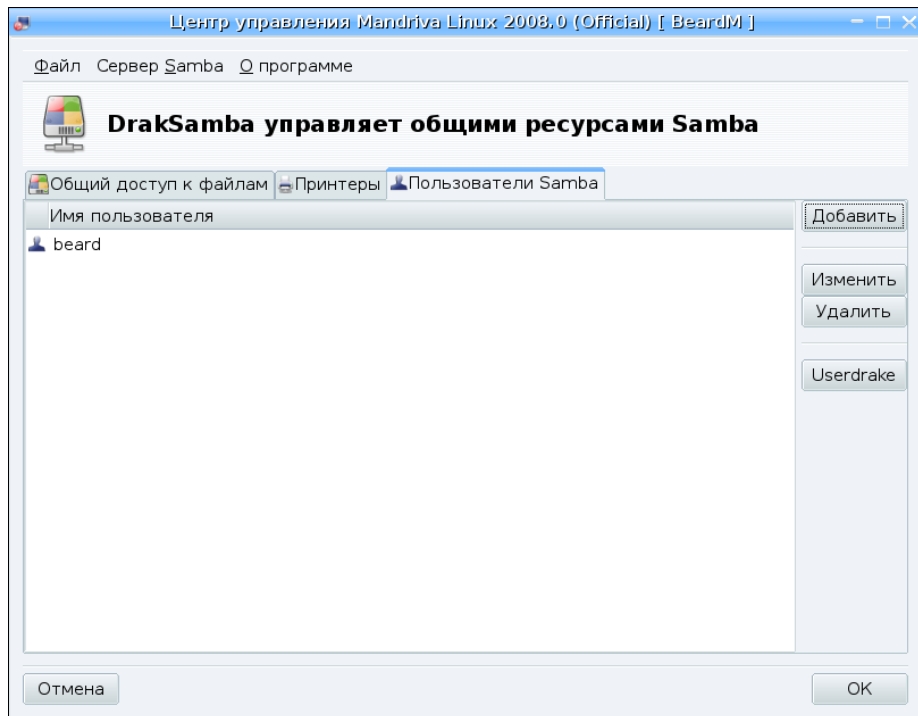


Рис. 1.39. Окно Центр управления Mandriva Linux 2008.0, вкладка Пользователи Samba

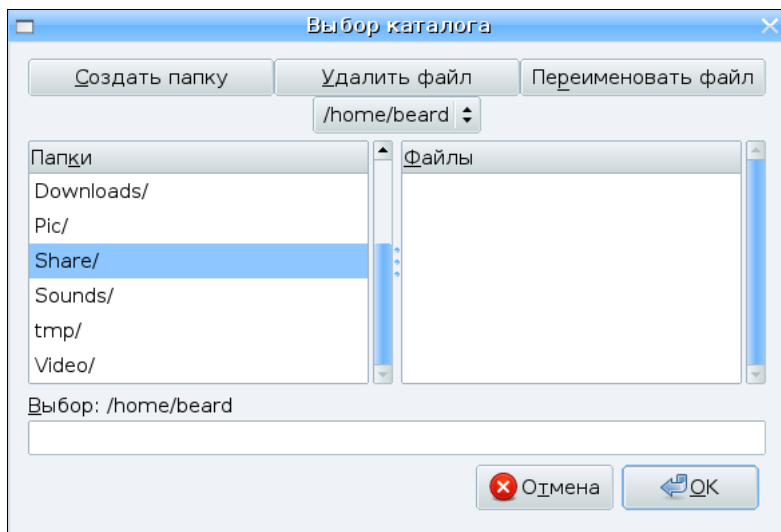


Рис. 1.40. Окно Выбор каталога

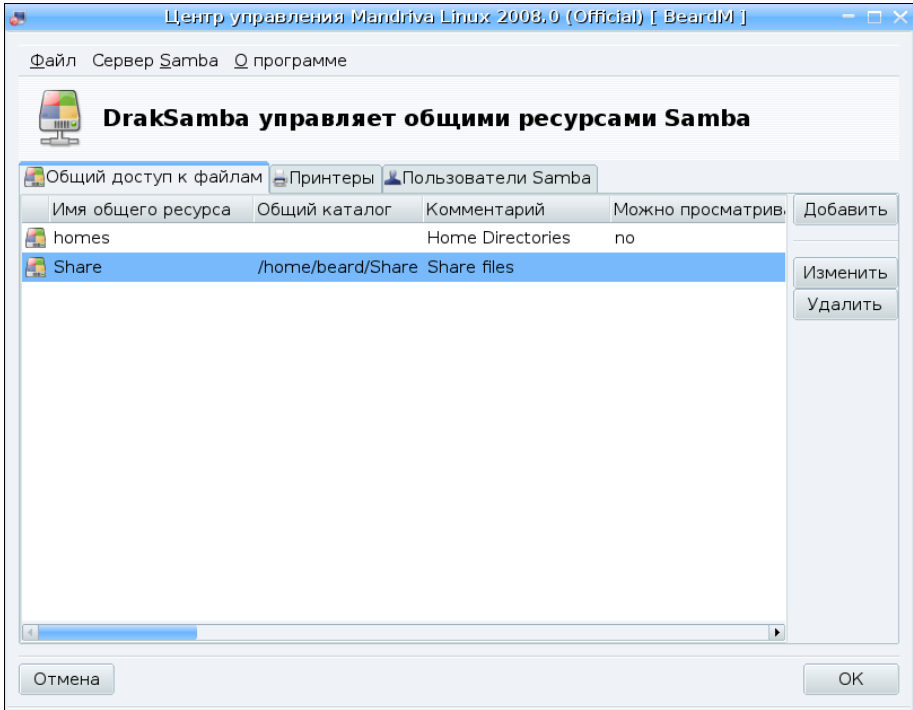


Рис. 1.41. Окно Центр управления Mandriva Linux 2008.0, вкладка **Общий доступ к файлам**

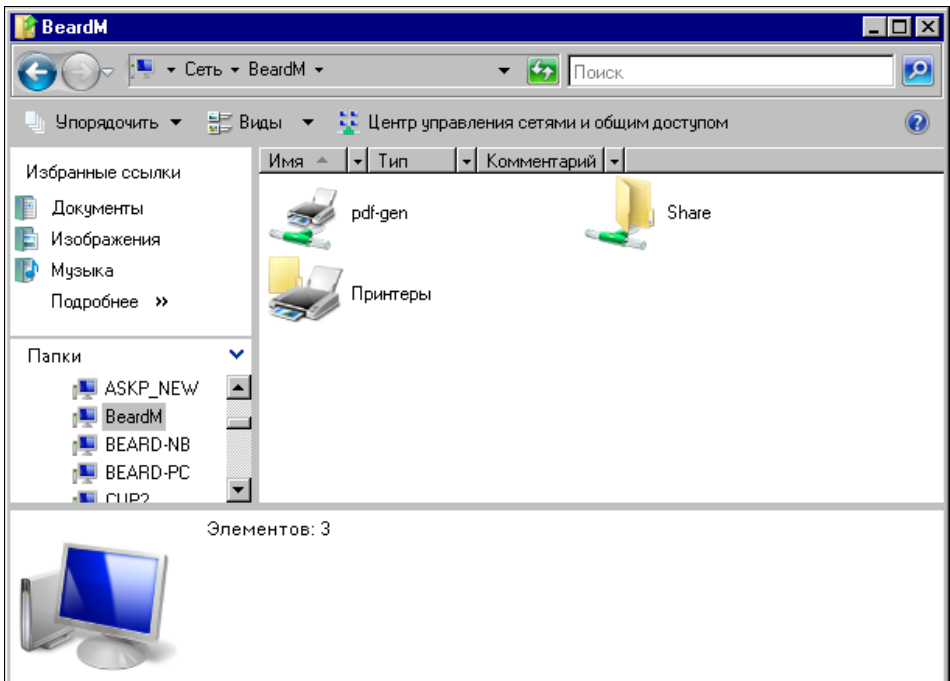


Рис. 1.42. Окно **BeardM** (доступные по сети ресурсы)



## Особенности сетевого доступа к файлам из Linux к Windows Vista

К сожалению, не всегда удастся такими простыми настройками обеспечить доступ к файлам и папкам по сети. Если из Linux выполнять подключение к ресурсам Windows до ОС Windows Vista, то проблем не возникает. Но в Windows Vista изменен протокол доступа к файлам и папкам. Этот протокол есть и в Linux, но в большинстве существующих у пользователей версий этой системы он не имеет графической оболочки для настройки. Тем не менее, это не является существенным препятствием для организации передачи файлов по сети между всеми вашими компьютерами. Придется обратиться к командной строке. В Linux аналог командной строки Windows — это Terminal.

В ASP Linux это окно можно вызвать **Приложения | Стандартные | Терминал**. Но можно просто войти в консольный сеанс после нажатия комбинации клавиш `<Ctrl>+<Alt>+<Fn>`, где `n` — любое число от 1 до 6, определяющее номер консоли. Можно запускать до шести консольных сеансов одновременно. Для перехода снова в оконный режим следует нажать комбинацию клавиш `<Ctrl>+<Alt>+<F7>`.

Работая в терминале, необходимо получить права администратора, для этого следует ввести команду `su` и пароль пользователя `root`. В консольном сеансе, зарегистрировавшись обычным пользователем, также введите команду `su` и пароль пользователя `root`. Далее для подключения к доступному по сети каталогу компьютера под управлением Windows Vista необходимо ввести следующую команду:

```
mount -t cifs //10.15.0.5/share /mnt/shr
```

где `shr` — каталог, в который будет смонтирован доступный по сети каталог из Windows Vista. В данном примере он был предварительно создан в каталоге `mnt` файловой системы Linux.

При выполнении этой команды потребуется ввести пароль для доступа к сетевому каталогу. Имя пользователя в данном случае не требуется, поскольку оно одно и то же на всех наших компьютерах.

После завершения команды доступ к сетевому каталогу будет обеспечен. Вы имеете возможность проверить наличие доступа, не выходя из консольного режима, запустив файловый менеджер командой `mc` и перейдя в каталог `shr`. Ранее пустой каталог будет содержать файлы, помещенные в открытый для доступа через сеть каталог Share на компьютере под Windows Vista.

Перейдя в графический режим, вы можете работать с каталогом и содержащимися в нем файлами как обычно.

Если необходимо размонтировать сетевой каталог, прекратив доступ к его файлам, достаточно ввести команду `umount -t cifs //10.15.0.5/share /mnt/shr`.

Надо сказать, что Mandriva Linux 2008 даже из графического интерфейса успешно справляется с доступом к файлам в Windows Vista.

### ПРЕДУПРЕЖДЕНИЕ

При копировании файлов с машины, на которой установлена ОС Linux, на машину с Windows это следует делать из Windows. Запись на разделы NTFS из Linux ранних версий чаще всего происходит с ошибками. В последних версиях Linux эта проблема исправлена.

## Соединяем компьютеры без кабеля

### ПРЕДУПРЕЖДЕНИЕ

Если вы еще не уверенно чувствуете себя в сети, не достаточно хорошо владеете настройками компьютеров в обычной кабельной сети, то этот раздел стоит прочитать довольно бегло, вернувшись к нему, при необходимости, позднее после прочтения книги.

Вариантов такого соединения существует несколько. Но самый подходящий стандарт для организации беспроводного объединения компьютеров в сеть это Wi-Fi (Wireless Fidelity). Этот вариант объединения компьютеров в сеть требует дополнительного оборудования, но от компьютера не будет тянуться кабель. Это может быть особенно удобно, когда вы используете ноутбук. Достаточно просто включить его, и сетевое подключение может быть установлено.

В последнее время такие сети все чаще используются в общественных местах, таких как кафе, аэропорты, и в других учреждениях. Но и дома или в офисе мобильный компьютер удобно подключать к сети через Wi-Fi.

В отличие от кабельного соединения компьютеров, беспроводное подключение требует наличия коммутатора. Причем, коммутатор должен содержать в себе и *точку доступа к радиосети*.

Снова придется забежать вперед, поскольку имеющееся у нас оборудование имеет более широкие возможности. Но и при соединении двух компьютеров эти возможности могут пригодиться. По приведенному далее описанию можно подключить не только два компьютера друг к другу, но и создать беспроводную одноранговую сеть. Более подробно одноранговые сети мы рассмотрим в *главе 2*, а теперь поговорим именно о беспроводном доступе к сети.

## Оборудование

Прежде всего, для организации беспроводного доступа к сети необходимо иметь соответствующее оборудование. В данном примере комплект оборудования был приобретен обычным пользователем ПК для организации доступа к домашней сети и Интернету с ноутбука. Но, прочитав описание, приведенное далее, вы увидите, что можно просто подключить второй ноутбук или обычный ПК к коммутатору, организовав между ними сетевую связь. Используя дополнительные возможности комплекта приобретенного оборудования, можно к получившейся простейшей сети подключить принтер, и даже организовать доступ в Интернет.

В состав комплекта вошло следующее оборудование.

- *Модем D-Link DFM-562E* (рис. 1.43). 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 сети Интернет 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 и коррекцию ошибок для быстрого и надежного приема/передачи.



Рис. 1.43. Вид модема D-Link DFM-562E



Рис. 1.44. Вид беспроводного адаптера D-Link DWL-G122 USB

В примере не описываются настройки модема, поскольку для большинства модемов они похожи, или даже практически всегда такие настройки вообще не нужны. Но если будет необходимость применения модема совместно с маршрутизатором, который применяется 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, который используется для соединения компьютера с высокоскоростной беспроводной сетью (рис. 1.44). 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 обладает скоростью 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, адаптер 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. Адаптер 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 переда-

че данных динамически выполняется шифрование данных. Технология WPA (Wi-Fi Protected Access, защищенный доступ в беспроводной сети) обеспечивает авторизацию и идентификацию пользователей на основании секретного ключа, который автоматически меняется по истечении некоторого периода времени. При совместной работе с сервером RADIUS технология WPA использует протокол TKIP (Temporal Key Integrity Protocol, протокол целостности временного ключа) для смены временного ключа каждые 10000 пакетов. Это обеспечивает более высокий уровень безопасности, чем стандарт WEP (Wireless Encryption Protocol, протокол шифрования в беспроводной связи), 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 в независимости от того, используют ли они стандарт 802.11b или более быстрый 802.11g.

- *Беспроводный 802.11g VPN маршрутизатор DI-824VUP+*, объединяющий функции широкополосного доступа в Интернет с надежной VPN-защитой (Virtual Private Network, виртуальная частная сеть) межсетевым экраном, встроенным принт-сервером и 4-портовым коммутатором для подключения принтера и рабочих станций (рис. 1.45). 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 по отношению к внешнему миру. Благодаря встроенной беспроводной точке доступа, 4-портовому коммутатору 10/100 Мбит/с и принт-серверу, этот 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 маршрутизатор DI-824VUP+ поддерживает передачу данных на скорости до 54 Мбит/с. Маршрутизатор совместим со всеми беспроводными устройствами стандарта 802.11b/b+, имеет встроенную поддержку VPN, что позволяет создавать множество туннелей IPSec для удаленных офисов. Реализация IPSec использует шифрование DES (Data Encryption Standard, стандарт шифрования данных), 3DES, AES (Advanced Encryption Standard, расширенный стандарт шифрования) 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 использованием шифрования triple DES. Это позволяет пользователям 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 использовать 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* (Uniform Resource Locator, унифицированный указатель информационного ресурса) 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 (Demilitarized Zone, демилитаризованная зона) применяются для единичного клиента (например, Web-сервера), находящегося за маршрутизатором для полного доступа к нему из Интернета и гарантии полной совместимости приложений сети Интернет, даже если определенный порт неизвестен. 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, позволяя пользователям офисной сети совместно использовать параллельный и USB-принтеры для печати файлов и Web-страниц.



Рис. 1.45. 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. При описании примера мы используем лишь небольшую их часть.

## Организация сети

Один из распространенных вариантов использования беспроводного оборудования — это подключение к сети офиса или квартиры. На рис. 1.46 представлена схема домашней сети с использованием маршрутизатора DI-824VUP+. Вариант устройства "цифрового дома", который можно увидеть на странице <http://www.dlink.ru/products/home/dhome.php>, отличается значительно большим числом точек радиодоступа и других устройств беспроводной связи. 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.

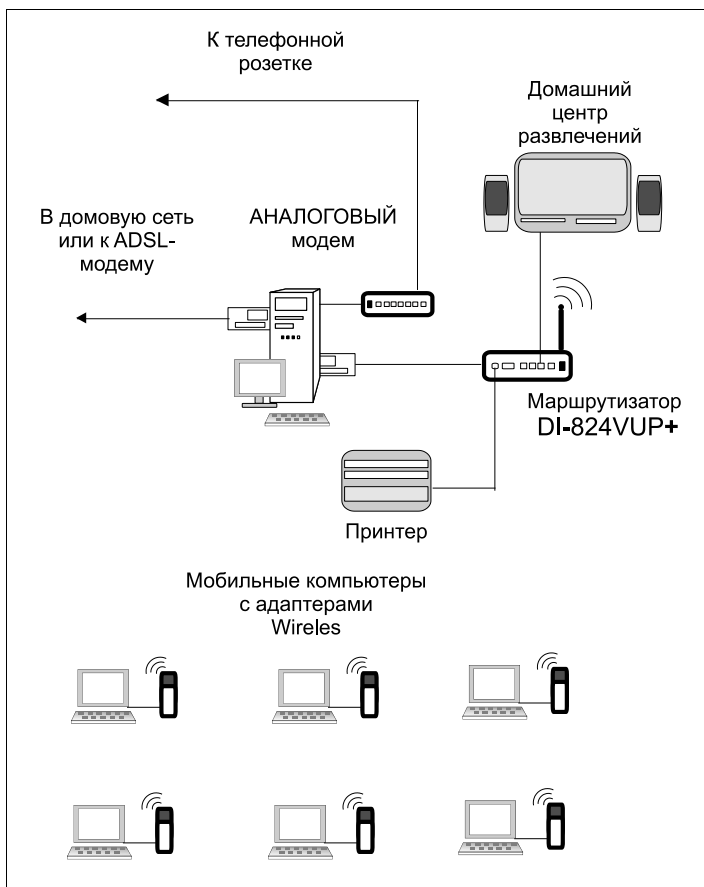


Рис. 1.46. Общая схема домашней сети с использованием маршрутизатора DI-824VUP+

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 домашней сетью, через которую

осуществляется предоставление доступа в Интернет. Для этого подключения 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 подключение дополнительных устройств в имеющиеся Ethernet-порты самого маршрутизатора, который может выполнять функции коммутатора в сети.

Для того чтобы иметь возможность изменять настройки маршрутизатора, контролировать его работу, необходим компьютер. Чтобы работа маршрутизатора уже на самом начальном этапе была близка к реальной, мы применили ноутбук с подключенным к нему беспроводным адаптером D-Link DWL-G122 USB стандарта 802.11g.

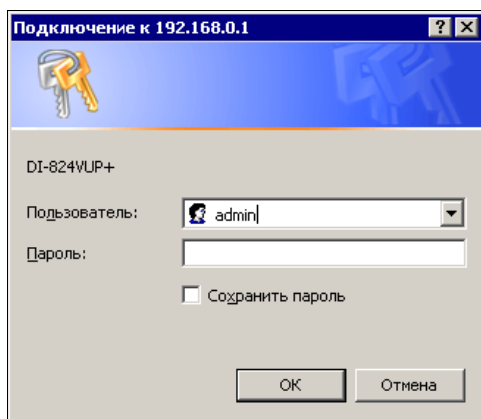


Рис. 1.47. Окно Подключение к 192.168.0.1 (окно авторизации)

Достаточно установить программное обеспечение, прилагаемое к адаптеру, и вы уже можете соединяться с маршрутизатором для его настройки и администрирования, подсоединив его, конечно, к источнику питания. Для подключения к маршрутизатору через радиоканал необходимо в адресной строке Internet Explorer набрать — 192.168.0.1. Именно такой адрес по умолчанию имеет маршрутизатор. Для подключения необходимо ввести имя и пароль администратора (рис. 1.47). Для но-

вого 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.

После успешной авторизации появится страница, предлагающая для настройки воспользоваться мастером настройки (рис. 1.48).

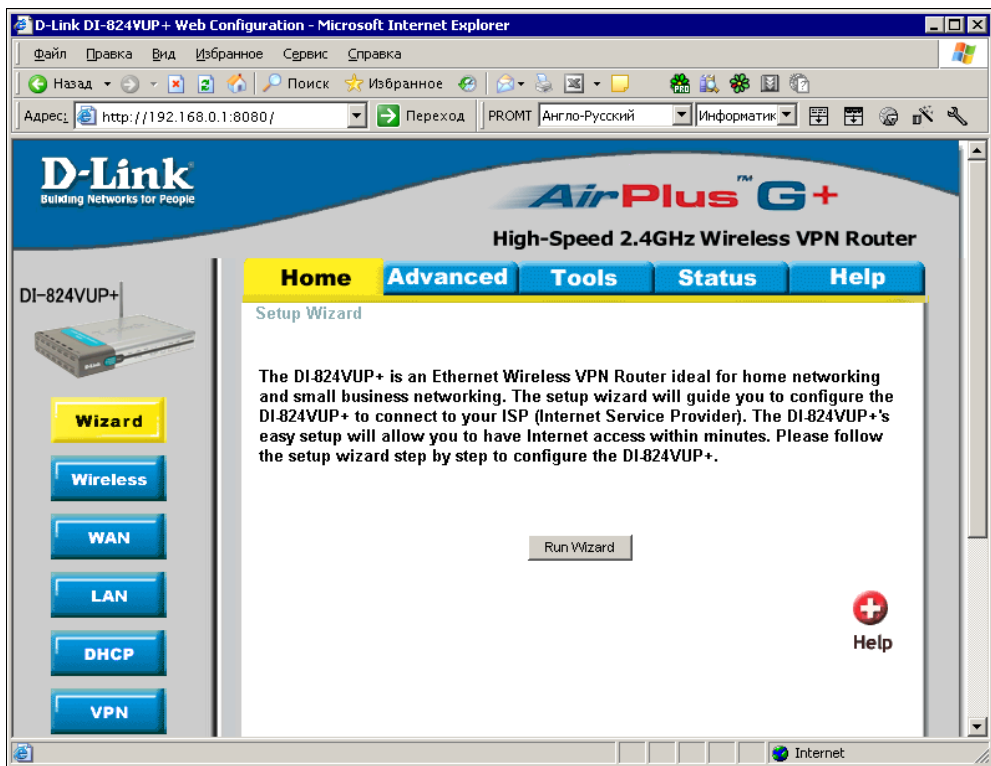


Рис. 1.48. Окно конфигурации маршрутизатора DI-824VUP+

На этой странице предлагается воспользоваться мастером настройки, который поможет выполнить быстрое подключение к Интернету. Для этого следует нажать кнопку **Run Wizard**.

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. 1.49). Нажав на кнопку **LAN**, можно увидеть, а при необходимости изменить эти настройки. Однако в этом редко возникает необходимость. Значительно чаще требуются настройки внешней для маршрутизатора WAN-сети. Нажав на кнопку **WAN**, вы получите доступ к этим настройкам (рис. 1.50). Маршрутизатор может быть подключен к сети как одно из рядовых устройств. Поэтому и IP-адрес маршрутизатора не отличается какими-



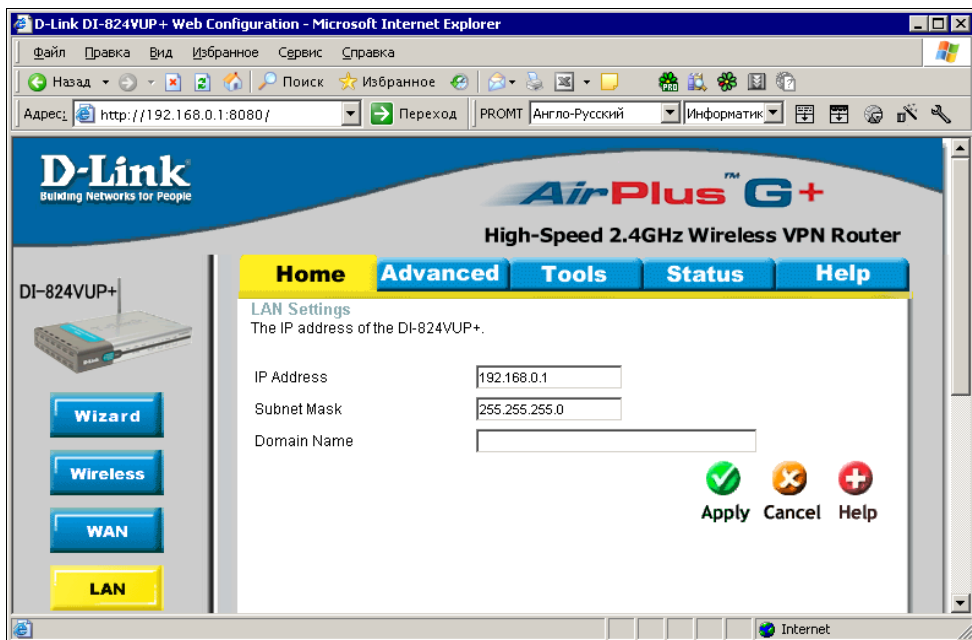


Рис. 1.49. Окно конфигурации маршрутизатора DI-824VUP+ . LAN Settings — настройка локальной сети

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.

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 написать электронное письмо, которое тут же может быть отправлено. Имеется возможность 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.

Если вам придется иметь дело именно с таким маршрутизатором, который рассмотрен ранее, то вы увидите, что его возможности намного 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, но при необходимости воспользоваться тем или иным вариантом подключения изменять настройки маршрутизатора.

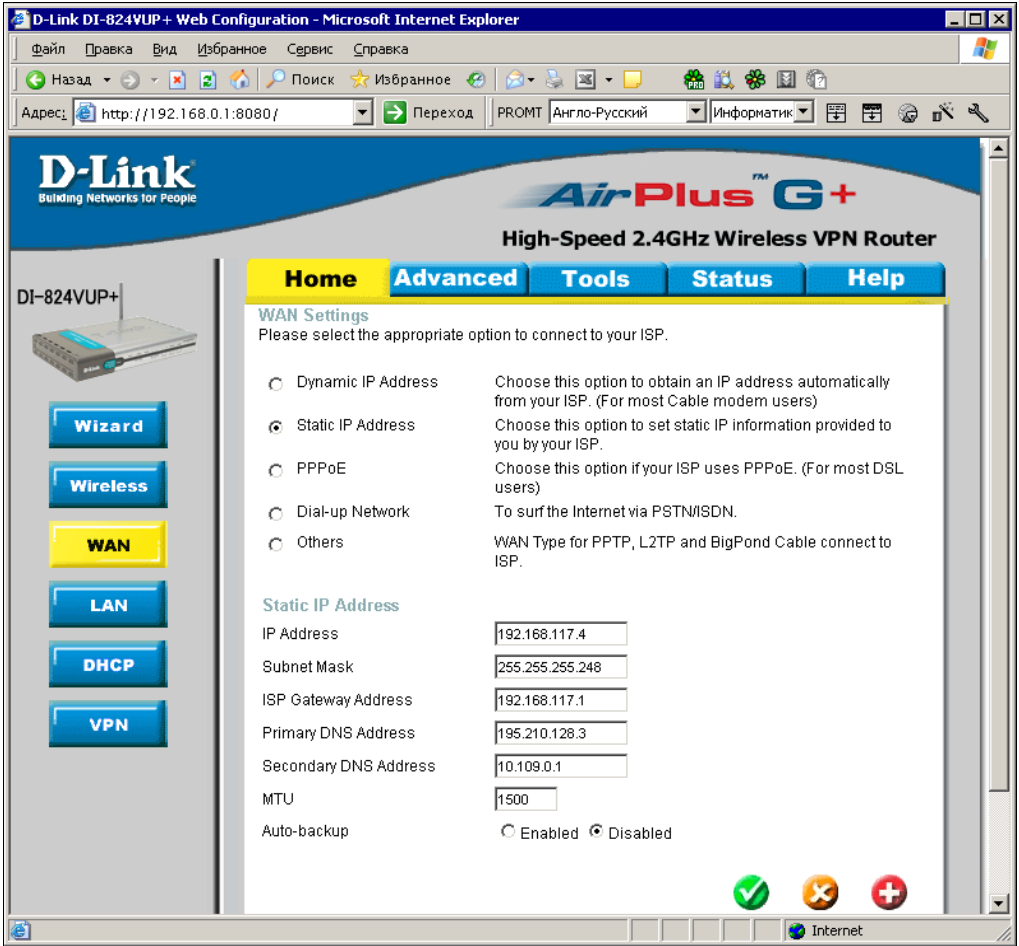


Рис. 1.50. Окно конфигурации маршрутизатора DI-824VUP+ .  
WAN Settings — настройка параметров глобальной сети

Среди прочих устройств на схеме сети (см. рис. 1.46) 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.

Остальные настройки вы сможете рассмотреть подробно, если столкнетесь именно с таким устройством. Но прежде, чем вы будете приобретать необходимое оборудование, необходимо проанализировать потребности, и не покупать устрой-

ства 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 по радиосвязи (Wireless) подключился сетевой адаптер DWL-G122 USB, появляется теоретическая возможность подключения к этому компьютеру и из другой радиосети. Но это возможно только при отключенном брандмауэре для данного подключения. Но независимо от наличия защиты на компьютерах сети, возможен доступ к настройкам маршрутизатора со стороны злоумышленника. Однако можно выбрать защищенный режим работы сети. На рис. 1.51 показано окно настройки сети со списком возможных вариантов.

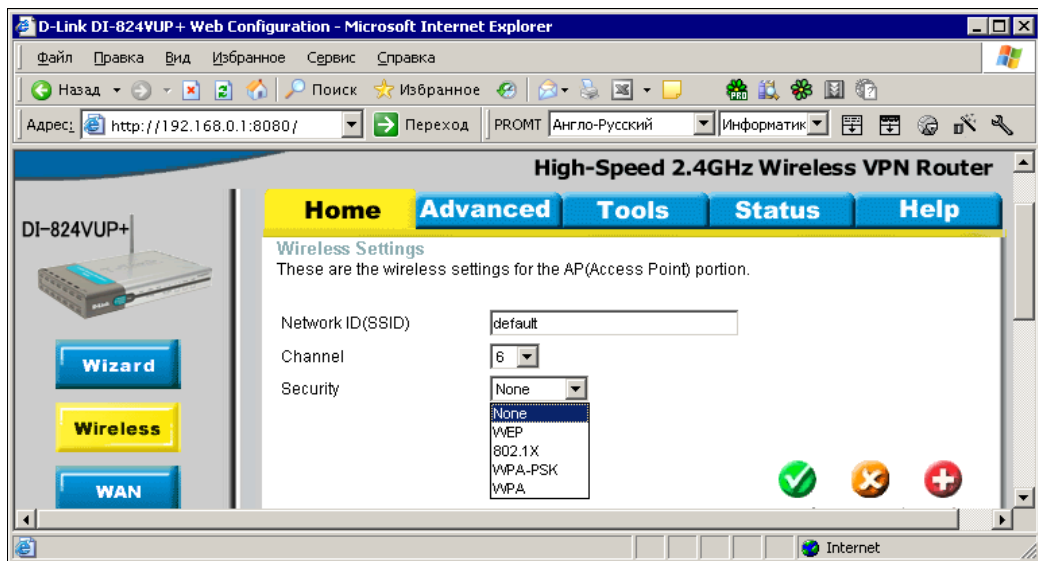


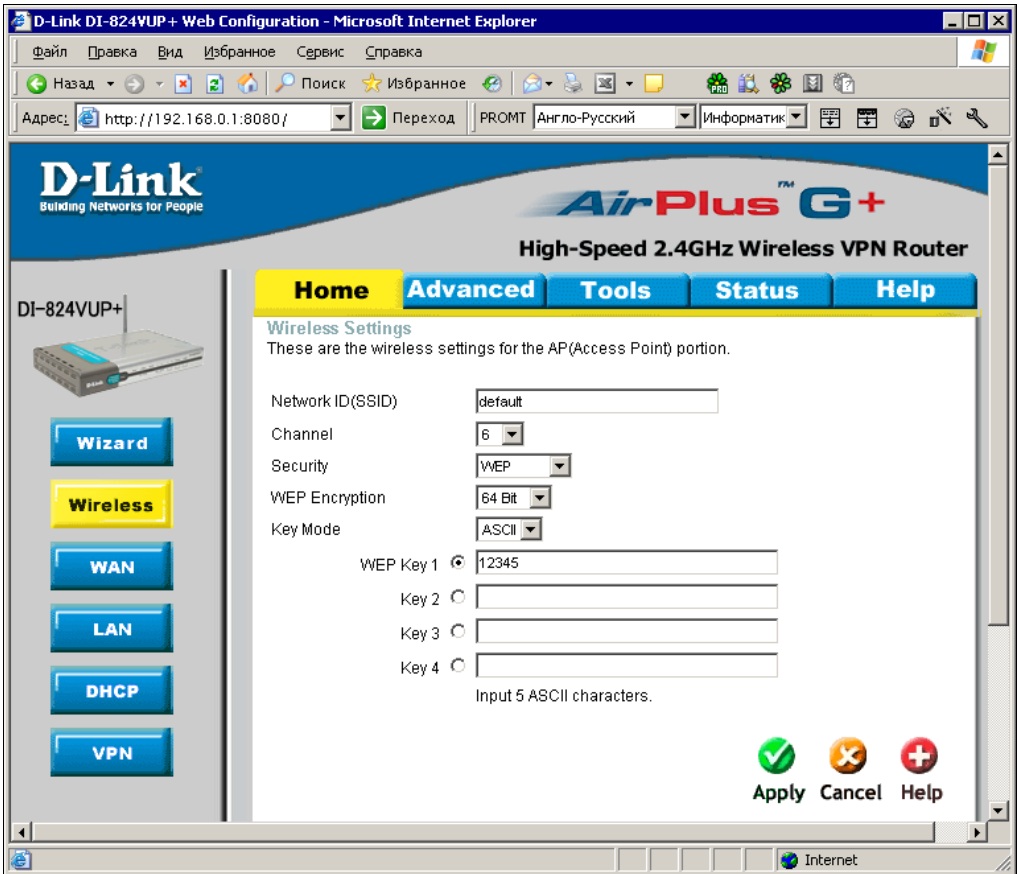
Рис. 1.51. Окно конфигурации маршрутизатора DI-824VUP+ .  
Wireless Settings — настройка параметров защиты радиосети

На рисунке (рис. 1.52) 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!

Ничего страшного, на самом деле паниковать не стоит. Откройте свойства вашего подключения (рис. 1.53) 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 на эту кнопку придется воспользоваться каким-либо тонким предметом, например спичкой.



**Рис. 1.52.** Окно конфигурации маршрутизатора DI-824VUP+. **Wireless Settings** — настройка параметров защиты радиосети, выбор варианта шифрования

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.

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 ноутбуком, 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.

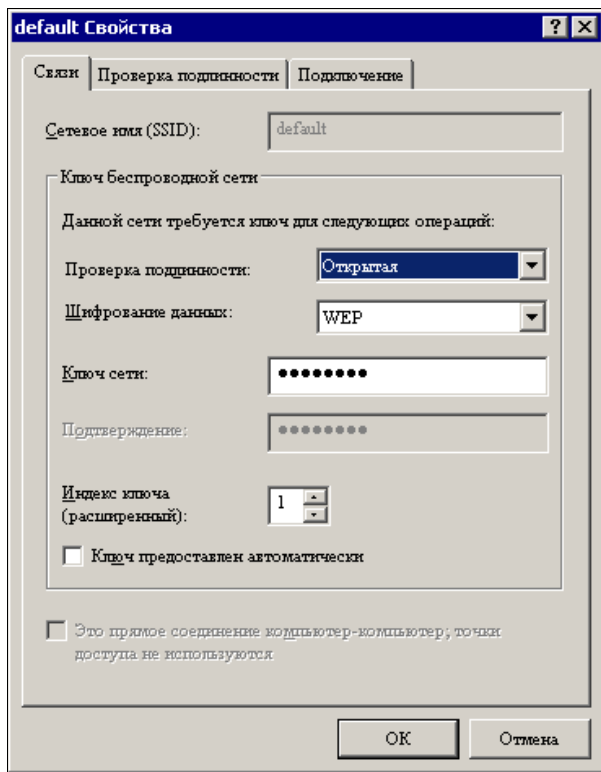


Рис. 1.53. Окно свойств wireless-подключения на компьютере. Ввод ключа сети

Тема защиты радиосетей достаточно широка, и если вы хотите ознакомиться с другими методами защиты беспроводной сети, обратитесь к ресурсам Интернета:

- ❑ [http://www.rozetka.de/publication/cat\\_4](http://www.rozetka.de/publication/cat_4)
- ❑ <http://www.cir-sanych.ru>
- ❑ [http://www.citforum.netis.ru/nets/wireless/seti\\_efir](http://www.citforum.netis.ru/nets/wireless/seti_efir)

или к справочной информации Windows.

По ссылке, приведенной далее, можно прочитать о применении другого типа устройств при организации беспроводной сети:

[http://www.murava.ru/articles/wlan\\_home.php](http://www.murava.ru/articles/wlan_home.php)

Сайт производителя описанного оборудования тоже содержит много полезной информации:

<http://www.dlink.ru/products/home/dhome.php>

Далее в книге мы не будем касаться темы беспроводных сетей. Информации, приведенной в этой главе и в указанных источниках в Интернете, вполне достаточно, чтобы использовать беспроводную связь и в более сложных сетях. Следующая глава посвящена одноранговым сетям, содержащим более двух компьютеров.

## Соединяем компьютеры посредством Bluetooth

Этот способ объединения компьютеров в сеть, как и описанный ранее, не предполагает использования кабеля. В ряде случаев и на обычную сеть это объединение не совсем похоже. Тем не менее, применение технологии Bluetooth заслуживает рассмотрения ввиду достаточно широкого распространения устройств, ее поддерживающих. Чаще всего Bluetooth применяют для связи между мобильными телефонами, связи мобильных телефонов с компьютерами или подключения беспроводных устройств к компьютерам. Но при необходимости Bluetooth может частично заменить другие средства организации сети для двух-трех компьютеров.

Для операционной системы Windows производители Bluetooth предлагают программы, которые позволяют создать сеть между двумя компьютерами или просто передать файлы между ними. Часто эти программы требуется приобретать, поскольку в бесплатных версиях могут быть установлены ограничения на объем переданной информации или другие ограничения. В ОС Linux программы для работы с Bluetooth написаны программистами, не зависящими от изготовителей USB-устройств. Эти программы работают одинаково с устройствами различных производителей и не имеют ограничений по каким-либо параметрам передачи данных.

Рассмотрим возможности одной из таких программ на примере последней на сегодняшний день версии *Linux Mint* — операционной системы, созданной на основе Ubuntu, которая в свою очередь создана на основе Debian. Загрузить образ диска с дистрибутивом системы можно с сайта <http://www.linuxmint.com>.

Когда система уже установлена, добавляем необходимые дополнительные компоненты. В данном случае нас интересует программа *Blueman*. Ее можно установить двумя простыми способами (имеются и более сложные, но их рассматривать мы не будем). Первый способ состоит в том, чтобы выбрать имя этой программы в Менеджере пакетов *Synaptic*, который установлен по умолчанию. Для ускорения поиска введите имя или часть имени программы в поле **Быстрый поиск** (рис. 1.54).

Щелкнув правой кнопкой на строке с именем программы, выберите пункт **Отметить для установки**, а затем в меню окна нажмите кнопку **Применить** и следуйте указаниям менеджера пакетов (если программа в менеджере пакетов помечена затененным квадратом, то она уже установлена).

Второй способ — просто ввести в окне терминала команду: `sudo apt-get install blueman`. Дальше, после запроса вашего пароля, система все сделает сама.

Установленная программа *Blueman* проявляет свое присутствие в системном лотке стандартным синим значком Bluetooth (рис. 1.55) (на рисунке он третий справа), но только если само устройство Bluetooth подключено к компьютеру.

В следующем примере рассмотрим настройку двух компьютеров для передачи файлов между ними посредством Bluetooth. Операции необходимо выполнять на обоих соединяемых компьютерах после подключения к ним устройств Bluetooth. В примере рассматривается подключение ноутбука к стационарному компьютеру.

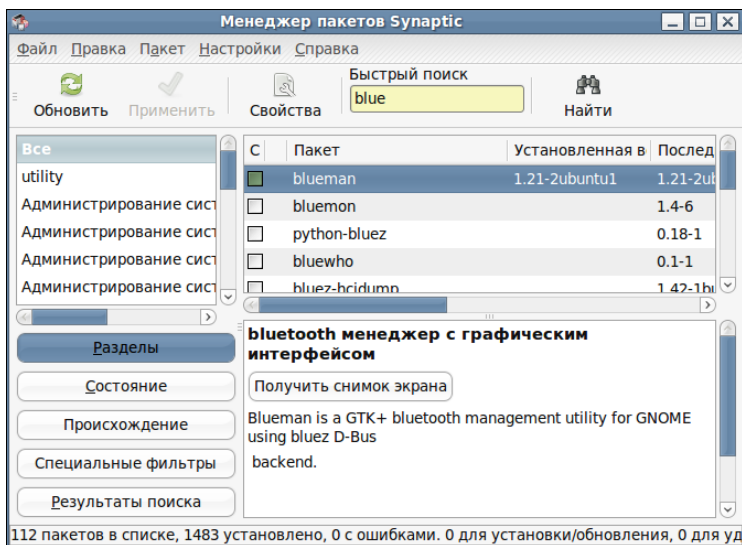


Рис. 1.54. Менеджер пакетов Synaptic. Поиск программы

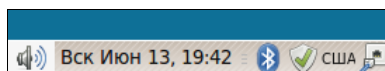


Рис. 1.55. Значок Bluetooth в системном лотке

## Настройка Bluetooth

Условно обозначим наши компьютеры (стационарный и ноутбук) как Компьютер 1 и Компьютер 2.

На Компьютере 1 щелкните правой кнопкой мыши на значке Bluetooth и выберите в открывшемся меню пункт **Адаптеры**. В открывшемся окне **Адаптеры Bluetooth** (рис. 1.56) выберите переключатель **Видимый всегда** и закройте окно.

Повторите эти же действия на Компьютере 2.

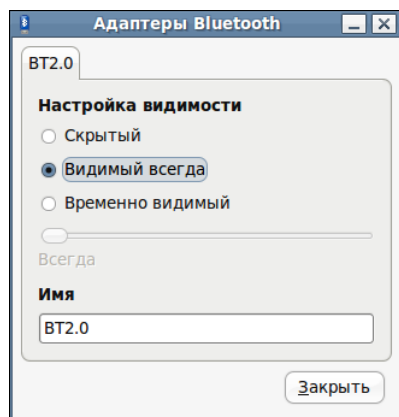


Рис. 1.56. Окно Адаптеры Bluetooth

Позднее при необходимости можно изменить режим видимости устройства, но пока мы должны видеть все используемые устройства.

Теперь щелкните правой кнопкой мыши на значке Bluetooth и выберите в открывшемся меню пункт **Установить новое устройство**. Откроется окно **Помощь**

ник настройки **bluetooth**, в котором начнет свою работу **Мастер установки устройств bluetooth**, который на первом шаге предлагает нажать кнопку **Вперёд**. Нажмите ее. Если в открывшемся окне **Помощник настройки bluetooth** не появилось строки с устройством Bluetooth другого компьютера, нажмите кнопку с изображением бинокля. Если все устройства исправны, вы увидите строку с именем устройства Bluetooth на втором компьютере (рис. 1.57).



Рис. 1.57. Окно  
Помощник настройки bluetooth

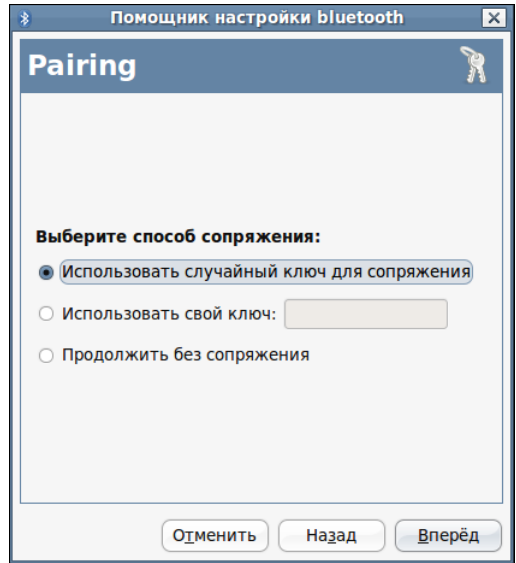


Рис. 1.58. Окно  
Помощник настройки bluetooth — Pairing  
(выбор способа сопряжения)

Повторите поиск устройств на Компьютере 2.

Затем на компьютере 1 выделите эту строку и нажмите кнопку **Вперёд**. При этом мастер предложит выбрать способ сопряжения устройств (рис. 1.58).

Теперь не спешите. Доступ к результату следующего действия ограничен по времени. Второй компьютер должен быть рядом, чтобы вы успели ответить на запрос pin-кода, который отобразится на мониторе Компьютера 1.

Выберите вариант **Использовать случайный ключ для сопряжения**.

Введите предложенный код в поле ввода, появившееся на мониторе Компьютера 2. Через секунду мастер поздравит вас с успешным добавлением устройства. Окно **Помощник настройки bluetooth** можно закрыть на обоих компьютерах.

После установления соединения между компьютерами значок Bluetooth в системном лотке украсится зеленым сигналом, похожим на огонек такси.

Теперь щелкните левой кнопкой мыши на значке. В открывшемся окне **Устройства Bluetooth** вы увидите устройство, с которым выполнено сопряжение (рис. 1.59).

Отметьте на каждом компьютере подключенное устройство, как доверенное, выбрав в меню **Устройства | Доверенный**.



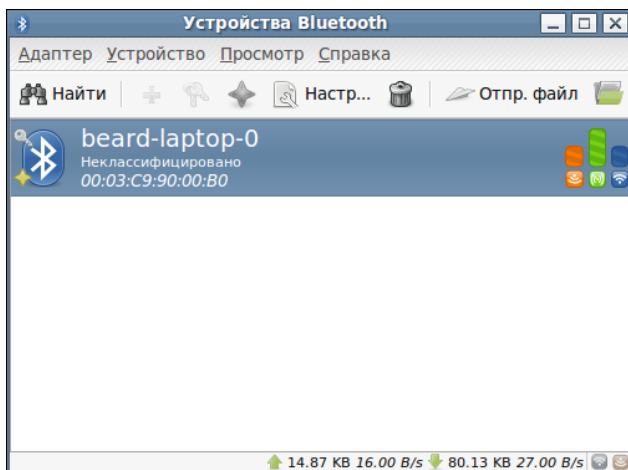


Рис. 1.59. Окно Устройства Bluetooth

Все. Теперь можно просматривать каталоги на сопряженном компьютере и отправлять на него файлы. Эти действия не вызовут затруднений.

Полезно ознакомиться с другими возможностями программы Blueman. Щелкнув правой кнопкой мыши на значке Bluetooth, выберите пункт **Модули** и затем пункт **Локальные службы**. Откроются одноименные окна (рис. 1.60 и 1.61).

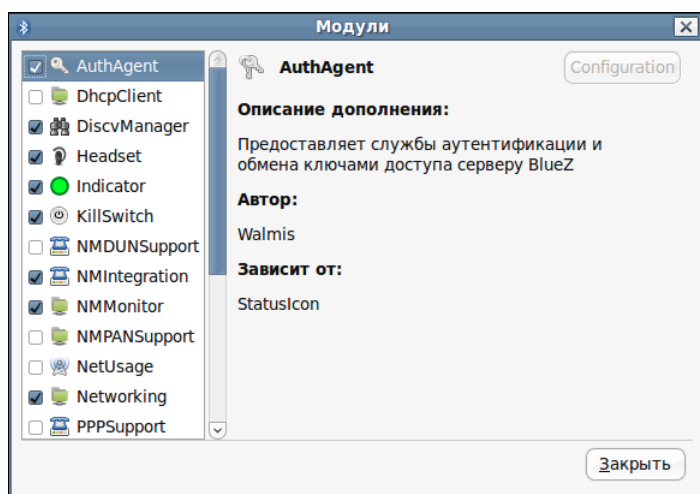


Рис. 1.60. Окно Модули

Изучение возможностей служб и модулей может занять продолжительное время. Но если это вам интересно, вы сможете организовать доступ в Интернет для ноутбука через стационарный компьютер посредством беспроводной сети, организованной через сопряженные Bluetooth-устройства.

Само собой разумеется, что есть и все обычные возможности работы с сотовыми телефонами и беспроводными устройствами.

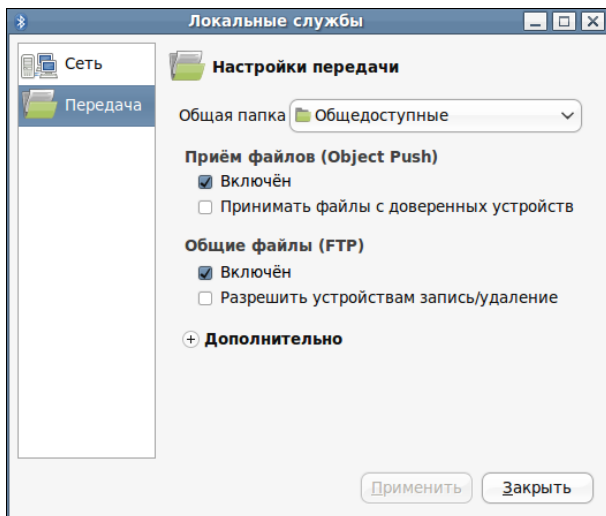


Рис. 1.61. Окно Локальные службы

## Windows 7 в сети

Итак, мы рассмотрели настройки операционных систем Windows разных выпусков. Но корпорация Microsoft не останавливается в совершенствовании своих операционных систем и в настоящее время предлагает ОС Windows 7.

Если вы внимательно прочитали предыдущий материал, то настройка сети в Windows 7 не вызовет затруднений. Следует только учесть некоторые особенности интерфейса новой операционной системы.

Все, что касается настройки сети, теперь можно найти в **Центре управления сетями и общим доступом**. Доступ к нему возможен через **Пуск | Панель управления | Сеть и Интернет | Центр управления сетями и общим доступом** (рис. 1.62).

Доступ к настройкам сетевого адаптера можно получить через пункт меню **Изменение параметров адаптера**, расположенный в левой части окна.

По сравнению с ОС Windows Vista появилось еще одно свойство сетевого подключения, которое следует указывать при первом его использовании. Это тип сети. Сеть может быть **Домашней**, **Рабочей** и **Публичной**. Отличия заключаются в том, что для каждого типа сети предусмотрены свои настройки брандмауэра. Самая низкая защита компьютера при работе в **Домашней** сети, самая высокая — в **Публичной**.

Настраивая Windows 7, вы обнаружите еще некоторые особенности этой системы, но отличия от Windows Vista не столь существенны, чтобы их отдельно описывать.

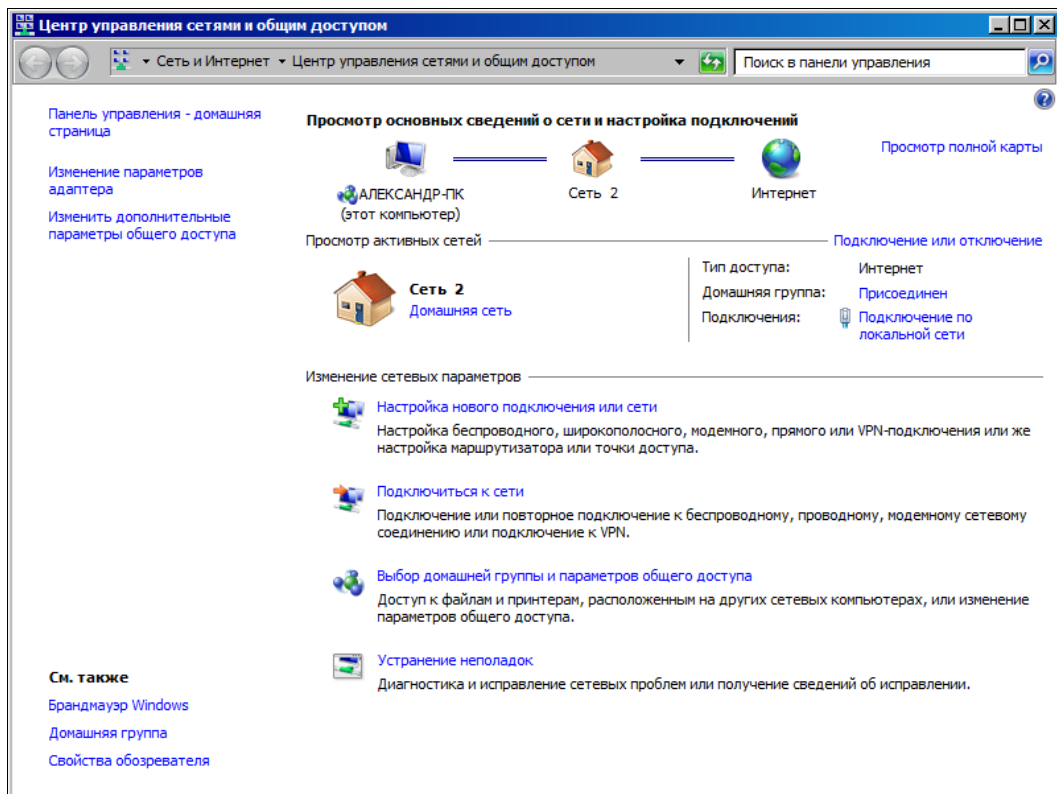


Рис. 1.62. Окно Центр управления сетями и общим доступом

## Соединяем компьютеры через Интернет

Этот вариант объединения компьютеров довольно сложен, и мы подробно рассмотрим варианты его реализации позднее в *главе 4*. Пока только отметим, что вычислительные сети могут быть построены не только с применением кабеля, Wi-Fi, Bluetooth или других адаптеров.

Еще в 60-е годы в США появилась услуга Centrex, позволявшая на базе существующих телефонных сетей создавать (тогда этот термин еще не применялся) виртуальную сеть, которая не имела привязки к определенной АТС. Абоненты такой сети могли находиться везде, где есть телефонные линии. Постепенно подобный подход к организации сетей передачи данных проник и в компьютерные сети, а также в Интернет.

Когда-то создание виртуальной сети было возможно только для организаций, которым требовалось защитить свои данные при передаче по каналам связи. Теперь практически каждый может воспользоваться достижениями компьютерных технологий, создав свою собственную виртуальную сеть, объединяющую домашний и офисный компьютеры или персональные компьютеры двух друзей. Учитывая, что доступ в Интернет стал достаточно простым, а в крупных городах есть несколько

вариантов беспроводного подключения к Интернету, есть возможность объединить свой мобильный и домашний компьютер в одну виртуальную сеть. Кроме того, можно расширить эту сеть, подключив в нее компьютеры родственников и друзей. Конечно, качество подключения к Интернету наложит отпечаток на скорость передачи данных по такой сети. Но автор этих строк не очень расстраивается, когда при передаче файла с удаленного на 80 км компьютера приходится подождать минутую-другую. А когда друзьям, подключенным к этой сети, требуется помощь, достаточно подключиться к компьютеру, пользователь которого ожидает помощи, и выполнить необходимые действия для решения проблемы. При этом, можно сидеть в кафе, где есть возможность бесплатного подключения к сети Интернет через Wi-Fi, или в любом месте, где есть возможность использовать мобильный Интернет от операторов сотовой связи или Mobile WiMax от Yota (Скартел).

Выглядит заманчиво?

Тогда продолжаем чтение следующих глав книги.

## ГЛАВА 2



# Создаем одноранговую сеть

В главе 1 мы коснулись вопроса организации сетевой связи между двумя компьютерами. Но, где есть два компьютера, со временем обязательно появятся и третий, и четвертый... То есть получится настоящая локальная сеть. Вот тут-то появляется простор для творчества. Как должна быть устроена наша сеть? Какими возможностями она будет обладать? Какие устройства понадобятся для нормальной и удобной работы сети? Как, в конце концов, это все настроить? Да, и к Интернету хотелось бы подключить все компьютеры сети. Не заказывать же для каждой рабочей станции отдельное подключение у провайдера! Нет, этого делать не надо. Современная операционная система для персонального компьютера содержит в своем составе средства, которые позволяют подключить все компьютеры небольшой локальной сети к Интернету, используя единственное существующее подключение, настроенное на одной машине. Но, давайте будем решать проблемы по мере их поступления.

## Настраиваем сетевое подключение

Задача состоит в том, чтобы подключить к уже имеющейся сети из двух компьютеров третий ПК. На первый взгляд ничего сложного в задаче нет. Коммутатор мы уже поставили, мастер настройки сети запускали — можно подключить третий компьютер и снова запустить **Мастер настройки сети**. Но, если вы думаете о расширении сети, а не просто о добавлении третьего компьютера, придется окунуться в проблему глубже. Любая автоматическая настройка с помощью мастера позволяет добиться лишь начального результата. Например, мастер настройки сети не позволяет выбрать произвольный IP-адрес для сети. Во-первых, многим это не понравится просто потому, что это ограничение права на собственный выбор, а во-вторых, IP-адрес компьютера может быть задан другими условиями при решении различных сетевых задач. Отсюда вывод — на мастеров надейся, а сам не плошай! Будем настраивать сетевые подключения с заранее заданными параметрами.

Приступим.

В качестве исходных данных для решения задачи примем следующее:

- каждый компьютер уже имеет сетевую карту;
- у вас уже есть все необходимое для обжима кабелей и патчкордов или кабели и патчкорды уже заготовлены;
- у вас есть дополнительная сетевая карта и есть компьютер, в который ее можно установить (пригодится для настройки доступа в Интернет через ADSL-модем);
- у вас есть обычный модем, через который тоже можно предоставить доступ в Интернет клиентам сети;
- на компьютерах установлена операционная система не ниже Windows 98 или более новая;
- самое главное условие — вы знаете, зачем вам нужна сеть!

## Сетевое подключение в одноранговой сети

Итак, все готово для настройки сети.

Дальнейшие действия в некоторой степени зависят от версии операционной системы, которая установлена на ваших компьютерах. Если вы все еще используете Windows 95, то убедитесь, что это версия OSR2, в которой есть встроенная поддержка необходимых для работы сети функций, или установите хотя бы Windows 98. Подавляющее большинство компьютеров, работающих в настоящее время, позволяют использовать эту операционную систему. Мы будем ориентироваться на Windows 98 и более поздние версии.

Компьютеры одноранговой сети совершенно равноправны. Поэтому и настройки каждого компьютера в основном одинаковы. Отличаться, главным образом, будут индивидуальные характеристики, которые позволяют идентифицировать компьютер в сети.

Рассмотрим настройку компьютера с операционной системой Windows 98.

Для доступа к настройкам такого компьютера необходимо 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 кнопкой мыши откройте одноименное окно.
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.
5. Для вставки компонентов нажмите кнопку **Добавить**, откроется окно **Выбор типа компонента**. В этом окне выберите тип, например, **Клиент, Протокол** или **Служба** в соответствии с типом устанавливаемого компонента. После выбора типа компонента станет доступной кнопка **Добавить**. Нажав на нее, вы сможете указать необходимый компонент.

6. 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 адаптером, а другой — с *контроллером удаленного доступа*, который уже установлен. Это необходимо учесть при настройке сети. Протокол, работающий с контроллером удаленного доступа, настраивать не следует, чтобы не испортить подключение к Интернету.
7. Выбирать следует компоненты, разработанные корпорацией Microsoft.
8. Для работы одноранговой сети, построенной на компьютерах под управлением Windows 9x, потребуется также протокол NetBEUI.
9. Настройка компьютера с операционной системой Windows 2000 начинается так же, как и для Windows 98, но в **Панели управления** надо искать значок **Сеть и удаленный доступ к сети**. Далее, в открывшемся одноименном окне следует выделить значок **Подключение по локальной сети**, щелкнув по нему правой кнопкой мыши, и, выбрав пункт меню **Свойства**, открыть диалоговое окно **Подключение по локальной сети — свойства**, которое позволит установить необходимые компоненты, как это уже было описано ранее.

В Windows XP название значка на панели управления — **Сетевые подключения**.

#### **ПРИМЕЧАНИЕ**

При описании настроек для Windows XP здесь и далее мы будем использовать классический вид рабочего стола и меню **Пуск**. Для реализации классического вида настроек достаточно в свойствах **Панели задач** и меню **Пуск** установить переключатель **Классическое меню "Пуск"**.

Кроме того, 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 nbfsys 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.

Для совместимости со старыми компьютерами, работающими под управлением операционных систем Windows 9x, установите также драйвер сетевого монитора, который появится в списке протоколов после установки протокола NetBEUI.

Завершив установку компонентов, можно приступить к их настройке.

Для того чтобы не потерять выполненные для каждого протокола настройки, после их изменения необходимо каждый раз закрывать окно **Подключение по локальной сети — свойства** для Windows XP/2000 или **Сеть** для Windows 9x. Более того, в Windows 9x лучше перезагружать систему после любого применения выбранных настроек.

Сам протокол NetBEUI не требует настройки.

Теперь проверим сетевую идентификацию компьютера. Для этого в Windows 9x откроем окно **Сеть** и выберем вкладку **Идентификация**.

Имя каждого компьютера в вашей сети должно быть уникальным. Имя *рабочей группы* может быть любым, но если вы хотите, чтобы все компьютеры сети были сразу видны в сетевом окружении (об этом окне будет рассказано несколько позже), то лучше для всех компьютеров небольшой сети выбрать одну рабочую группу. Это особенно важно, когда вы используете компьютеры с Windows 2000/XP в вашей сети. Для этих операционных систем рабочая группа — это не просто группа компьютеров, а *домен*, т. е. часть большой сети, объединенная общими свойствами. "Чужая" рабочая группа может быть и не видна в сетевом окружении, а ее компьютеры придется обнаруживать с помощью средств поиска компьютеров в сети. Но если вы считаете необходимым создание нескольких рабочих групп, или будут использоваться несколько файловых серверов (для каждой рабочей группы свой сервер), то можно давать различные имена и рабочим группам. Единственное ограничение, которое следует учитывать, присваивая имена компьютерам и рабочим группам, — это запрет на использование специальных символов, пробелов и символов кириллицы.

Для компьютеров с Windows XP/2000 доступ к настройкам идентификации осуществляется с помощью значка **Мой компьютер** на рабочем столе. Необходимо, щелкнув по нему правой кнопкой мыши, выбрать пункт меню **Свойства**, а затем — перейти на вкладку **Сетевая идентификация**, на которой нажать кнопку **Свойства** и выполнить необходимые изменения в открывшемся окне.

На компьютерах с операционной системой Windows XP немного отличаются названия вкладок, но это не вызовет затруднений.

Интересно, что в старых операционных системах Windows 9x имя компьютера и сетевая идентификация компьютера могут отличаться. Новые версии операционных систем ориентированы преимущественно на работу в сети, и имя компьютера совпадает с его идентификационным именем в сети.

Теперь следует настроить протокол TCP/IP.

На компьютерах с Windows 9x откройте окно **Сеть** и выделите протокол TCP/IP, связанный с сетевым адаптером. Нажмите кнопку **Свойства**. Установите необходимые свойства протокола. Можно ввести фиксированный сетевой адрес или выбрать автоматическое назначение адреса.

Для компьютера с Windows XP/2000 откройте окно **Подключение по локальной сети** — **свойства** и, выделив протокол TCP/IP, нажмите кнопку **Свойства**. В открывшемся окне можно ввести фиксированный сетевой адрес или задать режим автоматического назначения адреса.

Для небольшой сети, не связанной с другими сетями и Интернетом, сетевые адреса могут быть установлены явно. Важно, чтобы эти адреса не повторялись в сети. Если в одно и то же время в сети окажутся два компьютера с одним значением сетевого адреса — возможно нарушение работы сети.

Можно и не присваивать конкретных значений адресов, оставив их выбор на усмотрение компьютера. Все версии Windows, начиная с Windows 98, могут самостоятельно назначить себе IP-адрес, обеспечивая его уникальность.



После завершения всех настроек и перезагрузок компьютеры одноранговой сети "увидят" друг друга в сетевом окружении. Мы можем убедиться в этом, найдя на рабочем столе значок **Сетевое окружение** и открыв его двойным щелчком мыши.

Настройку подключения для Windows Vista и Linux мы достаточно подробно рассмотрели в *главе 1*. Как и в старых версиях Windows, следует обратить внимание на идентификацию компьютера в сети. Указать или изменить имя компьютера и рабочей группы в ОС Windows Vista можно в свойствах системы. Откройте **Панель управления | Система** (рис. 2.1). В разделе **Имя компьютера, имя домена и параметры рабочей группы** найдите ссылку **Изменить параметры**. Нажав на эту ссылку, вы откроете окно **Свойства системы**, где можно внести необходимые записи или выполнить их изменения.

Несколько иначе устанавливается имя компьютера в Linux. Эта операционная система имеет как свои собственные сетевые протоколы, так и совместимые с Windows. Для работы в сетях Windows применяется клиент и сервер Samba. Установить принадлежность компьютера к рабочей группе Windows можно в настройках сервера Samba.

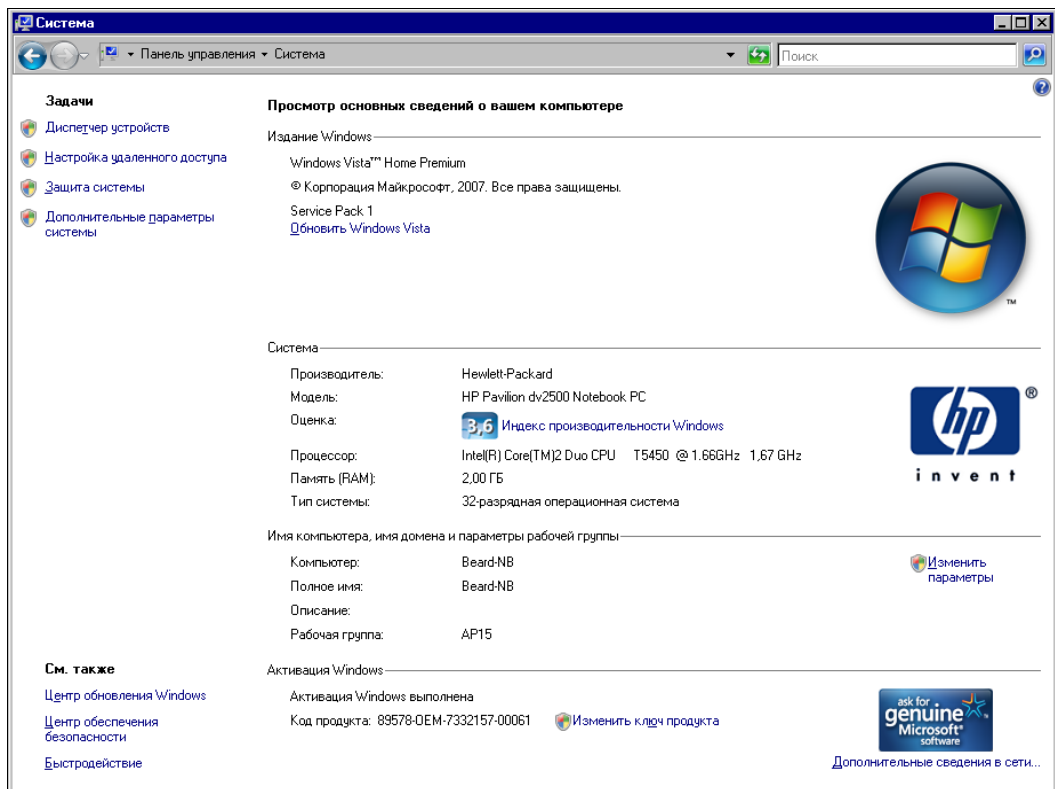


Рис. 2.1. Окно Система

## Настройка сервера Samba в Linux

Рассмотрим настройки этого сервера в Mandriva Linux 2008. К сожалению, пока нет стандарта для интерфейса Linux, поэтому в других версиях он будет выглядеть иначе. Но поскольку суть настроек не изменится, вы сможете выполнить их и в других Linux.

Откройте Система | Администрирование | Настройка компьютера | Сетевые службы | Сервер Samba. Откроется первое окно **Мастера настройки сервера Samba** (рис. 2.2), в котором следует выбрать роль вашего компьютера в сети. В иерархических сетях существует понятие *Контроллера домена*. Это сервер, который позволяет управлять всей сетью, производить авторизацию пользователей сети, идентифицировать компьютеры, входящие в нее. Но для одноранговой сети достаточно, чтобы каждый компьютер, входящий в нее, выполнял некоторые функции сервера, например обеспечивал доступ других пользователей к общим ресурсам. Поэтому мы выбираем опцию **Standalone — отдельный сервер**. В рабочей группе каждый компьютер работает самостоятельно, не требуя наличия некоего главного сервера.

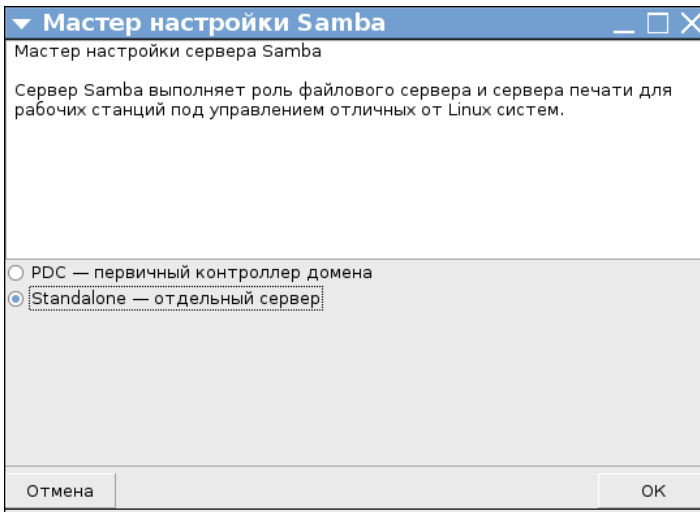


Рис. 2.2. Окно **Мастер настройки Samba** — **Мастер настройки сервера Samba** (выбор роли компьютера)

Нажав кнопку **ОК**, мы попадем в окно **Мастер настройки сервера Samba — Рабочая группа** (рис. 2.3). В этом окне следует указать имя рабочей группы и компьютера. Сама операционная система Linux не использует понятие рабочей группы, а для Windows Vista принадлежность компьютера к рабочей группе ускоряет его поиск в сети. Для других Windows принадлежность к рабочей группе значительно важнее. Вы можете не "увидеть" в сетевом окружении компьютер, если он принадлежит к другой рабочей группе.

Введя необходимые значения имен рабочей группы и компьютера и нажав кнопку **ОК**, переходим к окну **Мастер настройки сервера Samba — Режим без-**

опасности (рис. 2.4). В этом окне наш выбор не велик. Поскольку центрального сервера нет, **Режим безопасности** имеет только значение **user**. Это значит, что компьютер будет определять права пользователя на доступ к ресурсам по его имени. В одноранговой сети необходимо иметь одинаковые учетные записи на разных компьютерах, чтобы иметь возможность доступа к сетевым компьютерам. В поле **Разрешённые хосты** можно ввести имена или адреса компьютеров, которым разрешен доступ к данному. Можно не вводить ничего. В этом случае все компьютеры сети будут иметь доступ к серверу Samba, который мы настраиваем.

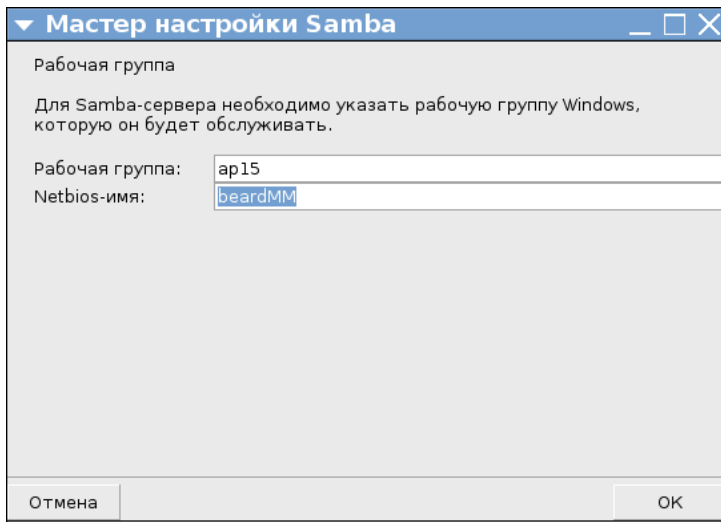


Рис. 2.3. Окно **Мастер настройки сервера Samba** — **Рабочая группа**

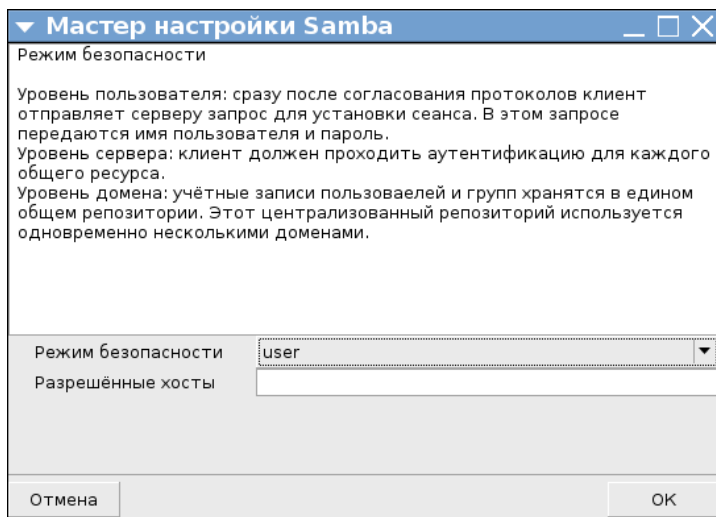


Рис. 2.4. Окно **Мастер настройки Samba** — **Режим безопасности**

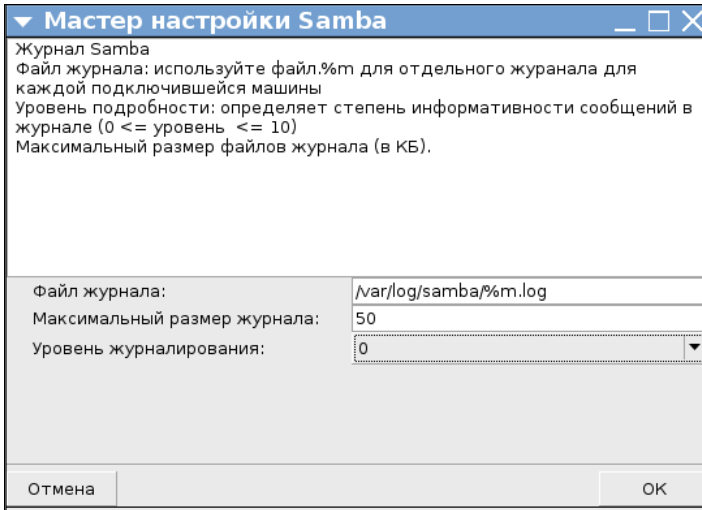


Рис. 2.5. Окно **Мастер настройки Samba — Журнал Samba**

В следующем окне мастера (рис. 2.5) **Мастер настройки Samba — Журнал Samba** можно ничего не изменять. Впоследствии, осваивая Linux, вы сможете самостоятельно настроить параметры журнала. Журнал это просто файлы, в которые записываются события сервера, такие как доступ к файлам, авторизация пользователя, ошибки в работе сервера и др.

В следующем окне мастера (рис. 2.6) **Мастер настройки Samba — Описание сервера** также ничего не меняем. Но при желании вы можете внести свое описание сервера. Важно, чтобы в описании применялась латиница. В противном случае Windows-компьютеры могут не прочесть его ввиду различных используемых кодировок.

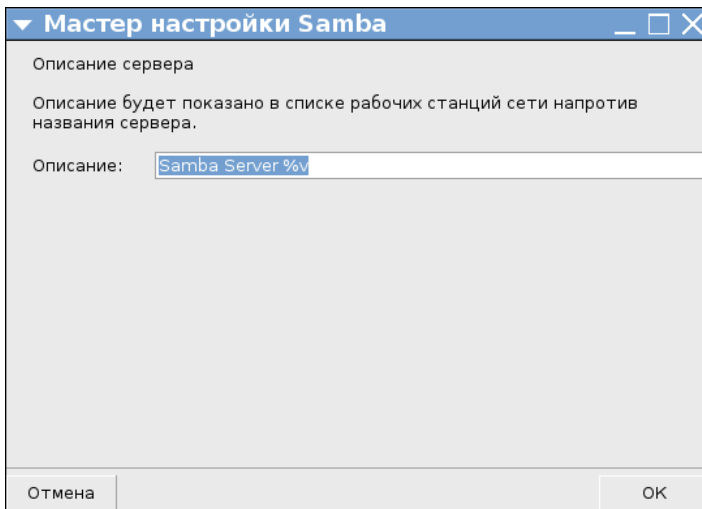


Рис. 2.6. Окно **Мастер настройки Samba — Описание сервера**

В завершающем окне мастера (рис. 2.7) можно убедиться в том, что настройки сервера соответствуют нашим пожеланиям. Если что-либо вас не устраивает, можно отменить настройки, нажав кнопку **Отмена**, и выполнить их заново. Нажатие кнопки **ОК** приведет к сохранению настроек.

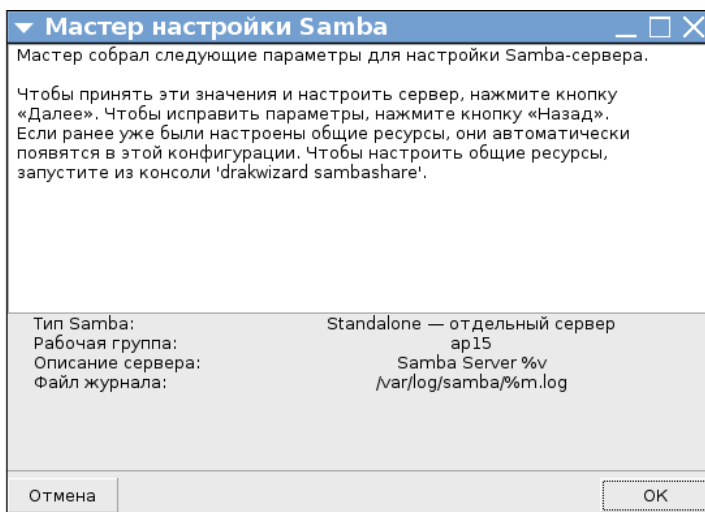


Рис. 2.7. Окно **Мастер настройки Samba**. Сведения о выполненных настройках

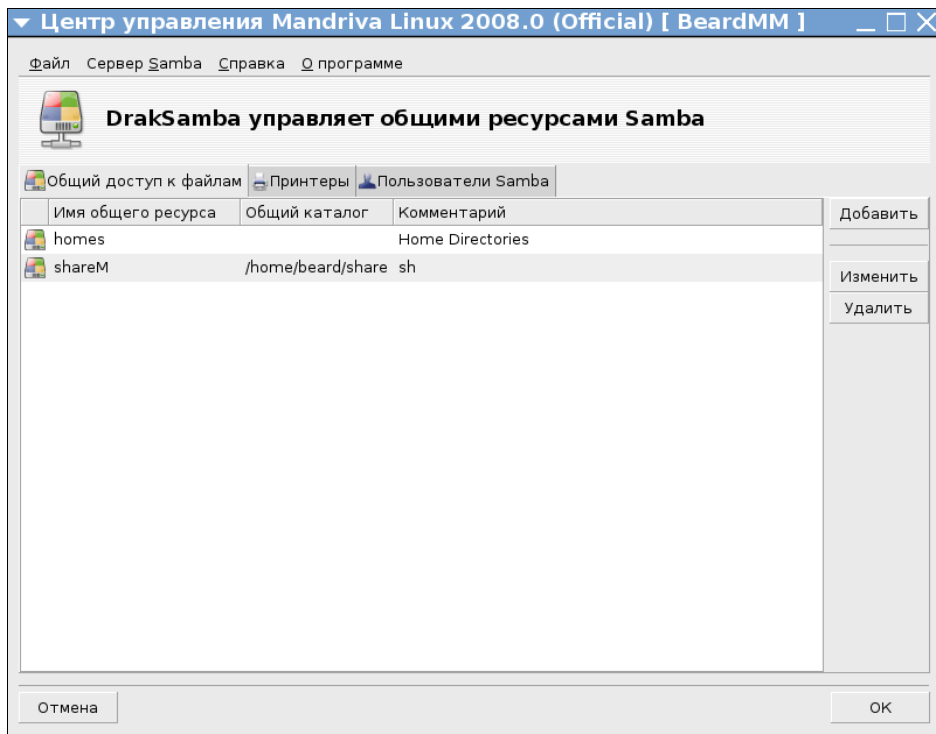


Рис. 2.8. Окно **Центр управления Mandriva Linux 2008** для сервера Samba

При этом откроется окно **Центр управления Mandriva Linux 2008** для сервера Samba (рис. 2.8), где можно выполнить дополнительные настройки, например, указать общие ресурсы, выбрать пользователей, которые должны иметь доступ к общим ресурсам.

## Подключаем общий принтер

Раз уж у нас есть сеть, необходимо максимально использовать ее возможности. Работа на персональном компьютере предполагает, что время от времени появляется необходимость напечатать только что созданный или полученный по электронной почте документ. Если для отдельно стоящего (не включенного в сеть) компьютера принтер обычно является необходимым устройством, то сетевая рабочая станция вполне может обойтись без принтера. Важно лишь иметь принтер в сети. А если он есть, необходимо предоставить его в общее пользование для всех клиентов сети.

Во всех версиях Windows процедуры настройки сети во многом схожи. Поэтому при рассмотрении подключения общего принтера будем рассматривать настройки для ОС Windows Vista, а в других версиях вы сможете выполнить настройки самостоятельно.

## Общий принтер в Windows Vista

Принтер, может быть, и не дорогое устройство, но дома он должен иметь свое место. Даже если у вас всего два компьютера и находятся они недалеко друг от друга, разместить рядом два принтера бывает не очень просто. Особенно если один компьютер стационарный, а другой ноутбук, не занимающий постоянного места на компьютерном столе. Конечно, можно отключать принтер от домашнего компьютера и подключать к ноутбуку, когда требуется распечатать документ. Но намного удобнее просто послать документ на печать через сеть на установленный принтер.

Принтеры требуют установки *драйверов* — программ, управляющих работой этих устройств. Обычно драйверы находятся на диске, прилагаемом к принтеру при продаже. Нередко драйверы известных принтеров содержатся и в самой операционной системе. Процедура установки принтера не вызывает проблем, поскольку на диске или в бумажном виде всегда приложена инструкция по установке. Не намного сложнее и обеспечение сетевого доступа к установленному принтеру. Тем не менее, у пользователей Windows Vista нередко возникают проблемы с подключением к принтеру по сети. Множество существующих драйверов принтеров разрабатывались для Windows XP и более ранних систем. Старые драйверы зачастую работают не совсем корректно с Windows Vista. Необходимо устанавливать самые последние драйверы с сайтов производителей принтеров. Для принтеров Hewlett-Packard выпущен универсальный драйвер HP LaserJet Universal Print Driver, под управлением которого работают практически все принтеры HP. Загрузить этот драйвер можно со страницы по ссылке, приведенной далее.

<http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=us&prodTypeId=18972&prodSeriesId=74341&prodNameId=74343&swEnvOID=228&swLang=8&mode=2&taskId=135&swItem=ja-35999-21>

Настраивая сетевой доступ к общему принтеру в Windows Vista, желательно удалить все имеющиеся принтеры. В противном случае нет гарантии, что установка и подключение пройдут без ошибок.

Для предоставления доступа к принтеру (считаем, что он уже установлен) необходимо сделать следующее:

1. Откройте окно свойств принтера. Установленные принтеры можно найти в папке **Пуск | Панель управления | Принтеры**. Щелкните правой кнопкой по значку выбранного принтера и выберите пункт **Свойства**. В открывшемся окне перейдите на вкладку **Доступ** (рис. 2.9).

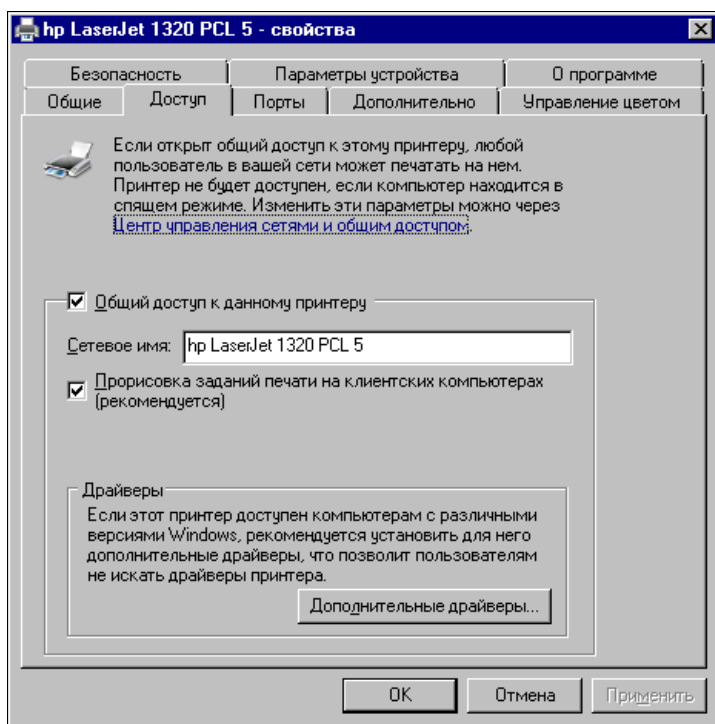


Рис. 2.9. Окно свойств принтера

2. Выберите переключатель **Общий доступ к данному принтеру**.
3. Нажмите кнопку **ОК**.
4. Теперь перейдите на компьютер, с которого хотите получить доступ к принтеру. Конечно, компьютер должен быть подключен к вашей сети.
5. Войдите в Центр управления сетями и общим доступом (**Пуск | Настройка | Панель управления | Центр управления сетями и общим доступом**).

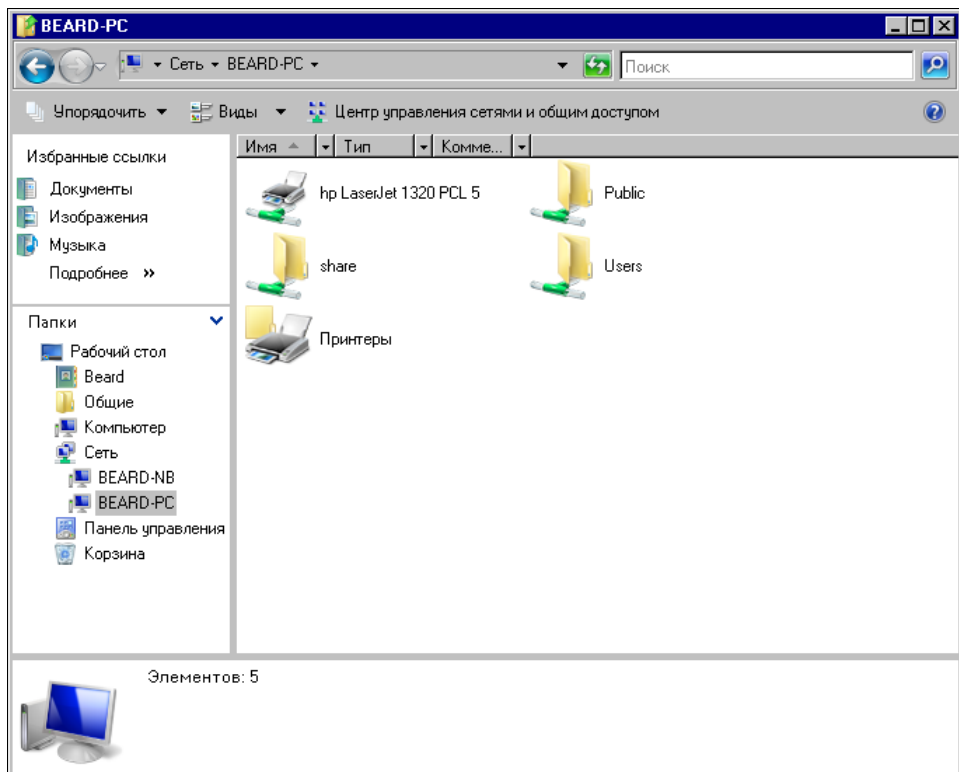


Рис. 2.10. Окно Сеть BEARD-PC

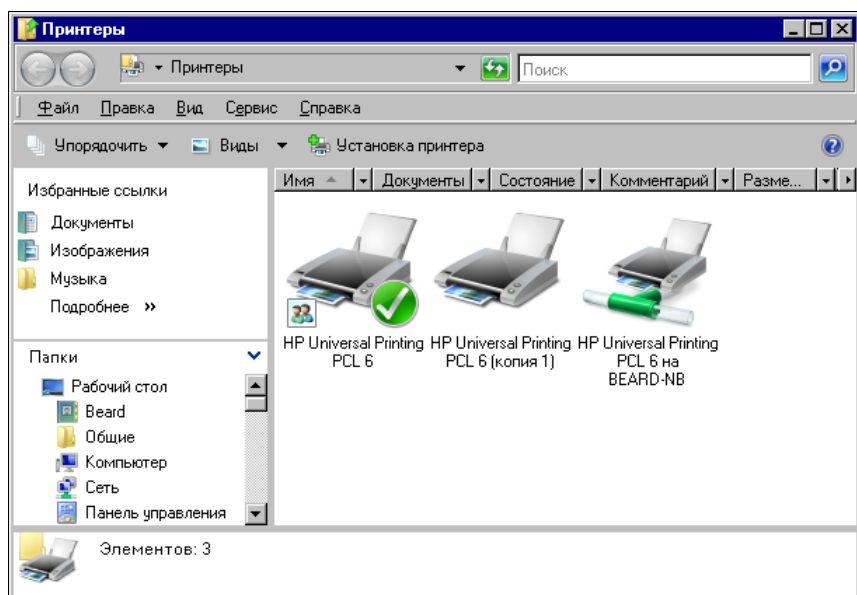


Рис. 2.11. Окно Принтеры



6. В левой части окна выберите задачу **Просмотр компьютеров и устройств**. Откроется окно **Сеть**. Найдите в сети компьютер с подключенным принтером и откройте его (рис. 2.10).
7. Выберите подключаемый принтер и в контекстном меню (после щелчка правой кнопкой) выберите пункт **Подключить**. Если драйверы установлены верно и полностью совместимы с Windows Vista, принтер будет подключен.

На рисунке (рис. 2.11) приведено изображение папки **Принтеры**, в которой содержится (слева направо) локальный принтер с общим доступом, включенный по умолчанию, локальный принтер без общего доступа, подключение к принтеру на компьютере BEARD-NB.

## Подключение из Linux

Настроив доступ к принтеру в Windows Vista, можно подключаться к нему и из Linux. Это не сложнее, чем подключение из Windows Vista. Скорее, даже проще. В Linux содержится множество универсальных драйверов принтеров, что позволяет подключаться к принтеру в сети, марка которого не известна, но известен его тип. В ASP Linux это делается следующим образом:

1. Откройте окно **Настройка принтера** (рис. 2.12), пройдя по пути **Система | Администрирование | Печать**.
2. Нажмите кнопку **Создать**.
3. Выберите **Сетевой принтер Windows (SMB)**. Укажите драйвер **PCL 6**.
4. Поиск принтера в сети может быть продолжительным и даже неудачным, поэтому введите вручную адрес принтера //10.15.0.6/HP\_PCL6. Здесь указан адрес компьютера, к которому подключен принтер и сетевое имя принтера.
5. Система проверит доступность принтера в сети, потребует ввести имя и пароль пользователя, которому разрешен доступ к принтеру. Принтер создан.

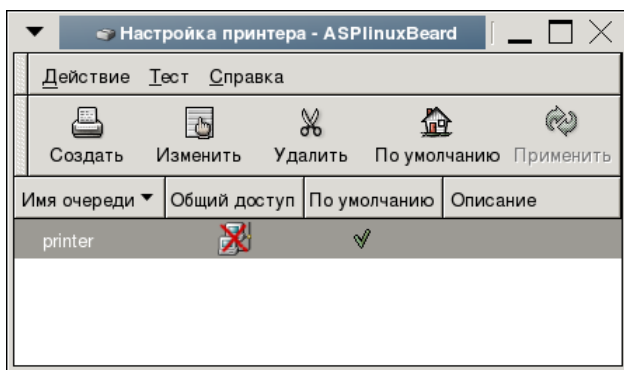


Рис. 2.12. Окно **Настройка принтера** — ASPIlinuxBeard

Теперь можно печатать документы, созданные в Linux, на принтере, подключенном к компьютеру под управлением Windows Vista.

## Общий принтер в Linux

Возможно, что вам больше подходит вариант подключения к принтеру через компьютер с операционной системой Linux. Подключимся к принтеру на машине с Mandriva Linux.

Сначала установим принтер на эту машину.

1. Подключите принтер к компьютеру и включите его.
2. Перейдите в **Центр управления Mandriva Linux**, пройдя по пути **Система | Администрирование | Настройка компьютера** (рис. 2.13).
3. Выберите в левой части окна **Оборудование**, а в правой **Настройка принтеров и очередей печати**. Откроется окно **Printerdrake** (рис. 2.14), в котором следует нажать кнопку **Да**. На другие вопросы системы также отвечайте положительно.

### ПРИМЕЧАНИЕ

Подробно о работе с этой утилитой можно прочитать по адресу в Интернете <http://www.linuxcookbook.ru/books/mandriva/printerdrake.html>.

4. В открывшемся окне **Найден новый принтер** (рис. 2.15) снова согласитесь с предложением системы установить принтер автоматически, нажав **ОК**. Откроется окно **Центр управления Mandriva Linux — Принтеры**, в котором вы увидите строку с именем установленного принтера.

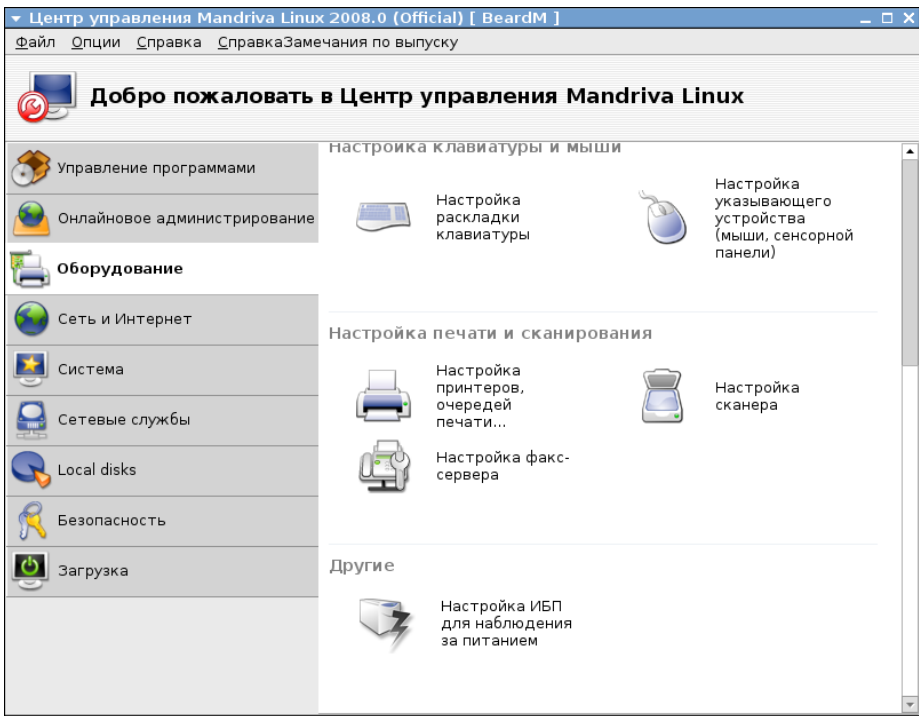


Рис. 2.13. Окно **Центр управления Mandriva Linux**

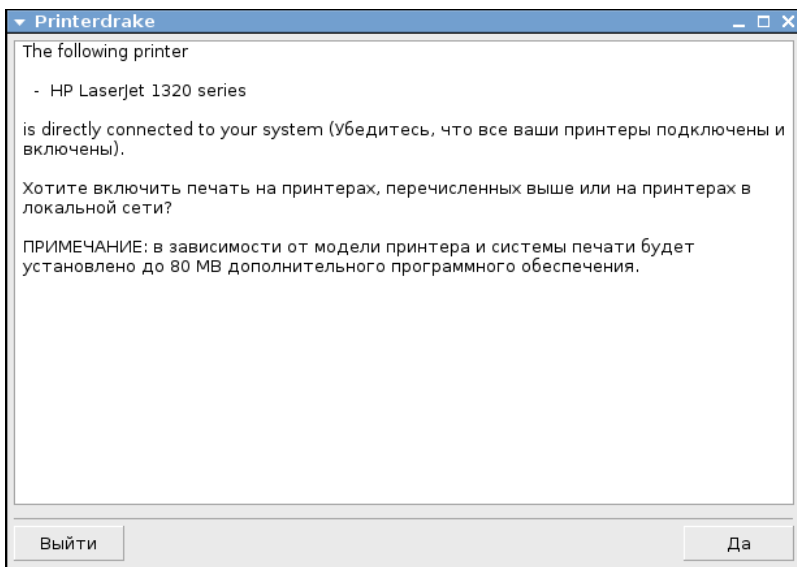


Рис. 2.14. Окно Printerdrake

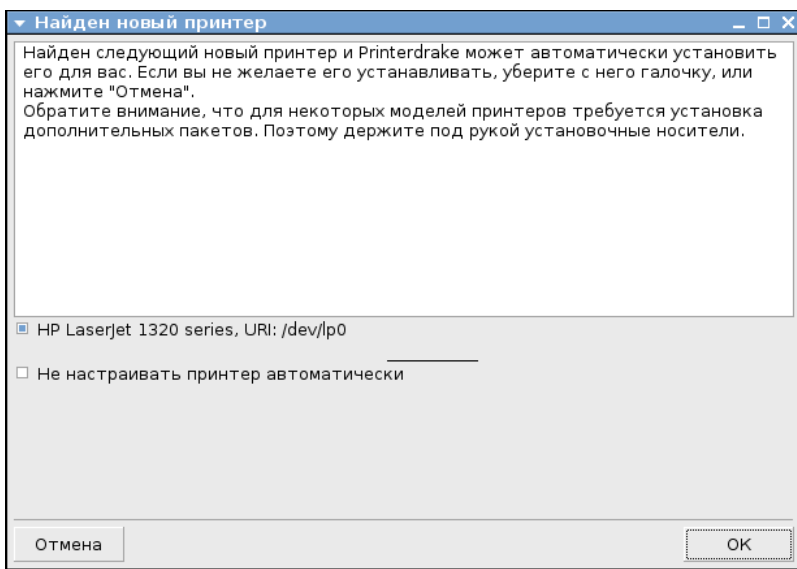


Рис. 2.15. Окно Найден новый принтер

Все, принтер установлен. В этом можно убедиться, посмотрев на открывшееся окно **Центр управления Mandriva Linux — Принтеры** (рис. 2.16). По умолчанию к нему открыт общий доступ. Вы можете распечатать какой-либо документ для проверки его работоспособности.

Подключаясь к принтеру с компьютера под управлением Windows Vista, необходимо указать драйвер этого принтера (рис. 2.17). Следует выбирать самую новую версию драйвера из установленных в системе.

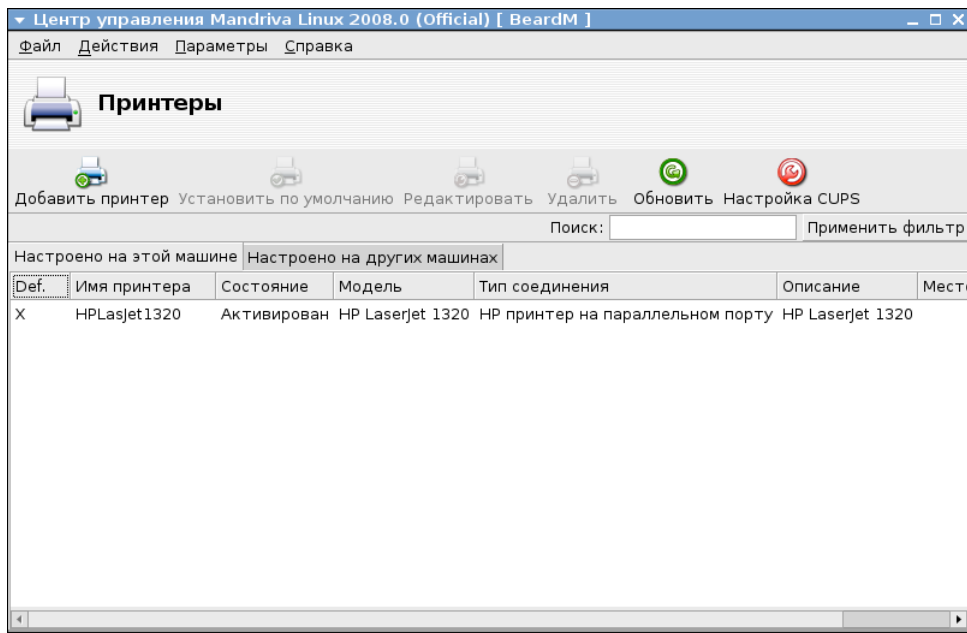


Рис. 2.16. Окно Центр управления Mandriva Linux — Принтеры

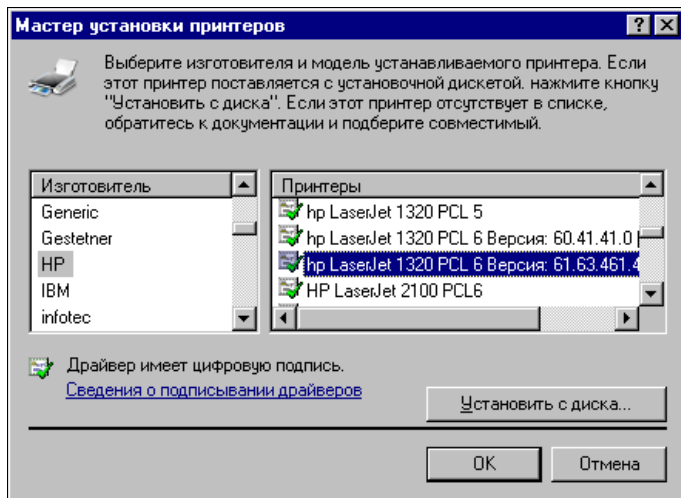


Рис. 2.17. Окно Мастер установки принтеров

Подключенный принтер можно увидеть в папке **Принтеры** (рис. 2.18). Можно использовать этот принтер для печати документов.

Подключение к принтеру из Linux мы уже рассматривали ранее. Если к принтеру предоставлен общий доступ, то не имеет существенного значения в какой ОС он установлен. Подключение к нему можно выполнять также из любой операционной системы.

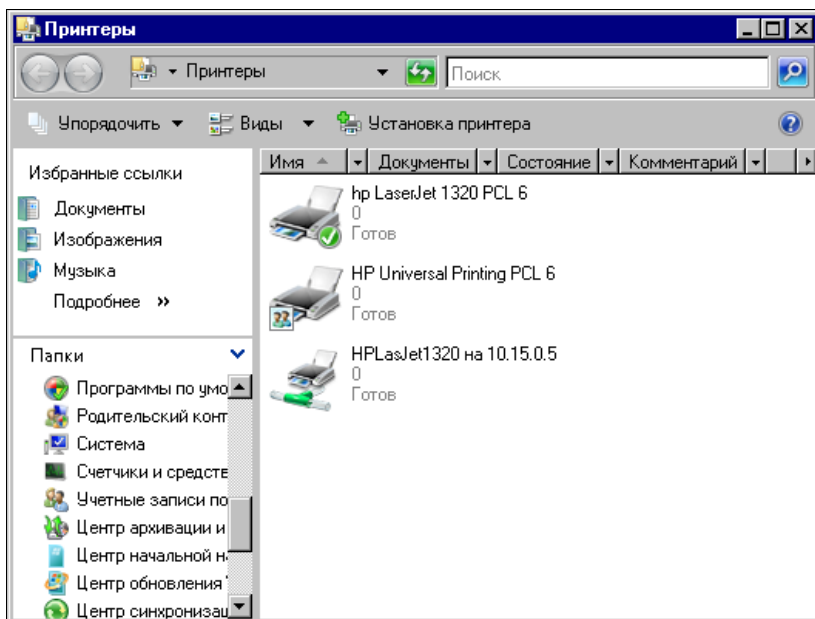


Рис. 2.18. Окно Принтеры

## Подключаем сеть к Интернету

Подключение всей сети к Интернету дает нам возможность использовать только одно реальное подключение. Конечно, их может быть несколько. У автора, например, есть и подключение через обычный аналоговый модем, и подключение через ADSL-модем, и подключение через Bluetooth-модем... Но эти подключения существуют в единственном экземпляре и могут использоваться всеми компьютерами домашней сети. Даже пришедший в гости друг может подключить свой ноутбук к домашней сети и получить доступ в Интернет.

Прежде чем мы начнем рассматривать настройку общего подключения, следует сделать небольшое теоретическое отступление. Дело в том, что в глобальной сети Интернет используется *DNS* (Domain Name System — система доменных имен). Это 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. Адреса сайтов в Интернете публикуются в символьном виде. Например, адрес известного поисковика Google — <http://google.ru>. Такой адрес называется также DNS-именем. Специальные DNS-серверы содержат в своей памяти таблицы соответствия символьных адресов IP-адресам компьютеров и серверов, где физически расположены сайты. При подключении к Интернету необходимо указывать компьютеру IP-адреса DNS-серверов, где необходимо искать эти таблицы. DNS-серверы работают переводчиками имен сайтов с языка людей на язык машин и обратно.

Вот теперь можно заняться настройкой подключения сети к Интернету.

## Настройка в старых версиях Windows

Для настройки общего доступа к подключению Интернета необходимо убедиться, что операционная система, установленная на этом компьютере, не ниже Windows 98 SE. Если вы хотите выполнить такие настройки для более ранних систем, вам придется обратиться к дополнительной литературе для более подробного изучения возможностей настройки маршрутизации для Windows 95/98<sup>1</sup>. На компьютере с операционной системой Windows 98 SE легко установить общий доступ к подключению Интернета, используя стандартные средства.

Для настройки такого доступа необходимо проделать следующее:

1. Нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, дважды щелкните кнопкой мыши значок **Установка и удаление программ** и перейдите на вкладку **Установка Windows**.
2. Выберите строку **Средства Интернета** и нажмите кнопку **Состав**.
3. Выберите **Общий доступ к подключению Интернета** и нажмите кнопку **ОК**. Если установка Windows выполнялась с компакт-диска, будет выведено приглашение вставить компакт-диск в компьютер.
4. Следуйте указаниям Мастера общего доступа к подключению Интернета.

После успешной установки выбранного компонента **Общий доступ к подключению Интернета** должен появиться в списке средств Интернета, входящих в состав операционной системы в окне **Средства Интернета**.

## Настройка компьютера общего доступа к Интернету

Для настройки компьютера общего доступа к Интернету выполните следующие действия:

1. Откройте вкладку **Подключение** в диалоговом окне **Свойства обозревателя**.
2. Для этого нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, дважды щелкните значок **Свойства обозревателя**, выберите вкладку **Подключение** и нажмите кнопку **Доступ** в группе **Настройка локальной сети**.
3. Если кнопка **Доступ** отсутствует в группе **Настройка локальной сети**, необходимо запустить Мастер общего доступа к подключению Интернета. Мастер назначит компьютеру общего доступа к подключению Интернета IP-адрес 192.168.0.1. Остальным компьютерам домашней сети могут быть назначены любые статические IP-адреса из диапазона 192.168.0.2—192.168.0.254.
4. В открывшемся окне **Internet Connection Sharing** (Общий доступ к подключению Интернета) введите следующие параметры (табл. 2.1).

---

<sup>1</sup> Поляк-Брагинский А. В. Сеть своими руками. — СПб: БХВ-Петербург, 2002. — 320 с.

Таблица 2.1. Параметры настройки общего доступа к подключению Интернета

Параметр	Описание
Разрешить общий доступ к подключению Интернета	Переключатель обеспечивает включение или отключение общего доступа к подключению Интернета
Выводить значок на панель задач	Установка этого переключателя добавляет значок общего доступа к подключению Интернета на панель задач. Значок показывает число подключенных в данное время компьютеров и выводит контекстное меню, содержащее параметры общего доступа к подключению Интернета
Выберите подключение удаленного доступа, используемое для доступа к Интернету	Из списка соединений следует выбрать то подключение, которое применяется для доступа к Интернету
Выберите сетевой адаптер, используемый для доступа к домашней сети	Из списка адаптеров нужно выбрать тот сетевой адаптер, который применяется для доступа к домашней сети

## Настройка остальных компьютеров сети

Для настройки остальных компьютеров сети выполните:

1. Откройте диалоговое окно **Сеть**. Для этого можно нажать кнопку **Пуск**, выбрать команды **Настройка** и **Панель управления**, а затем дважды щелкнуть кнопкой мыши значок **Сеть**.
2. Выберите в окне **Сеть** адаптер **TCP/IP(домашний) →... Ethernet** в списке **В системе установлены следующие компоненты**.

### ПРИМЕЧАНИЕ

Если настраиваемый компьютер не обеспечивает общий доступ к подключению Интернета для других компьютеров, то слова "домашний" может и не быть, сразу за символами "TCP/IP" может следовать название (тип) сетевого адаптера.

3. Нажмите кнопку **Свойства**.
  - Для того чтобы автоматически назначить IP-адрес, выберите опцию **Получить IP-адрес автоматически**. Если при этом в сети нет сервера DHCP, то компьютер автоматически назначит себе IP-адрес. То же произойдет и в случае сбоя в сети с включенной службой DHCP. После восстановления работы службы DHCP личный адрес будет отброшен и восстановлено получение адреса от сервера.
  - Для установки статического IP-адреса выберите переключатель **Указать IP-адрес явным образом**, а затем введите IP-адрес. Назначение статического IP-адреса отменяет динамическое получение адресов с серверов DHCP.

Как правило, личные автоматические IP-адреса используют пространство сетевых IP-адресов LINKLOCAL и формат 169.254.X.X. Сети с общим доступом к подключению Интернета применяют адреса из диапазона 192.168.0.xxx.

Правильно выбранные адреса компьютеров не вызовут затруднений в работе сети, но Microsoft рекомендует назначение IP-адресов доверять серверу, несмотря на то, что наша сеть одноранговая.

В Windows 98 протокол Microsoft TCP/IP обеспечивает механизм IP-адресации, который называют *автоматическим назначением личных IP-адресов*. Если есть небольшая сеть, в которой отсутствует служба DHCP, можно назначить сетевому адаптеру уникальный IP-адрес с использованием пространства сетевых IP-адресов LINKLOCAL. Сетевые адреса LINKLOCAL всегда начинаются с цифр 169.254 и имеют следующий формат:

169.254.x.x

Сетевые адреса LINKLOCAL применяются только для личной внутренней адресации и не являются действительными для узлов, видимых в Интернете. Их нельзя использовать для компьютеров, объединенных в сеть с общим доступом к подключению Интернета. После назначения сетевому адаптеру IP-адреса LINKLOCAL компьютер получает возможность связываться с помощью протокола TCP/IP с любым другим компьютером в сети, использующей ту же адресацию.

Компьютер с операционной системой Windows 98, настроенный на автоматическую личную IP-адресацию, может назначать себе личный IP-адрес, если выполняется любое из следующих условий.

- Компьютер не имеет конфигурации переносного, нет допустимой привязки в службе DHCP и в сети не найден сервер DHCP.
- Компьютер имеет конфигурацию переносного и в сети не найден сервер DHCP, вне зависимости от допустимой привязки в службе DHCP.

При автоматической IP-адресации становится возможной автоматическая настройка IP-адресов. Этот способ снижает временные затраты на администрирование и позволяет повторно применять IP-адреса. Рекомендуется использовать его в сетях любых размеров, не имеющих прямого подключения к Интернету или действующей службы DHCP. Статическая IP-адресация позволяет ввести постоянный IP-адрес вручную. Этот способ Microsoft рекомендует применять только в крайних случаях. Если в дальнейшем будет найдена служба DHCP, компьютер прекратит использование автоматически назначенных IP-адресов и будет применять IP-адреса, присвоенные службой DHCP. IP-адрес службы DHCP не заменяет статический IP-адрес. Последний должен быть изменен вручную. Если компьютер переводится из локальной сети со службой DHCP в локальную сеть без службы DHCP, то для освобождения адресов DHCP можно использовать служебную программу настройки IP WINIPCFG.

Для запуска программы выполните следующие шаги.

1. Нажмите кнопку **Пуск** и выберите команду **Выполнить**.
2. В поле **Открыть** введите: winipcfg.
3. Нажмите кнопку **Сведения**.
4. Для просмотра адресов серверов DNS, указанных в настройке компьютера, нажмите кнопку с многоточием (...) справа от поля **Серверы DNS**. Если эта кнопка отсутствует, то для данного компьютера поддержка DNS отключена.



5. Для просмотра сведений об адресах сетевых адаптеров выберите адаптер в поле со списком в группе **Ethernet: сведения**.

Служебная программа настройки IP позволяет пользователям и администраторам просматривать сведения о текущих IP-адресах и другие данные о сетевой конфигурации. Пользователь имеет возможность выполнить сброс одного или нескольких IP-адресов. Для одного IP-адреса следует использовать кнопки **Освободить** или **Обновить**. Если требуется обновить или освободить все IP-адреса, нажмите кнопку **Освободить все** или **Обновить все**. После нажатия одной из этих кнопок компьютер либо получает новый IP-адрес от службы DHCP, либо автоматически назначает себе личный IP-адрес.

В процессе работы Мастера общего доступа подключения к Интернету создается дискета, на которой содержится Мастер установки подключения обозревателя. Этот мастер позволяет быстро настроить подключение к Интернету для компьютеров сети.

Перед запуском Мастера установки подключения обозревателя убедитесь, что:

- компьютер настроен для работы в локальной сети, как это было описано ранее;
- в качестве обозревателя Интернета используется Microsoft(R) Internet Explorer версии 3.x или более новый либо Netscape Navigator версии 3.x или более новый;
- компьютер, обеспечивающий доступ, подключен и к Интернету, и к локальной сети.

Для запуска Мастера установки подключения обозревателя в первый раз выполните следующие действия:

1. Вставьте в дисковод компьютера, обеспечивающего подключение, дискету, созданную при установке общего доступа к подключению Интернета.
2. Нажмите кнопку **Пуск** и выберите команду **Выполнить**.
3. Введите команду: `a:\icsclset.exe`.
4. Нажмите кнопку **ОК**.

После этого компьютер может сразу соединиться с Интернетом, при условии, что компьютер, обеспечивающий общий доступ, уже подключен к глобальной сети.

Практически не отличается эта процедура и для компьютеров с Windows 2000/XP.

Достаточно, открыв окно свойств соединения на компьютере, через который осуществляется общий доступ, и выбрав вкладку **Дополнительно**, установить нужные флажки. При этом будет вызван Мастер настройки сети, который и поможет вам установить все необходимые параметры. В процессе работы мастера также будет предложено создать дискету, которая позволит настроить и остальные компьютеры для использования общего доступа к Интернету.

Очень подробно процедуры подключения рабочих станций к Интернету с использованием общего доступа описаны по ссылкам:

- <http://www.xnets.ru/plugins/content/content.php?content.118>;
- <http://www.diwaxx.ru/win/dual-internet-xp.php>.

## Настройка в Windows Vista и Linux

Работа на персональном компьютере редко проходит без взаимодействия с Интернетом. Школьники и студенты ищут материал для рефератов и курсовых, обычные пользователи используют Интернет как глобальную справочную систему и средство проведения досуга. Многие имеют электронную почту, доступ к которой невозможен без подключения к Интернету. Требуют подключения к Интернету и программы мгновенного обмена сообщениями и IP-телефонии. И это лишь небольшая часть задач, которые не могут быть решены без доступа к Интернету. Организовав домашнюю сеть, вы столкнетесь с проблемой подключения компьютеров, входящих в вашу маленькую сеть, к глобальной сети. Согласитесь, неудобно при наличии нескольких домашних ПК занимать очередь к компьютеру, подключенному к Интернету. Подключить все машины по аналогии с уже существующим подключением проблематично. Если, например, вы подключены через обычный модем или ADSL-модем по мостовому методу, как того требуют часто провайдеры, то для такого же подключения второго компьютера потребуется вторая телефонная линия, а для подключения третьего компьютера третья телефонная линия... Кабельный Интернет тоже приходит к одному компьютеру. Но сеть для того и существует, чтобы решить вопросы коллективного использования общих ресурсов. Интернет тоже общий ресурс, значит, необходимо настроить коллективный доступ к нему. В большинстве случаев это возможно. Какие же существуют варианты осуществления этой идеи?

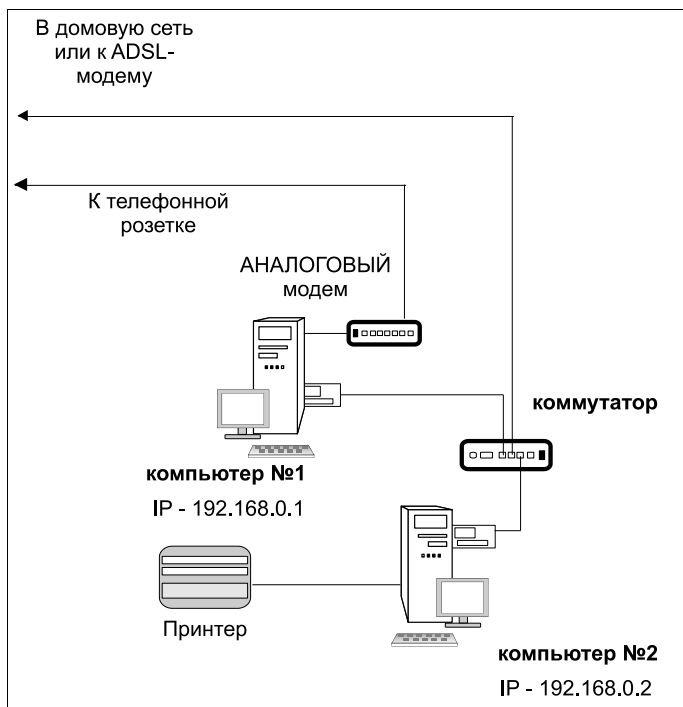
### Подключение через локальную сеть

Для начала посмотрим на настройки компьютеров, которые не имеют непосредственного выхода в Интернет, но используют существующее в сети подключение. Это подключение исполняет роль *шлюза* в Интернет, через который все компьютеры сети могут получить к нему доступ. Варианты создания самого шлюза мы рассмотрим позднее. Описывая настройки компьютеров для работы в сети, мы уже рассматривали параметры, которые необходимо настроить для доступа в Интернет, но не делали на них акцент. Теперь подробнее остановимся на особенностях этих настроек. Для наглядности приведем схематический рисунок нашей сети, которая уже подключена к Интернету одним из доступных способов (рис. 2.19). На рисунке изображены сразу два варианта выхода в Интернет, которые можно использовать и в совокупности. Сейчас нас будут интересовать настройки компьютера № 2, который не имеет собственного подключения. Для компьютера № 1 эти настройки будут похожими, если он подключается к Интернету через ADSL-модем.

Шлюзом в Интернет для компьютера № 2 может быть как ADSL-модем, так и компьютер № 1, если он подключен к Интернету через обычный модем.

IP-адреса, присвоенные компьютерам на рисунке, приведены условно, но при модемном подключении могут быть именно такими.

Мы уже рассмотрели настройки рабочих станций для работы в сети в *главе 1*. Здесь обратим внимание на те моменты, которые важны для работы с сетью Интернет.



**Рис. 2.19.** Вариант простой домашней сети с общим принтером и общим доступом в Интернет

В Интернете, как и в любой другой сети, компьютеры должны иметь свои IP-адреса. Но до тех пор, пока применяется четвертая версия протокола TCP/IP, адресов на всех пользователей Интернета хватать не будет. Поэтому компьютер в локальной сети должен использовать "чужой" внешний IP-адрес. Этот адрес может иметь компьютер или маршрутизатор, которые имеют непосредственный выход в Интернет и выполняют функцию шлюза. При этом и компьютер и маршрутизатор должны иметь не менее двух интерфейсов для подключения к сети. Через один интерфейс будет осуществляться подключение к Интернету, а через другой — к локальной сети. При подключении к Интернету любого компьютера локальной сети будет осуществляться трансляция сетевых адресов. Независимо от того, какой адрес компьютер будет иметь в локальной сети, в Интернете он будет "виден" с внешним IP-адресом шлюза. Это не всегда удобно. Например, некоторые бесплатные сервисы в Интернете ограничивают число обращений к ним с одного IP-адреса в сутки. Так, отправка SMS-сообщений с сайта MTS ограничена десятью сообщениями с одного адреса. Но для домашней сети такое ограничение может быть и не существенным. Некоторые другие проблемы могут быть решены с помощью различных сетевых инструментов. Во всяком случае множество не только домашних, но и серьезных сетей различных организаций подключаются к Интернету подобным образом и их пользователи не испытывают серьезных проблем при работе в Интернете, если сеть управляет грамотный администратор. В своей домашней сети таким администратором являетесь вы сами. Пока мы рассматриваем только настройки компьютера, находящегося внутри сети.

## В Windows

Откройте уже известное вам окно свойств сетевого подключения. Должно быть выбрано подключение, используемое в локальной сети. Мы рассматриваем здесь сеть, основанную на витой паре, но возможно, что вы используете беспроводное подключение (часто адаптер встроен в ноутбук). В этом случае настраивать следует его. Добраться до свойств сетевого подключения можно по следующему пути:

**Панель управления | Центр управления сетями и общим доступом | Управление сетевыми подключениями | Подключение по локальной сети (может иметь другое название) | Свойства.**

### ПРИМЕЧАНИЕ

Далее мы не будем указывать весь путь, просто предлагая открыть окно свойств сетевого подключения.

Само сетевое подключение имеет имя, которое вы можете изменить самостоятельно, как имя файла. В данном примере используется имя LocalNet. Подобные короткие имена удобнее, когда приходится управлять подключениями из командной строки, да и запоминать их легче. Если вам понадобится использовать несколько сетевых интерфейсов, каждому можно дать имя в соответствии с его назначением.

Откроем окно свойств подключения LocalNet (рис. 2.20).

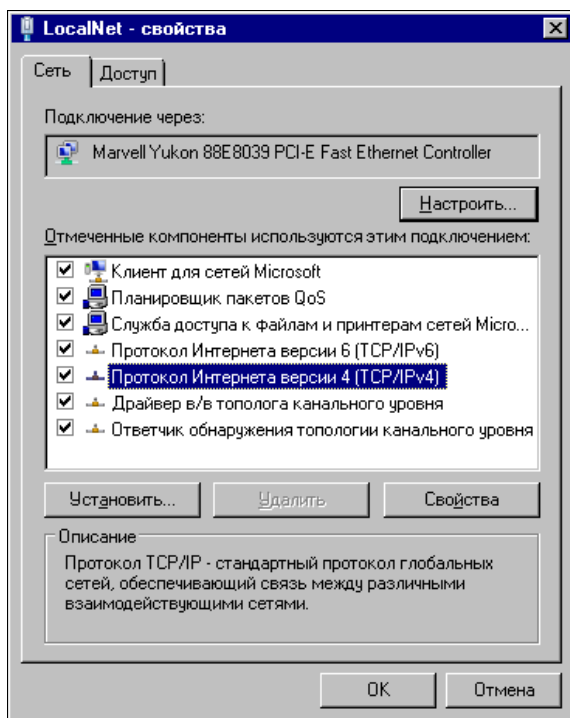


Рис. 2.20. Окно LocalNet — свойства

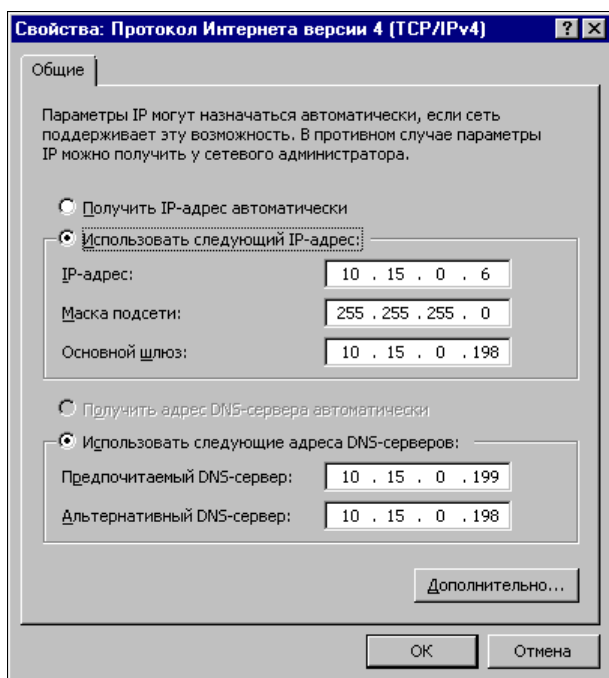
В этом окне нас интересуют свойства Протокола Интернета версии 4 (TCP/IPv4). Выделите строку, соответствующую этому протоколу, и нажмите кнопку **Свойства**.

**ПРИМЕЧАНИЕ**

В дальнейшем, при необходимости обратиться к окну свойств этого протокола, мы тоже просто будем говорить — "Откройте окно свойств TCP/IP".

Во многих случаях можно использовать автоматические настройки этого протокола. Позднее мы встретимся с такими ситуациями, но сейчас нам важно понять назначение и варианты каждой настройки. Рассмотрим назначение полей в окне **Свойства: Протокол Интернета версии 4 (TCP/IPv4)** (рис. 2.21).

- ❑ Поле **IP-адрес** содержит локальный адрес нашего компьютера. В целом ряде случаев он может присваиваться автоматически, но очень часто бывает удобнее назначить его вручную. Вы всегда будете знать IP-адрес каждого компьютера и при невозможности обратиться к нему по имени сможете использовать его адрес.
- ❑ Поле **Маска подсети** содержит значение маски локальной сети. Как IP-адрес, маска важна для работы внутри локальной сети и, соответственно, для связи со шлюзом в Интернет.



**Рис. 2.21.** Окно **Свойства: Протокол Интернета версии 4 (TCP/IPv4)**

Эти параметры не влияют на возможность работы в Интернете, тем не менее они должны быть настроены правильно, в соответствии с параметрами вашей сети.

Для обеспечения возможности работы в Интернете важны все следующие параметры.

- ❑ **Основной шлюз.** При неправильной настройке или при отсутствии этого параметра выйти в Интернет из локальной сети будет невозможно. В самой локальной сети никаких проблем вы не обнаружите. Если компьютеры "видели" друг

друга до изменения этого параметра, то они будут продолжать "видеть" и после его изменения.

- **Использовать следующие адреса DNS-серверов.** Найти ресурс в Интернете по его символьному имени невозможно, если не использовать DNS-серверы. Их в Интернете очень много, но пользователям обычно известны адреса серверов провайдера. Тем не менее, если вы узнаете другие адреса DNS-серверов, вы можете их использовать. Редко, но бывает, что какой-либо DNS-сервер не может разрешить символьное имя определенного сайта в его IP-адрес. В этом случае используется другой сервер, адрес которого можно указать в поле **Альтернативный DNS-сервер**. Если и этот сервер не может найти реально существующий в Интернете сайт, то браузер сообщит о невозможности открыть страницу. Можно попробовать изменить один из адресов DNS-серверов на имеющийся у вас в запасе.

Обратите внимание, что DNS-серверы никогда не указываются по своим именам, а только по IP-адресам.

## В Linux

В Linux все настройки для работы в Интернете совершенно аналогичны настройкам Windows. Ведь Интернет не требует использования конкретной операционной системы. Разницу мы увидим только в путях доступа к этим настройкам.

В ASP Linux доступ к рассматриваемым настройкам можно получить в окне **Настройка сети**, на вкладке **Устройства** (рис. 2.22) выбрать сетевой адаптер, используемый для подключения к локальной сети, и нажать кнопку **Изменить**. При этом откроется окно **Устройство Ethernet** (рис. 2.23).

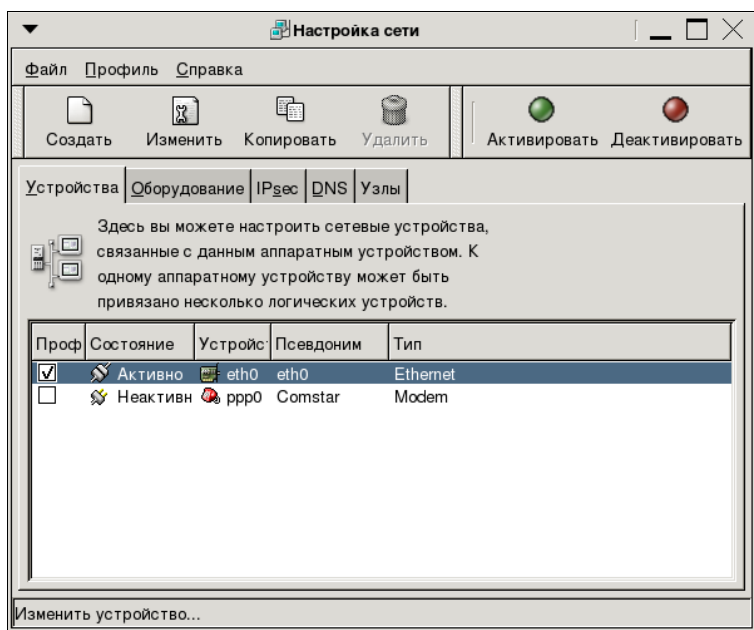


Рис. 2.22. Окно Настройка сети

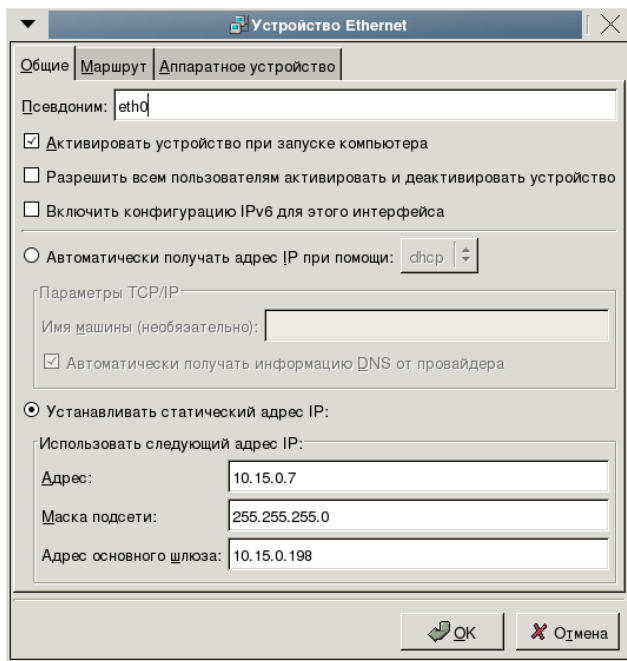


Рис. 2.23. Окно Устройство Ethernet

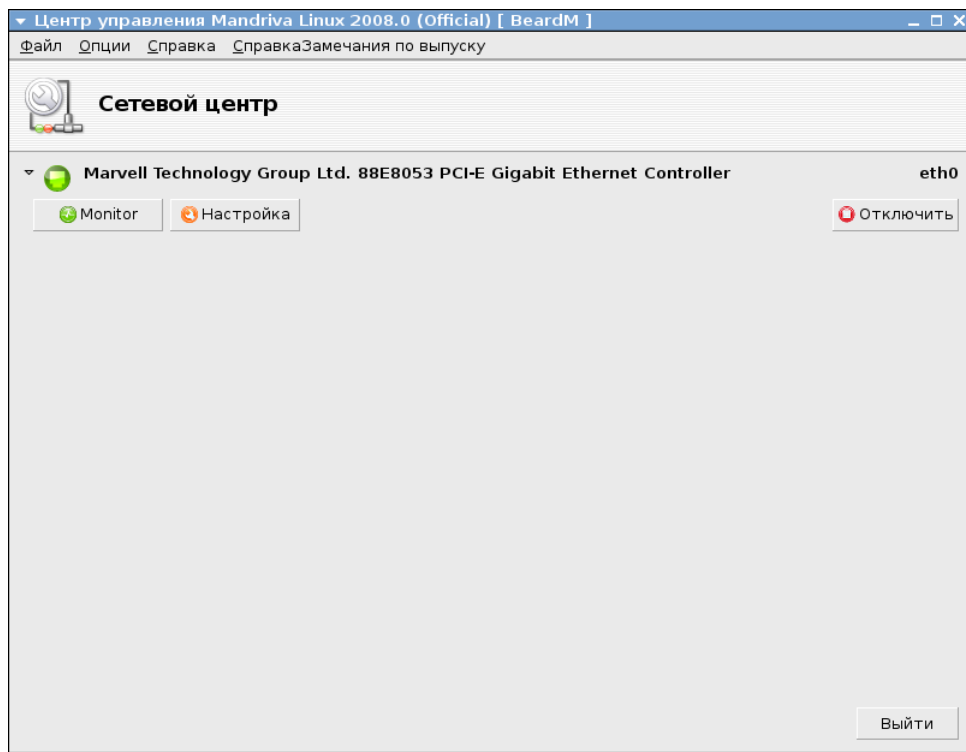


Рис. 2.24. Окно Центр управления Mandriva Linux — Сетевой центр

В этом окне вы увидите знакомые вам параметры, которые следует настроить в соответствии с имеющимися у вас данными сети.

В Mandriva Linux путь к настройкам несколько иной.

**Система | Администрирование | Настройка компьютера | Центр управления Mandriva Linux 2008.0 | Сеть и Интернет | Сетевой центр.**

В открывшемся окне (рис. 2.24) необходимо выбрать сетевой интерфейс и нажать кнопку **Настройка**. В открывшемся окне **Network settings** (рис. 2.25) появятся знакомые вам параметры.

Таким образом, настройка сетевых компьютеров для работы в Интернете существенных трудностей не вызовет. Возможно, что более сложной вам покажется настройка шлюзов. О них мы и поговорим далее.

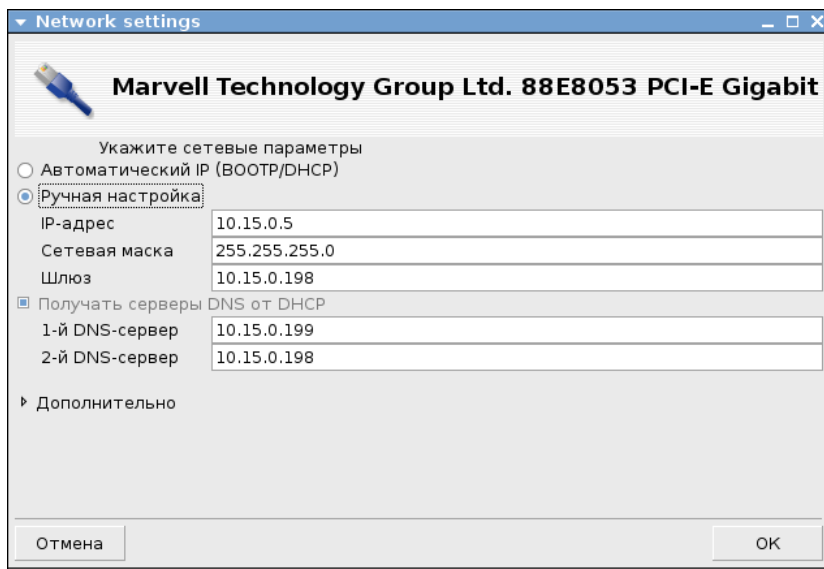


Рис. 2.25. Окно **Network settings**

## Подключение через ADSL-модем

ADSL-модемы могут содержать в себе маршрутизатор и коммутатор. Именно такой модем и желательно применить в вашей сети, чтобы не пришлось приобретать дополнительные устройства. Один из распространенных ADSL-модемов D-Link 500T, настройки которого для подключения к сайту провайдера Stream (<http://stream.ru>) мы и рассмотрим. Для подключения к другим провайдерам придется сделать корректировки настроек, но общий их ход останется таким же.

Модем имеет Web-интерфейс, что позволяет, подключив его в качестве сетевого устройства, получить доступ к настройкам через Web-браузер с компьютера под управлением любой операционной системы. Обычно устройства, обладающие Web-интерфейсом для настроек, имеют заранее заданный производителем IP-адрес, имя пользователя (login) и пароль (password). Эти данные указаны в документации на



устройство. Для данного модема по умолчанию заданы следующие параметры: IP-адрес — 192.168.1.1, login — admin, password — admin.

Введя login и password, когда они будут затребованы, вы увидите окно с несколькими вкладками и кнопочной панелью слева. Нас интересуют две вкладки — **Setup** и **Advanced**.

Рассматривая настройки модема, попутно глубже узнаем возможности нашей сети.

Начнем.

На вкладке **Setup** нажмите кнопку **DHCP Configuration** (рис. 2.26).

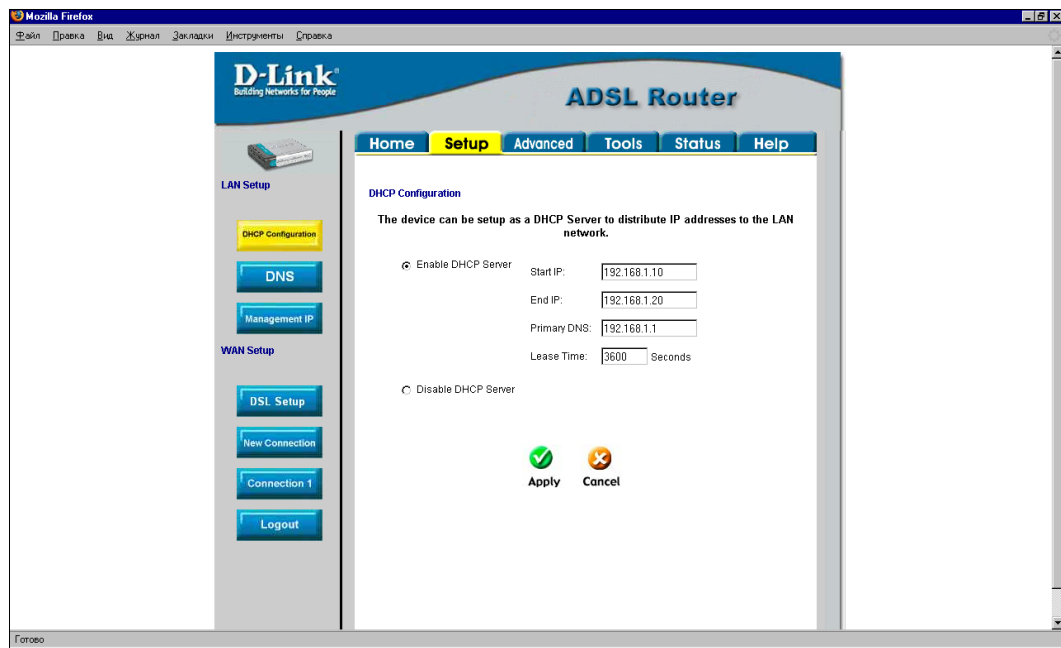


Рис. 2.26. Окно ADSL Router, вкладка Setup — DHCP Configuration

На открывшейся странице отметьте переключатель **Enable DHCP Server** (Включить DHCP-сервер). Мы упоминали о таком сервере в *главе 1*. В настраиваемое устройство он встроен. Включив DHCP-сервер, можно настроить его. Доступны следующие параметры DHCP-сервера:

- **Start IP** — начальный IP-адрес для присвоения компьютерам сети. Можно установить любой адрес из диапазона принятого для вашей сети, за которым есть еще один или более адресов.
- **End IP** — конечный IP-адрес для присвоения компьютерам сети. Можно установить любое значение, большее начального IP-адреса. На рисунке выбран диапазон из одиннадцати адресов. Это значит, что одиннадцать компьютеров сети могут получить автоматически IP-адрес и адрес DNS-сервера. Если компьютеру назначить вручную адрес не из этого диапазона, то вручную нужно будет указывать и адрес DNS-сервера.

- **Primary DNS** — IP-адрес первичного DNS-сервера, значение которого передается компьютерам сети. В данном примере указан адрес самого маршрутизатора. Дело в том, что это устройство может автоматически получать адреса DNS-серверов и транслировать запросы компьютеров на разрешение имен. Это очень удобно, если вам приходится давать доступ в Интернет гостям с ноутбуками. Достаточно указать адрес шлюза в Интернет, а все остальные параметры доступа гостевой ноутбук получит самостоятельно.
- **Lease Time** — время аренды IP-адреса. Выданный DHCP-сервером адрес может быть выдан повторно другому или тому же компьютеру при следующем подключении к сети. Если к вашей сети часто подключаются гостевые компьютеры, то полученные ими IP-адреса будут освобождаться после выхода из сети через 3600 секунд (один час). В больших сетях предприятий это время составляет обычно несколько дней.

Нажав кнопку **DNS**, переходим к указанию DNS-серверов или способу получения их адресов модемом (рис. 2.27). В данном случае модем автоматически получает их адреса от провайдера, а клиенты сети могут использовать адрес модема вместо DNS-сервера.

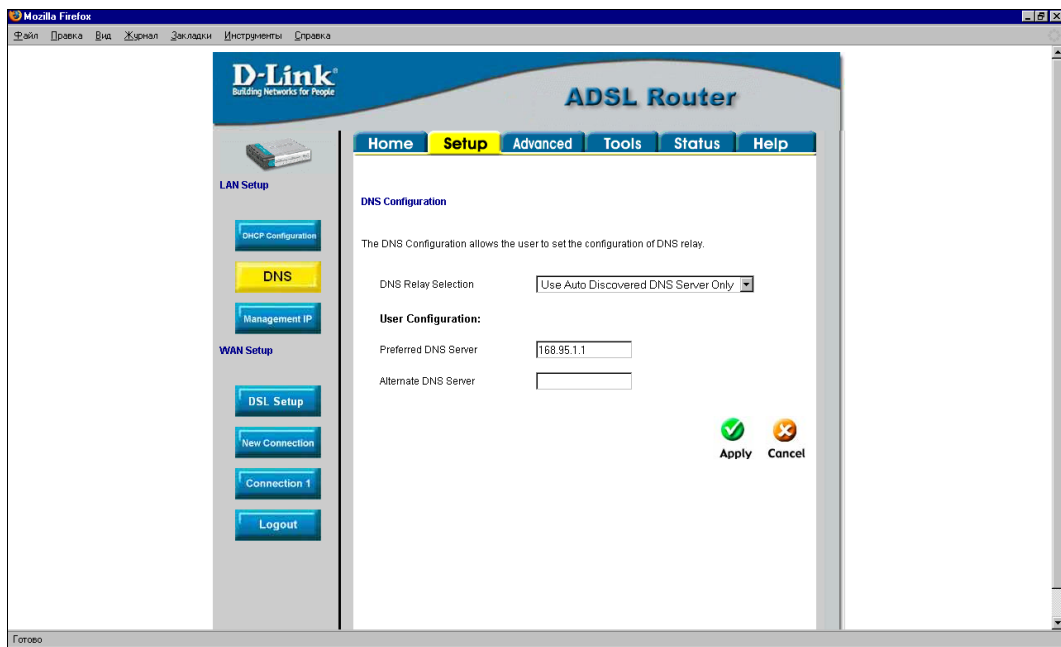


Рис. 2.27. Окно ADSL Router, вкладка Setup — DNS Configuration

Кнопкой **Management IP** открывается страница настройки адресов шлюзов (рис. 2.28). Маршрутизатор модема для внешней сети выглядит сетевым устройством, которое имеет свой IP-адрес и имя. Это устройство должно получить доступ в Интернет через шлюз провайдера. IP-адрес шлюза провайдера указан в поле **Default Gateway**. Значение этого адреса необходимо получить у провайдера. Сим-

вольные имена самого маршрутизатора и домена в данном случае могут быть любыми. **IP Address** (IP-адрес) и **NetMask** (маска подсети) соответствуют вашей сети. Внутренний (со стороны вашей сети) IP-адрес маршрутизатора это адрес шлюза для всех компьютеров вашей сети. Вы можете изменить его относительно заданного по умолчанию, если в своей сети вы приняли другой диапазон адресов.

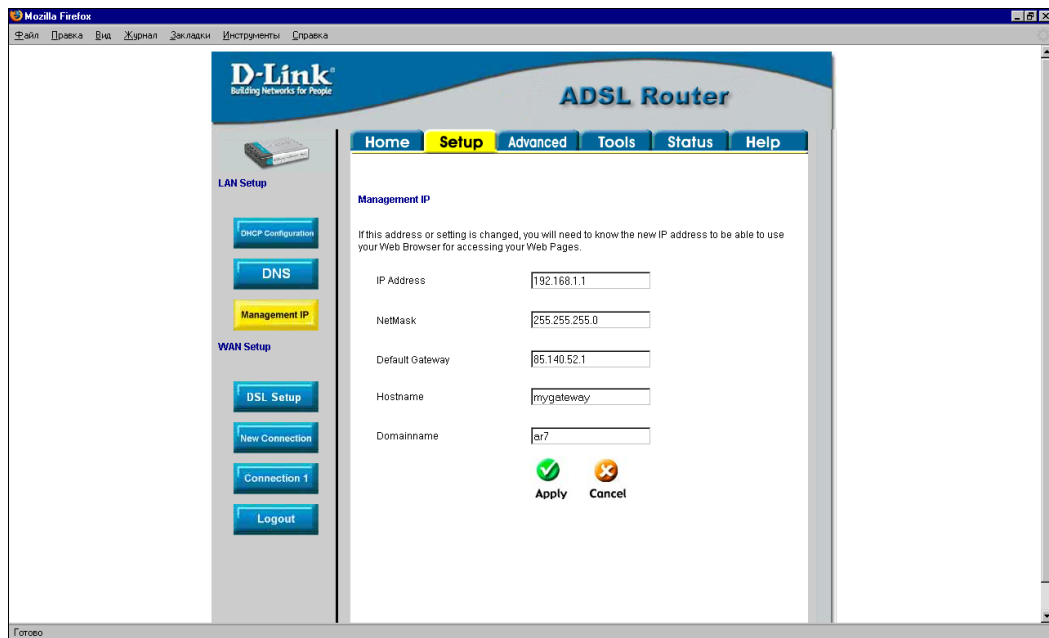


Рис. 2.28. Окно ADSL Router, вкладка Setup — Management IP

Кнопка **DSL Setup** открывает окно выбора (рис. 2.29) используемого провайдером типа модуляции при передаче данных между модемами. Если провайдер не дает других рекомендаций, то обычно подходит режим **MMODEM**.

После создания нового подключения на странице, открываемой кнопкой **New Connection**, для него автоматически создается новая страница и кнопка для ее открытия **Connection 1** (рис. 2.30). Параметры подключения могут быть отредактированы после его создания. Имя подключения может быть любым, тип подключения — **PPPoE**, имя пользователя и пароль предоставляются провайдером, как и параметры **VPI** и **VCI**.

Необходимо установить флажки **NAT** и **Firewall**. Это позволит повысить защищенность вашей сети от атак из Интернета и настроить преобразование сетевых адресов для доступа к некоторым службам в вашей сети из Интернета.

Сейчас только покажем страницу, открываемую кнопкой **Port Forwarding** на вкладке **Advanced**, где выполняются настройки для доступа к вашим компьютерам из Интернета (рис. 2.31).

На вкладке **Advanced** кнопкой **Advanced Security Settings** (рис. 2.32) включается доступ к Web-серверу и Telnet-серверу, которые могут находиться в вашей сети, и может быть определен компьютер, к которому определен доступ из Интер-

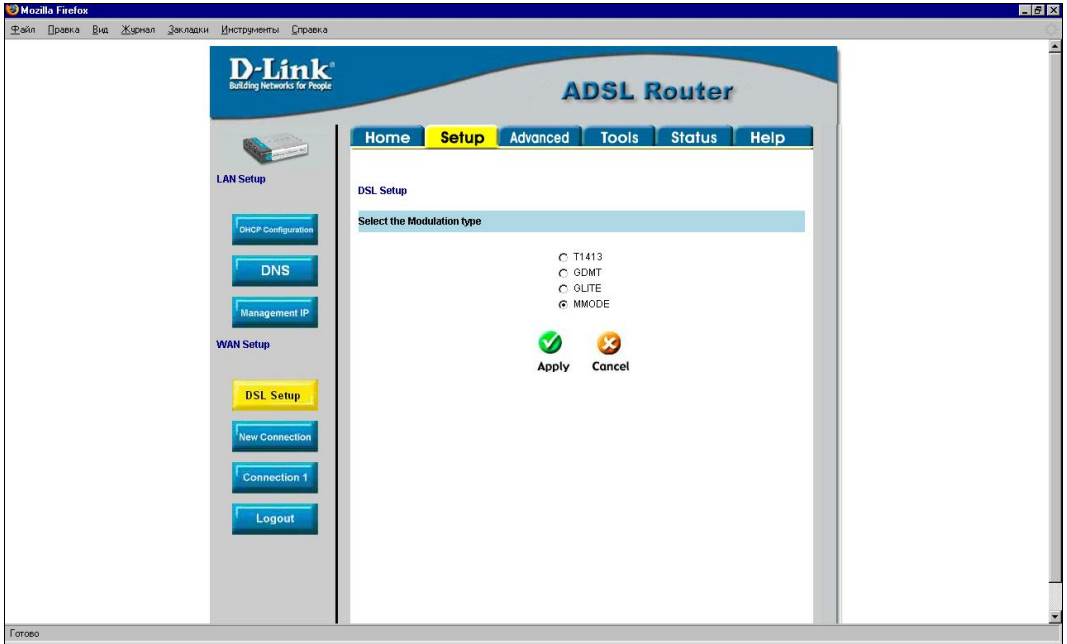


Рис. 2.29. Окно ADSL Router, вкладка Setup — DSL Setup

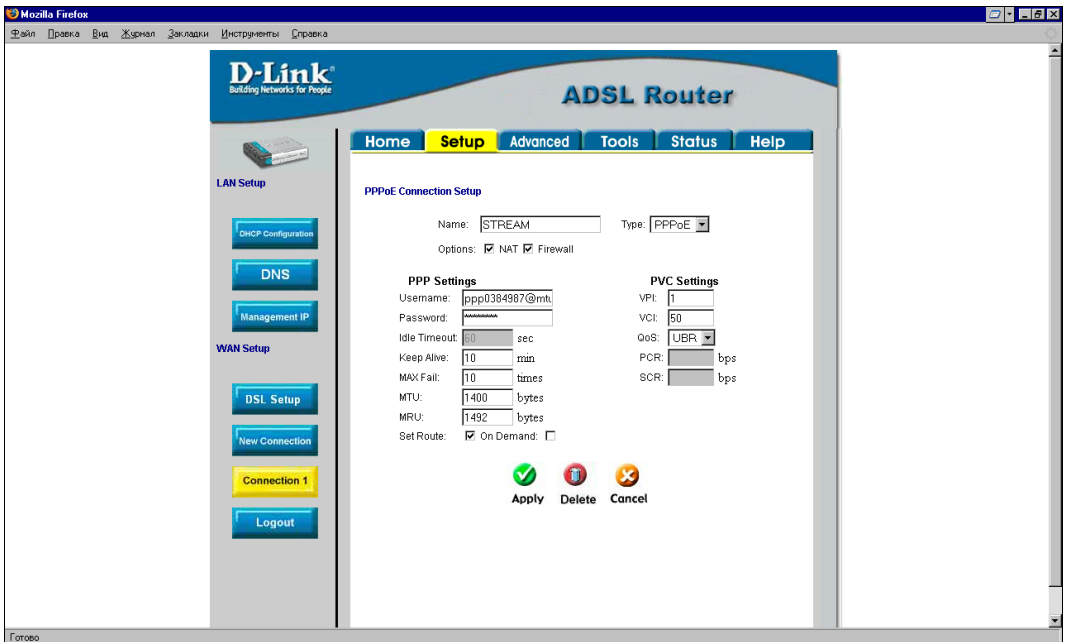


Рис. 2.30. Окно ADSL Router, вкладка Setup — PPPoE Connection Setup



Рис. 2.31. Окно ADSL Router, вкладка Advanced — Port Forwarding

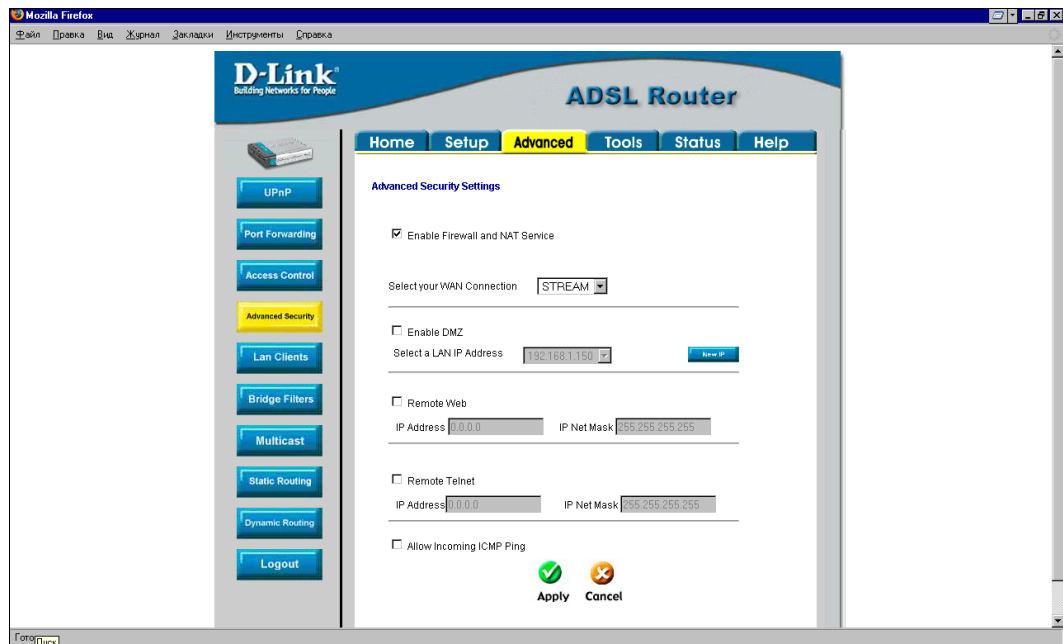


Рис. 2.32. Окно ADSL Router, вкладка Advanced — Advanced Security Settings

нета, но сам этот компьютер не имеет связи с вашей сетью (флажок **Enable DMZ**). Для этого компьютера маршрутизатором может быть создана *демилитаризованная зона (DMZ — demilitarized zone)*, откуда невозможны внешние атаки на вашу сеть.

И наконец, на вкладке **Advanced** кнопкой **LAN Clients** открывается одноименная страница, где можно указать IP-адреса компьютеров, к которым будет определен доступ из вне (рис. 2.33).

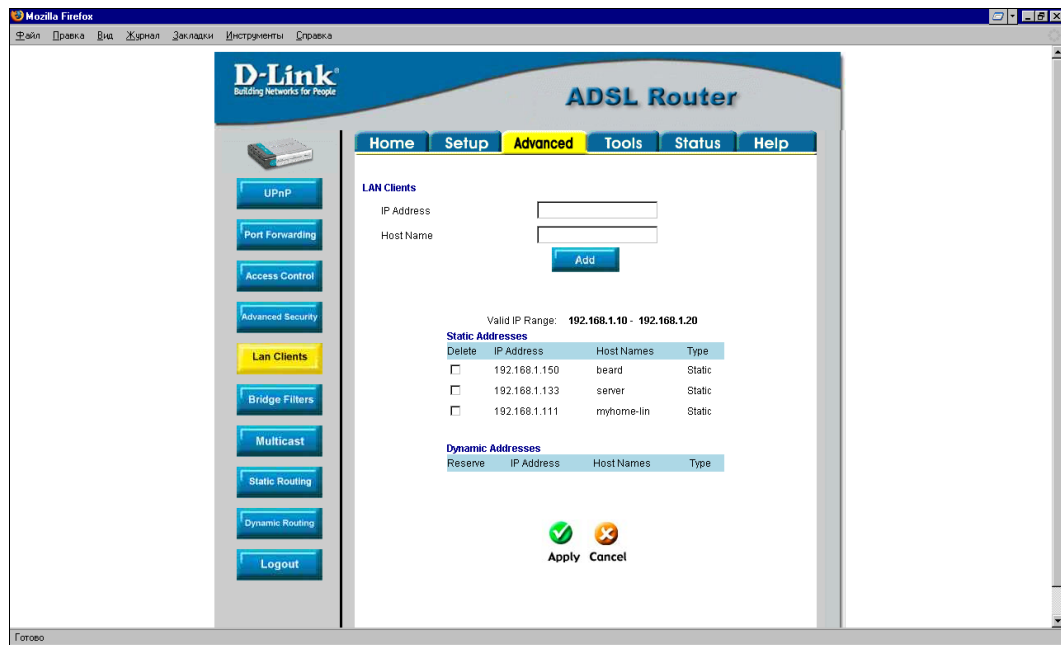


Рис. 2.33. Окно ADSL Router, вкладка **Advanced** — LAN Clients

Модем-маршрутизатор имеет еще множество настроек, которые возможно понадобятся вам, когда вы освоите работу в вашей сети в такой степени, что описанных в этой книге возможностей будет недостаточно. Тогда вы сможете эти настройки указать самостоятельно.

## Подключение через обычный модем

Вполне вероятно, что у вас нет возможности получить доступ в Интернет по технологии ADSL. До сих пор многие пользователи удаленных от центра регионов могут использовать только коммутируемый доступ в Интернет через обычный модем. В этом случае придется выделять один компьютер, через который доступ в Интернет будут получать остальные клиенты вашей сети.

Может быть, в случае доступности, использование сотового телефона в качестве модема, разумеется, если оператор сотовой связи предоставляет эту возможность. Рассмотрим настройку доступа в Интернет через коммутируемое соединение в Windows и в Linux.

## В Windows

Прежде всего необходимо подключить к компьютеру модем. Как и другие устройства, модем требует установки драйверов для обеспечения корректной работы, но часто достаточно драйверов, имеющихся в системе. Большинство модемов в ОС Windows могут работать как Стандартный модем.

В левой части окна **Центр управления сетями и общим доступом** (рис. 2.34) найдите задачу **Установка подключения или сети**. Щелкнув на этом пункте меню, откройте одноименное окно (рис. 2.35).

В этом окне выбираем вариант подключения **Настройка телефонного подключения** и нажимаем кнопку **Далее**.

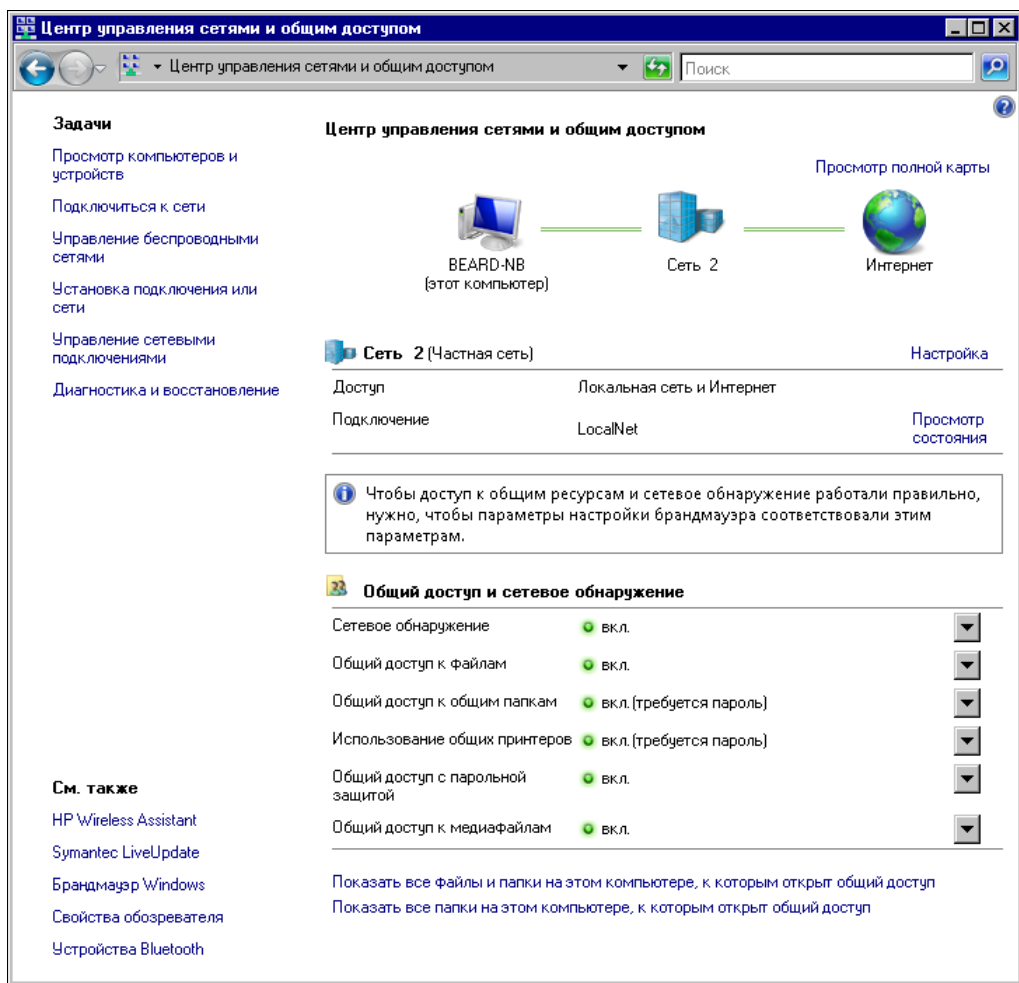


Рис. 2.34. Окно **Центр управления сетями и общим доступом**

В открывшемся окне **Настройка телефонного подключения** выбираем установленный модем (рис. 2.36). В следующем окне (рис. 2.37) вводим информацию

о телефонном подключении, полученную от провайдера. Пароль и логин, необходимые для подключения, можно ввести через Internet Explorer, открыв **Сервис | Свойства обозревателя | Подключения | Настройка**.

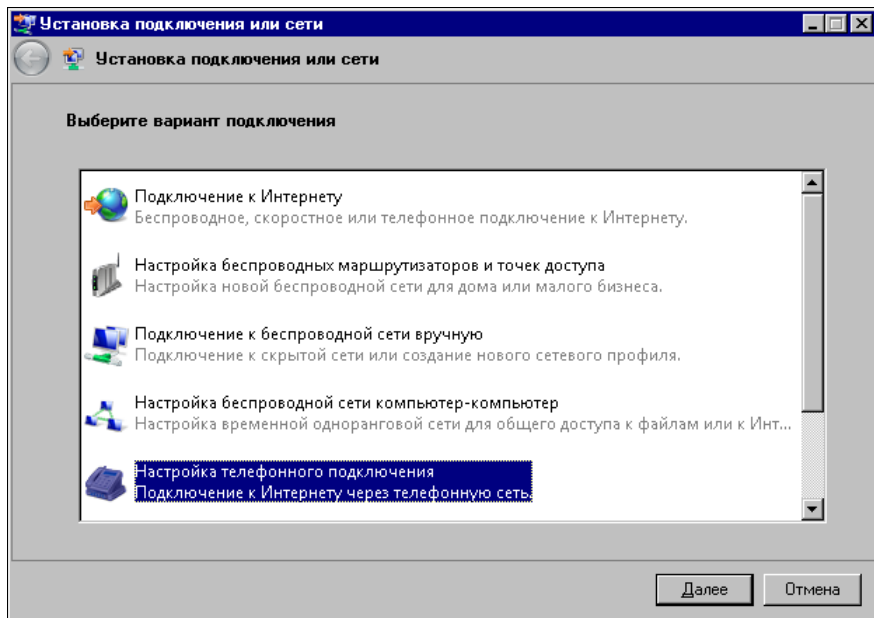


Рис. 2.35. Окно Установка подключения или сети

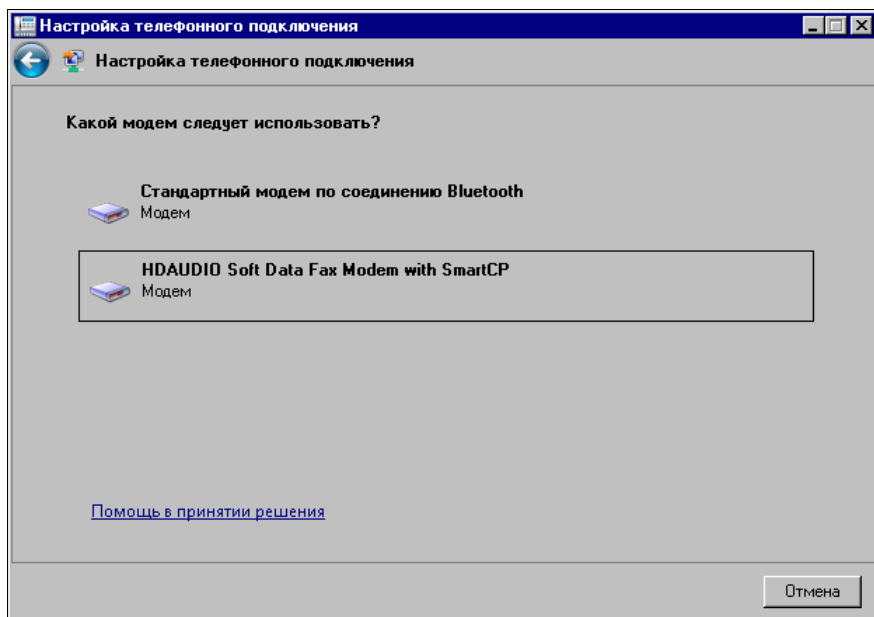


Рис. 2.36. Окно Настройка телефонного подключения (выбор модема)



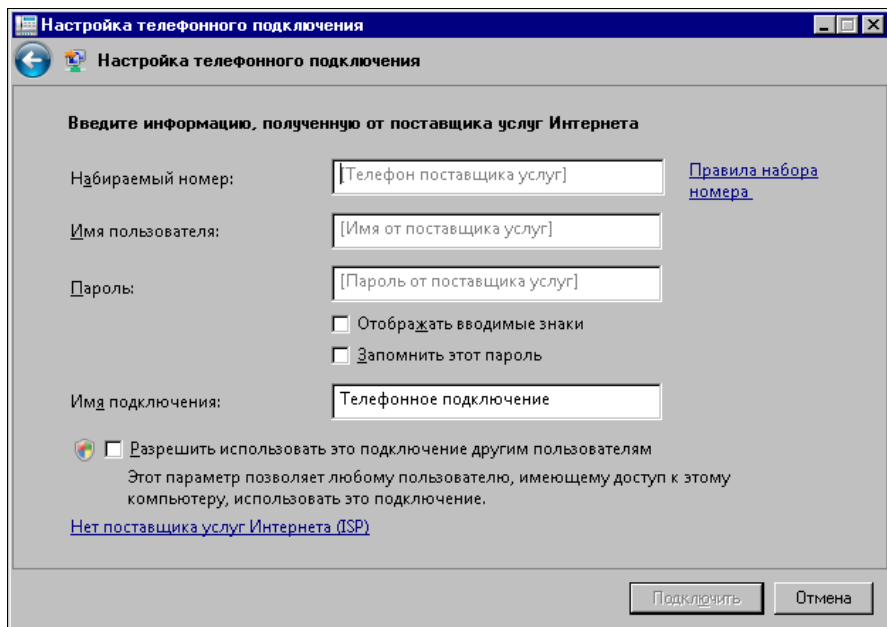


Рис. 2.37. Окно **Настройка телефонного подключения** (ввод информации)

Если вы хотите использовать настраиваемое соединение для общего доступа в Интернет, установите флажок **Разрешить использовать это подключение другим пользователям**. Это позволит подключаться к Интернету сетевым компьютерам независимо от того, сеанс какой учетной записи открыт на этой машине.

Созданное подключение появится в окне **Сетевые подключения** (рис. 2.38), которое можно открыть, выполнив **Центр управления сетями и общим доступом | Управление сетевыми подключениями**.

Создавая подключение, убедитесь, что установленный в системе модем действительно работает. Автору встретился экземпляр модема, ранее работавшего с другими компьютерами, который после установки на компьютер с Windows Vista работать отказался. Проверить это совсем не сложно. Найдите в панели управления апплет (от англ. applet) **Телефон и модем** и откройте его.

Окно откроется на вкладке **Набор номера** (рис. 2.39). Название размещения, которое вы увидите в списке **Размещение**, вы всегда можете изменить на желаемое. Но важно, чтобы это размещение было настроено в соответствии с вашими местными условиями. Нажмите кнопку **Изменить** и установите параметры размещения в открывшемся окне **Изменение местонахождения** (рис. 2.40).

Введите необходимые значения кодов набора, включая и код своего города. Установите тип набора номера, который допустим на ваших телефонных линиях.

Убедившись, что местонахождение настроено, нажмите кнопку **Применить**, а затем **ОК**.

Перейдите в окне **Телефон и модем** на вкладку **Модемы** (см. рис. 2.39) и откройте окно свойств установленного в вашей системе модема.

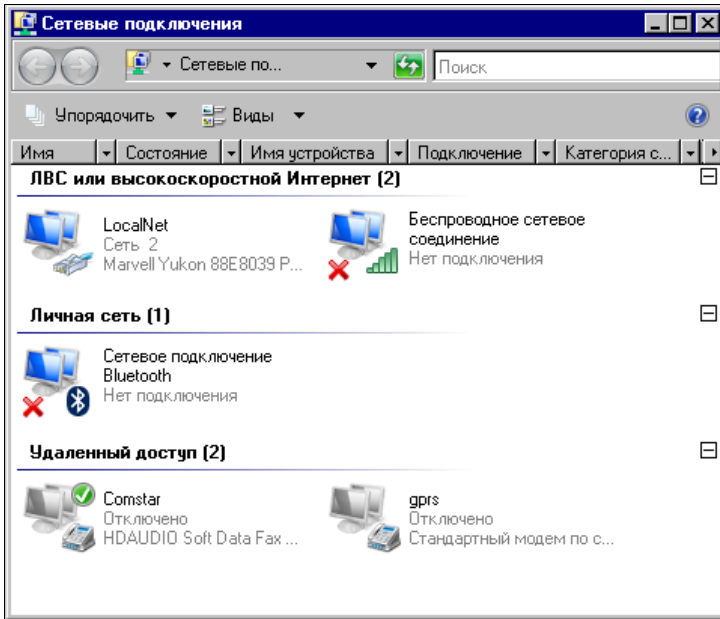


Рис. 2.38. Окно Сетевые подключения

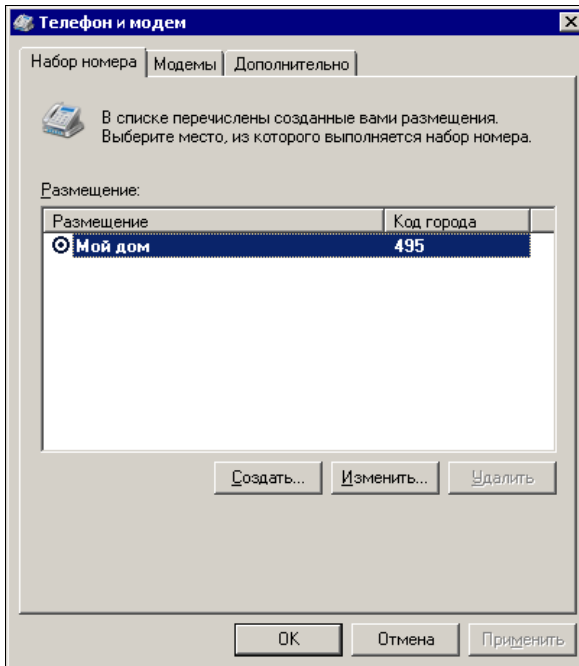


Рис. 2.39. Окно Телефон и модем, вкладка Набор номера

Нажмите кнопку **Опросить модем** и убедитесь, что модем отвечает на запросы системы.

Имя подключения можете изменить по вашему желанию. Ссылку на **Правила набора номера** можно проигнорировать, поскольку мы уже настроили эти правила,

задавая местонахождение. После ввода данных станет активной кнопка **Подключить**. Нажмите ее, но далее откажитесь от проверки подключения. Согласитесь с предложением системы создать подключение без проверки. Вернитесь к окну **Центр управления сетями и общим доступом**, найдите и запустите задачу **Управление сетевыми подключениями**. Откройте свойства созданного телефонного подключения (рис. 2.41).

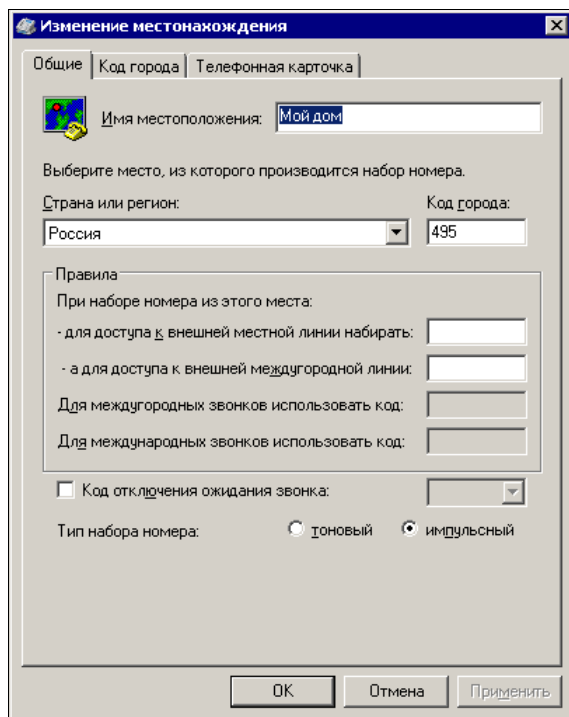


Рис. 2.40. Окно **Изменение местонахождения**

На вкладке **Общие** установите флажок **Использовать правила набора номера**. Перейдите на вкладку **Безопасность** (рис. 2.42) и установите флажок **Сценарий**. Сценарий потребуется потому, что при подключении к Интернету из сети неко- му будет вводить имя пользователя и пароль.

Создайте текстовый документ с содержанием, как в листинге 2.1.

#### Листинг 2.1. Сценарий подключения

```
proc main
  waitfor "login:"
  transmit "Имя_пользователя_интернета"
  transmit "^M"
  waitfor "password:"
  transmit "пароль_доступа_в_интернет"
  transmit "^M"
endproc
```

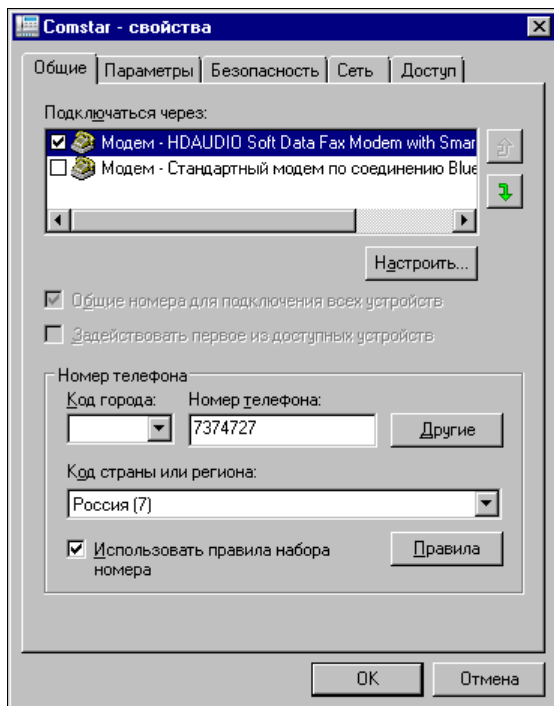


Рис. 2.41. Окно Comstar — свойства

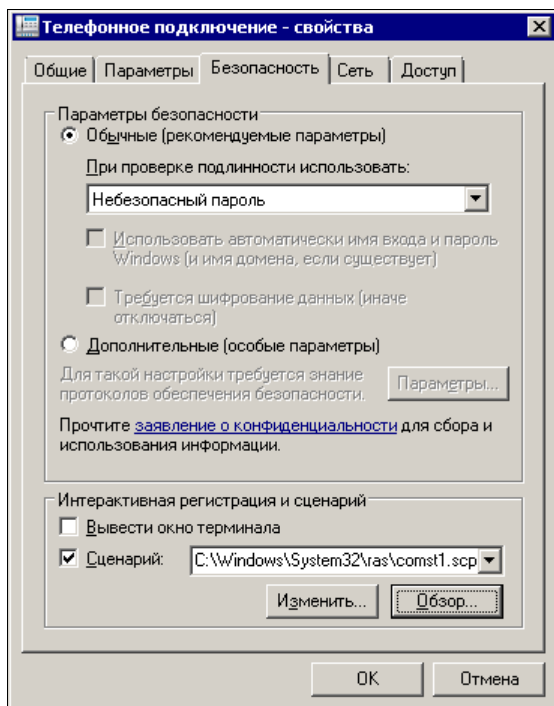


Рис. 2.42. Окно Телефонное подключение — свойства, вкладка Безопасность

Сохраните файл под любым именем, но с расширением scr.

В раскрывающемся списке **Сценарий** окна свойств телефонного подключения укажите путь к созданному файлу.

Закрыв окно свойств телефонного подключения, выберите **Подключить** в контекстном меню подключения. Если все параметры подключения заданы верно, то соединение должно установиться, но система предложит выбрать сетевое размещение (рис. 2.43).

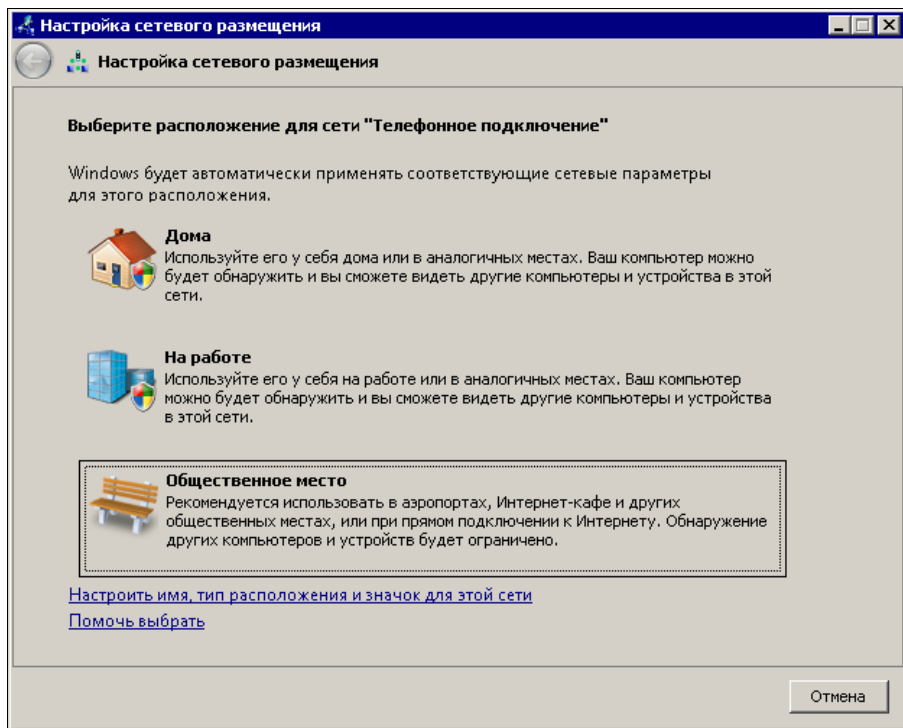


Рис. 2.43. Окно Настройка сетевого размещения

Лучше, если вы выберете **Общественное место**. Настройки вы делаете дома, но вход к вам из Интернета во время работы подключения лучше закрыть.

Когда соединение установится, проверьте его состояние.

В окне **Состояние — Телефонное подключение** (рис. 2.44) вы должны увидеть два IP-адреса — сервера и клиента. Снова откройте окно свойств телефонного подключения, но на вкладке **Доступ** (рис. 2.45).

Установите в этом окне все флажки. Вы увидите сообщение системы, показанное на рисунке (рис. 2.46).

В этом сообщении сказано, что сетевой плате вашего компьютера будет присвоен адрес 192.168.0.1... Если до настройки подключения к Интернету адрес уже был присвоен, вы можете его вернуть. Система меняет IP-адрес сетевой карты только после завершения настроек, а затем "согласится" использовать тот, что вы укажете сами. Например, в сети автора этих строк IP-адрес сетевой карты компьютера об-

щего доступа к Интернету равен 192.168.1.150. На других компьютерах сети следует этот адрес указать в качестве шлюза в свойствах сетевых подключений. При этом адрес DNS-сервера укажите тот, что выдан провайдером, а IP-адреса компьютеров сети должны находиться в одной подсети.

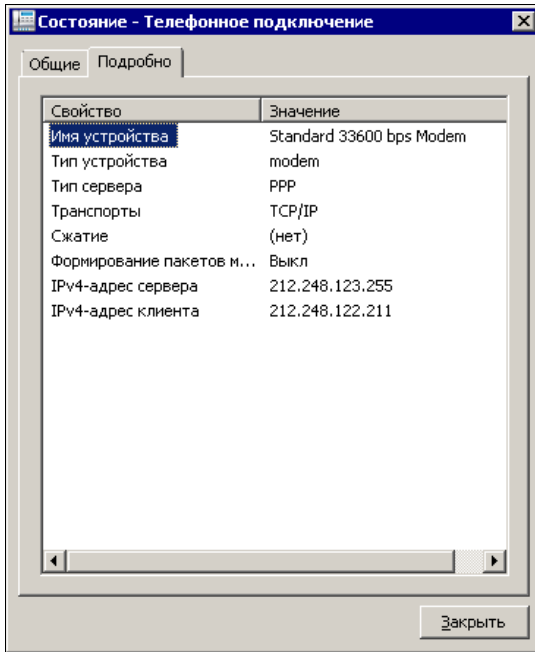


Рис. 2.44. Окно Состояние — Телефонное подключение

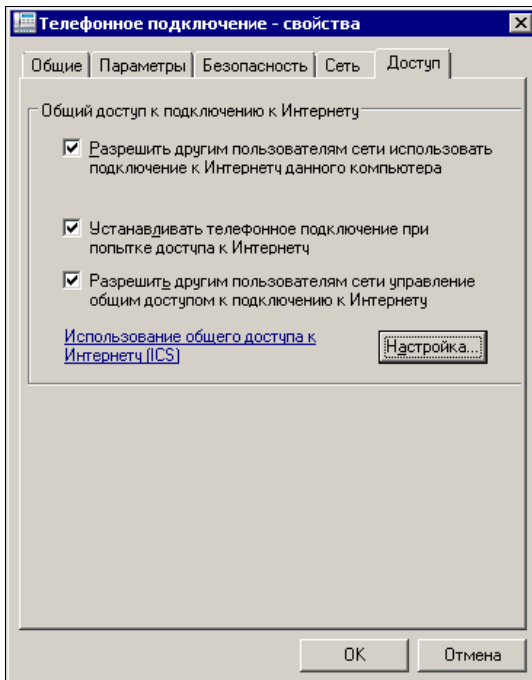


Рис. 2.45. Окно Телефонное подключение — свойства, вкладка Доступ

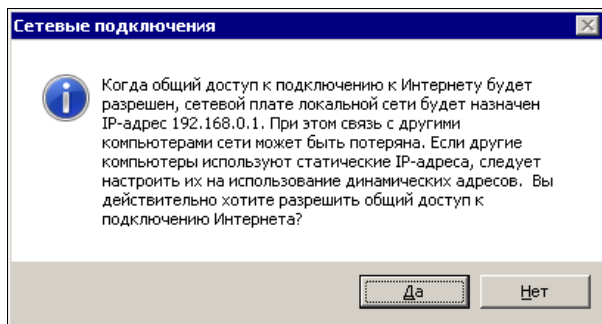


Рис. 2.46. Окно **Сетевые подключения** (сообщение)

В окне **Сетевые подключения** на других компьютерах сети (рис. 2.47) должно появиться еще одно подключение в разделе **Шлюз Интернета**. Теперь при попытке открыть адрес в Интернете будет устанавливаться подключение на компьютере общего доступа к Интернету, а компьютеры сети получают доступ во Всемирную сеть. Подключение для компьютеров сети устанавливается автоматически. Но иногда может потребоваться установка подключения по расписанию, например, для доступа к компьютеру из Интернета. Для этого можно создать пакетный файл с командой `Rasdial` и настроить его запуск с помощью планировщика задач Windows (**Панель управления | Администрирование | Планировщик задач | Создать задачу**).

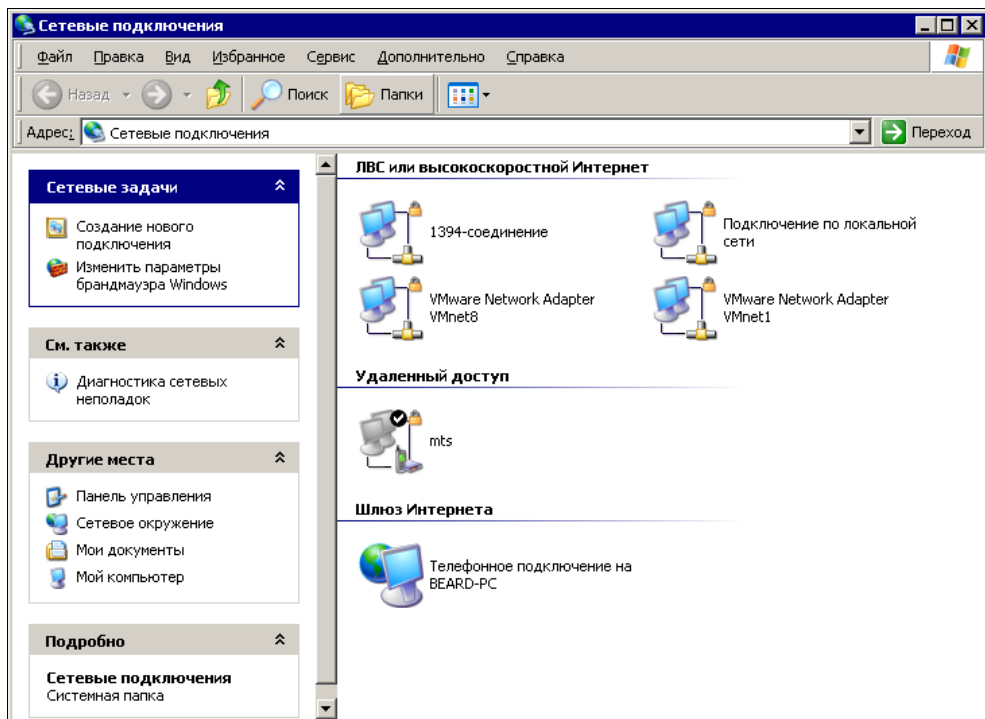


Рис. 2.47. Окно **Сетевые подключения** (на других компьютерах сети)

## Rasdial

Команда `Rasdial` выполняет автоматический набор номера для клиентов Microsoft.

В пакетном файле необходимо записать строку с командой и параметрами запуска. Все возможные параметры вы можете найти в справке по команде, но в нашем случае, когда все параметры подключения записаны в файле сценария и сохранены в самом подключении, достаточно написать лишь `rasdial comstar`, где `comstar` — это имя подключения (впишите свое).

Если запустить эту команду вручную из командной строки, вы увидите следующие строки, подтверждающие ее выполнение:

```
C:\Users\1>rasdial comstar
Установка связи с comstar...
Проверка имени и пароля пользователя...
Регистрация компьютера в сети...
Установлена связь с comstar.
Команда успешно завершена.
```

Для отключения от Интернета введите `rasdial /d`.

Соединение будет разорвано.

Если провайдер поддерживает обратный вызов, то в строке подключения потребуется добавить параметр `/callback:<ваш номер телефона>`.

## В Mandriva Linux

Настроим подключение к Интернету в Mandriva Linux. Подключите модем к компьютеру. Войдите в **Центр управления Mandriva Linux**. Выберите в левой части окна меню **Сеть и Интернет** (рис. 2.48), после чего в правой части окна найдите значок утилиты **Настройка нового сетевого интерфейса** и запустите ее.

В открывшемся окне **Настройка нового сетевого интерфейса** (рис. 2.49) выберите сетевой интерфейс, который необходимо настроить. В данном случае наш выбор — **Аналоговый телефонный модем (POTS)**. После этого нажмите кнопку **Далее**.

В следующем окне возможен выбор модели модема. Если вы подключили полноценный аппаратный модем, то система его не определит, и предложит самостоятельно выбрать модем для настройки (рис. 2.50).

Теперь необходимо указать порт, к которому подключен модем. В данном случае это порт COM1 (рис. 2.51). В Linux этому порту соответствует устройство `ttyS0`.

Может так случиться, что в системе не хватает какого-либо пакета, и поэтому система предложит установить его (рис. 2.52).

Далее появится окно (рис. 2.53) со списком возможных провайдеров. Российских провайдеров вы в нем не найдете, следовательно, будем редактировать вручную. В следующем окне (рис. 2.54) необходимо указать параметры учетной записи, которые вами получены у провайдера.

Далее необходимо указать IP-параметры подключения (рис. 2.55). Оставим для всех параметров автоматическое их получение.



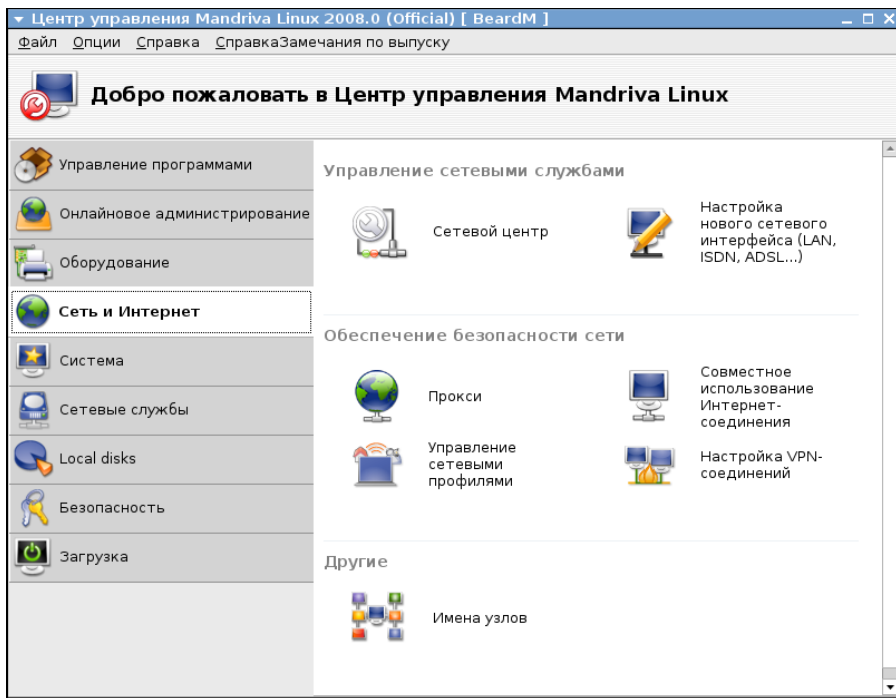


Рис. 2.48. Окно Центр управления Mandriva Linux меню Сеть и Интернет

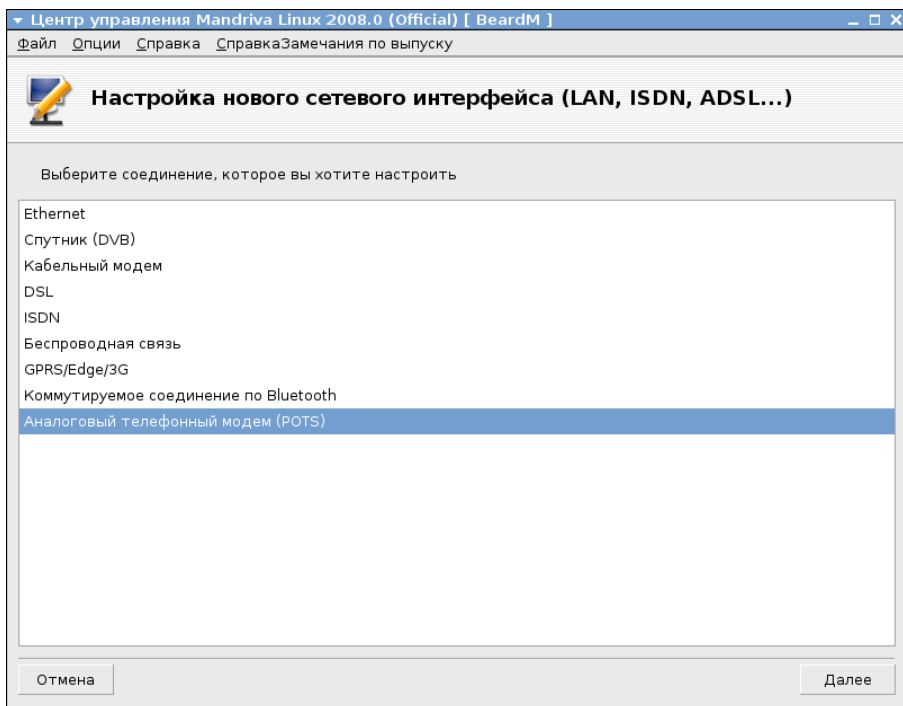


Рис. 2.49. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса

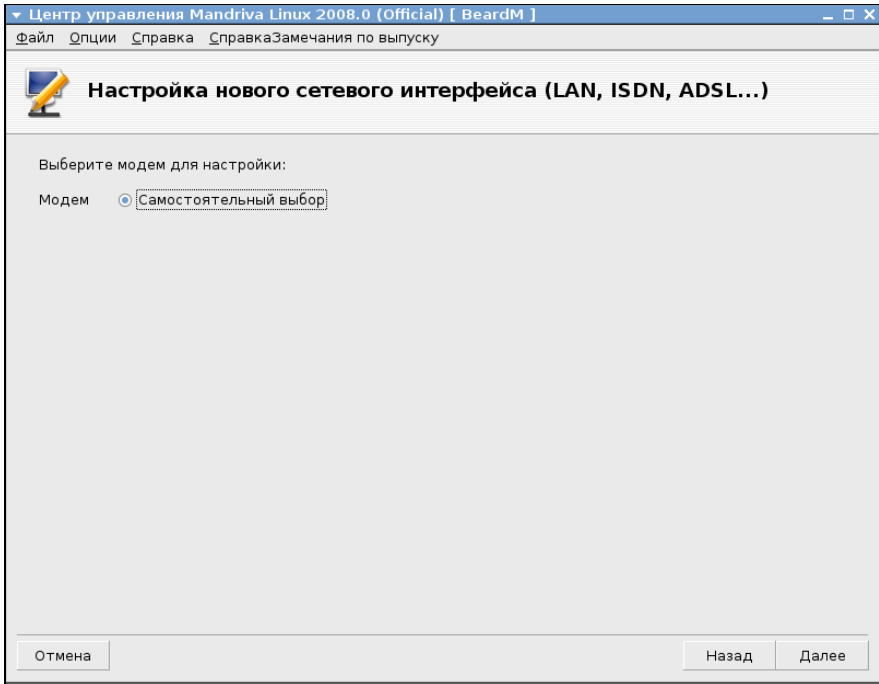


Рис. 2.50. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (выбор модема)

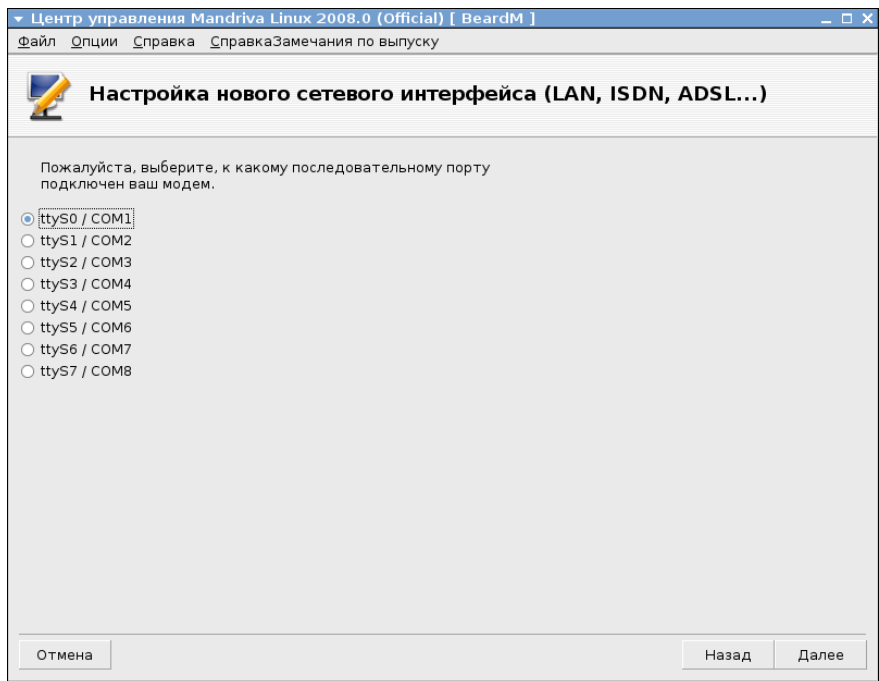


Рис. 2.51. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (выбор порта модема)

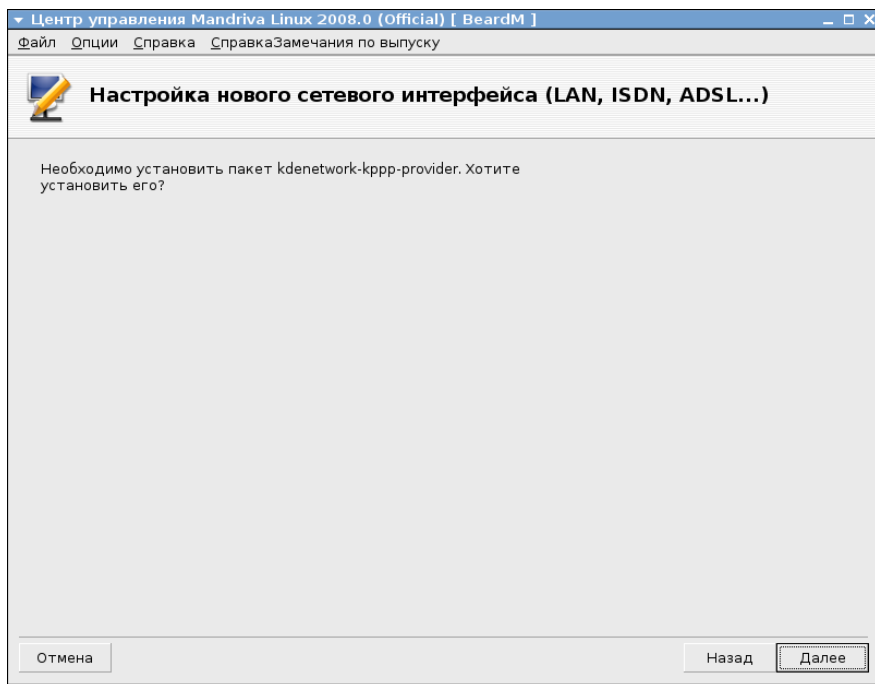


Рис. 2.52. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (запрос на установку дополнительных пакетов)

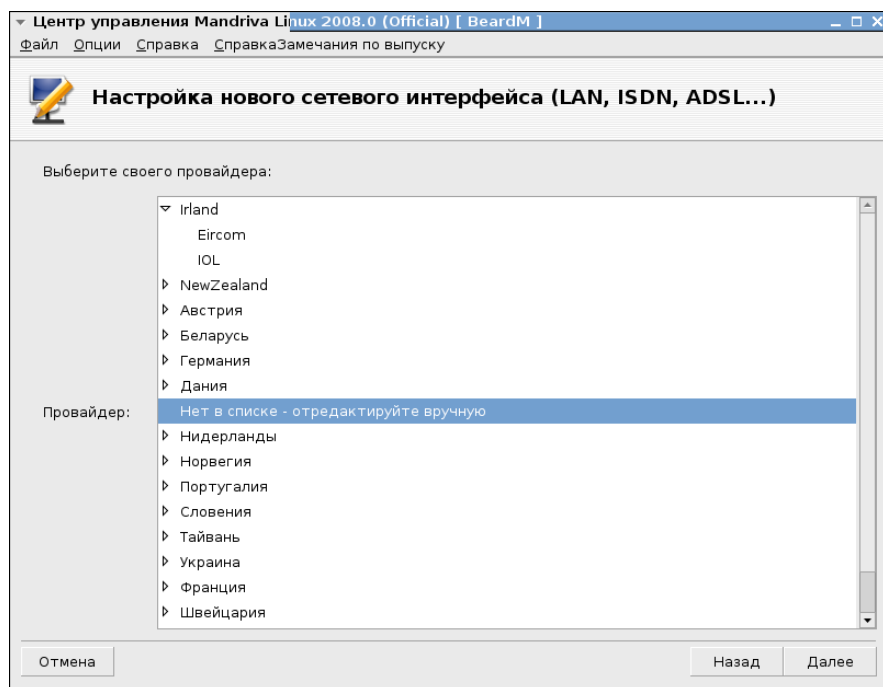


Рис. 2.53. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (выбор провайдера)

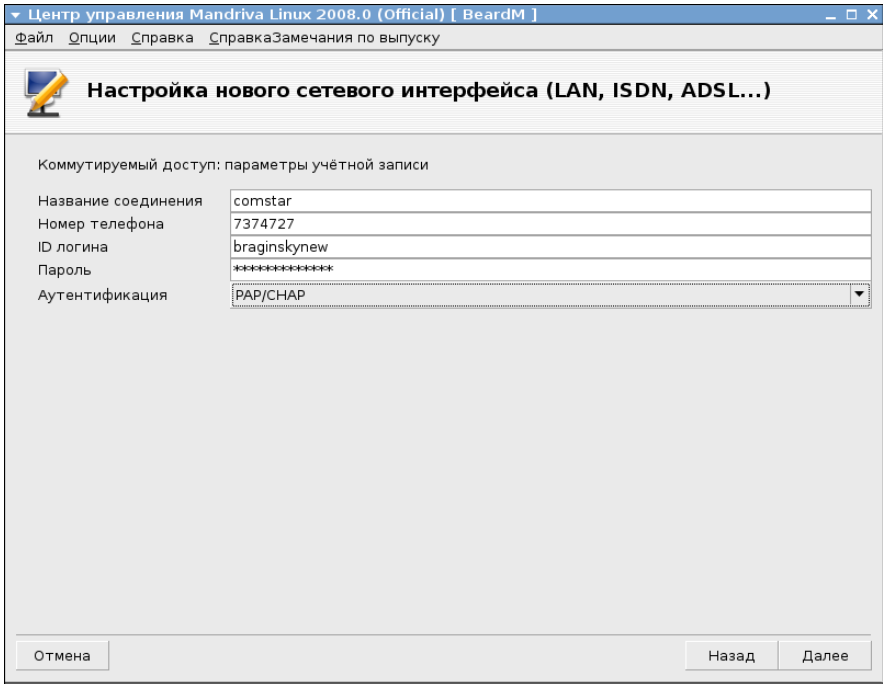


Рис. 2.54. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (параметры учетной записи)

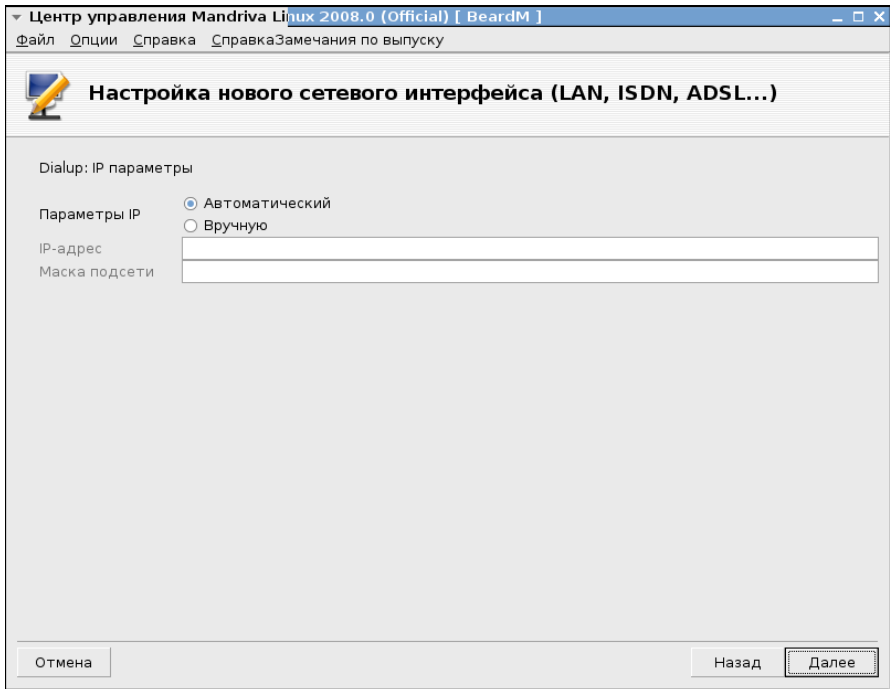


Рис. 2.55. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (задание IP-параметров)

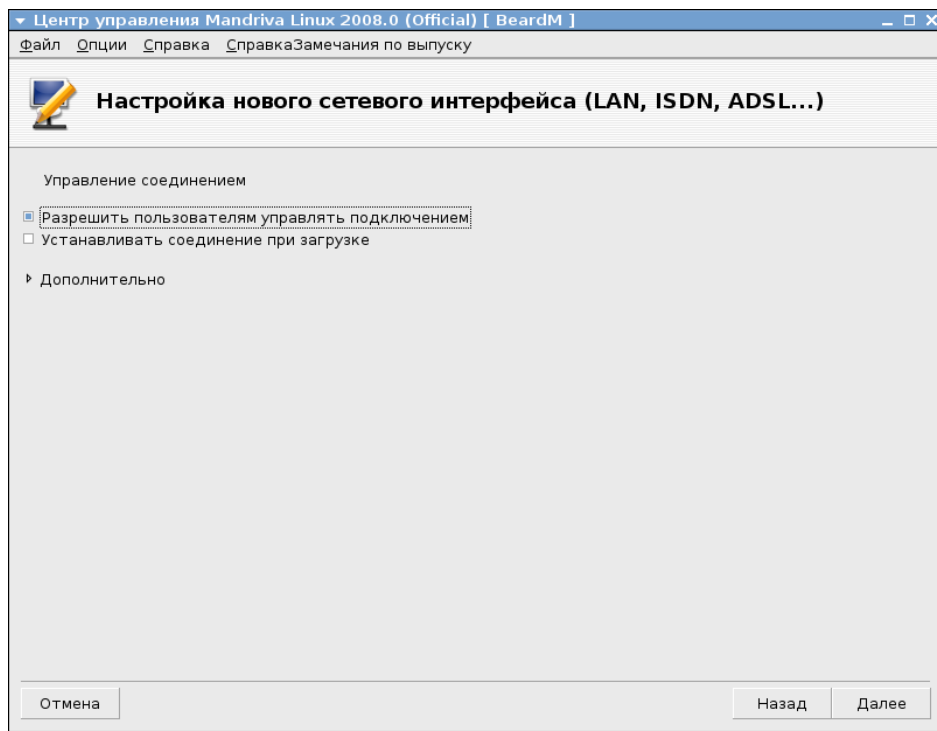


Рис. 2.56. Окно Центр управления Mandriva Linux — Настройка нового сетевого интерфейса (управление соединением)

Мы уже близки к завершению настройки подключения к Интернету через модемное соединение. В очередном окне (рис. 2.56) следует выбрать возможность управлять подключением, но не включать установку соединения при загрузке.

### **ВАЖНО!**

Если включить опцию **Устанавливать соединение при загрузке**, то система не загрузится, пока не будет установлено подключение к Интернету, а при ошибочной настройке подключения она не загрузится вообще.

После завершения настроек система предложит выполнить подключение к Интернету. Если ваша АТС позволяет производить набор в тональном режиме, то соединение состоится. В противном случае в этой версии Linux придется обратиться к программе **Gnome PPP** (рис. 2.57). Если она не установлена, то установите ее.

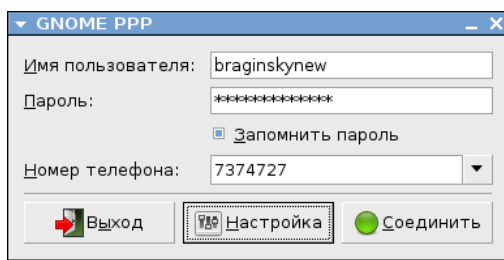
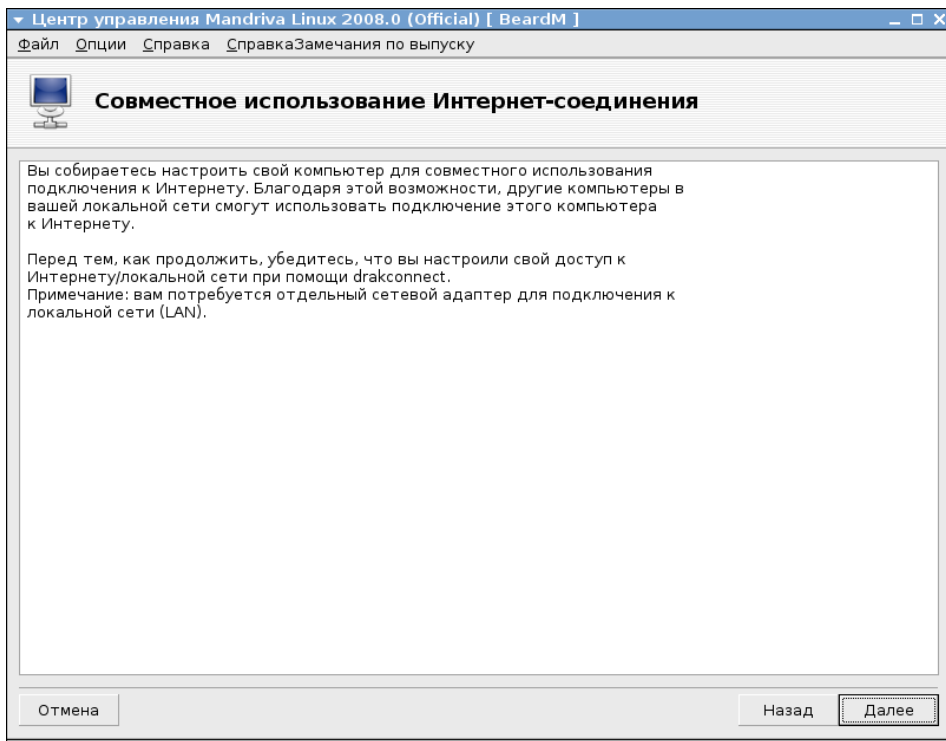


Рис. 2.57. Окно GNOME PPP

Эта программа позволяет дополнительно настроить существующее модемное подключение, а также комфортно управлять им.

Теперь выход в Интернет есть, но только для локального компьютера. Нам требуется настроить общий доступ к подключению Интернета. Снова обратимся к окну **Центр управления Mandriva Linux** меню **Сеть и Интернет** (см. рис. 2.48). Если ваш модем распознан системой, то утилита **Совместное использование Интернет-соединения** (рис. 2.58) поможет выполнить настройку общего доступа.



**Рис. 2.58.** Окно **Центр управления Mandriva Linux — Совместное использование Интернет-соединения**

В следующем окне (рис. 2.59) требуется выбрать интерфейс, непосредственно подключенный к Интернету. Предполагается, что система должна обнаружить подключенный модем, но вполне возможно, что этого не произойдет. Linux, в отличие от Windows, не всегда имеет графические средства для всевозможных настроек. Иногда приходится обращаться к файлам конфигурации и консоли (командной строке).

Чтобы заработал общий доступ к подключению Интернета, необходимо, чтобы наш компьютер мог исполнять роль маршрутизатора между локальной сетью и Интернетом. Для того чтобы включить маршрутизацию, найдите файл `/etc/sysctl.conf` и допишите в нем строку `net.ipv4.ip_forward = 1`.

Если уже есть строка `net.ipv4.ip_forward = 0`, то следует отредактировать ее, заменив ноль единицей.

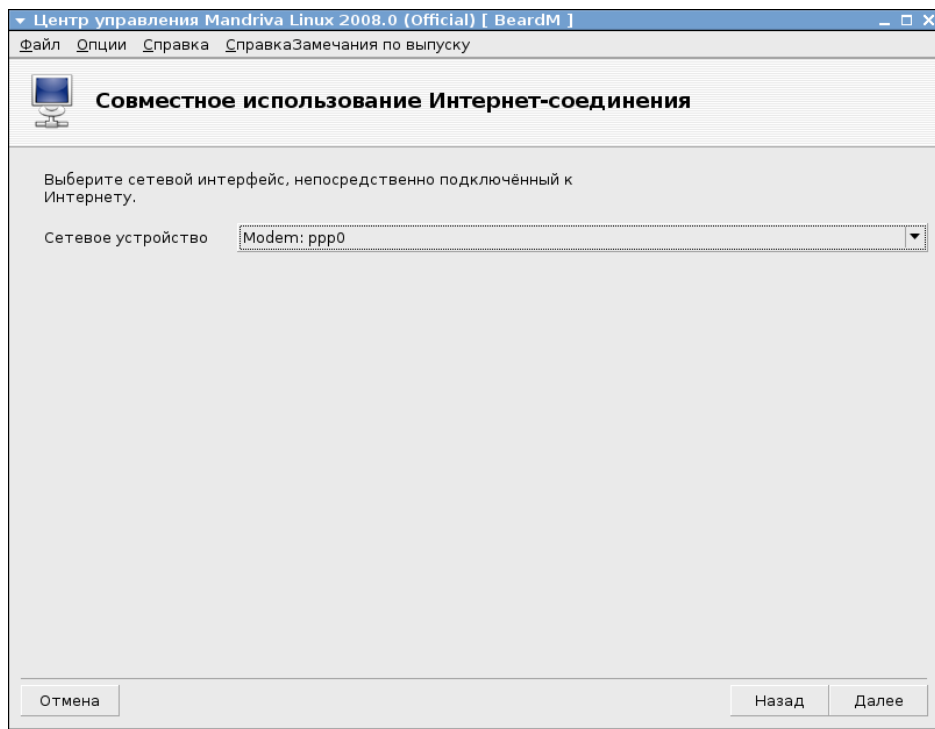


Рис. 2.59. Окно **Центр управления Mandriva Linux — Совместное использование Интернет-соединения** (выбор сетевого интерфейса)

### ПРИМЕЧАНИЕ

Для редактирования файла `sysctl.conf` потребуются права администратора. Проще всего сделать это из окна терминала. Введите команду `su`, затем пароль администратора. Теперь команду `mc`. Откроется файловый менеджер, в котором встроена возможность редактирования текстовых файлов. Все файлы конфигурации — текстовые файлы.

Теперь выполните команду `/sbin/sysctl -p /etc/sysctl.conf` и перезагрузите компьютер. Маршрутизация теперь будет включена, а наш компьютер может быть шлюзом в Интернет.

## В Linux Mint

Рассмотрим еще один вариант настройки общего доступа в Интернет в Linux на примере Linux Mint.

Не всегда есть необходимость компьютер с общим доступом в Интернет непосредственно подключать к Интернету. Нередко компьютер общего доступа используется только для управления подключениями других компьютеров, а выход в Интернет организован через аппаратный маршрутизатор. В операционных системах на основе Linux Debian, к которым относится и Linux Mint, есть много полезных средств для управления подключениями, причем как консольных (управление только из командной строки), так и графических.

Предположим, что само подключение к Интернету реализовано с помощью аппаратных средств, а для подключения сети к Интернету есть Ethernet-порт. Такой вариант, например, рассмотрен в разд. "Подключение через ADSL-модем" этой главы.

Компьютер общего доступа в этом случае должен иметь два сетевых интерфейса. Один интерфейс для собственного подключения к глобальной сети Интернет (внешний интерфейс), а второй для раздачи подключения компьютерам в локальной сети (внутренний интерфейс). Примем, что внешний интерфейс это eth0, а внутренний — eth1. Внешний интерфейс имеет IP-адрес, который не принадлежит локальной сети. Обоим интерфейсам должны быть назначены статические IP-адреса.

Для перенаправления запросов от компьютеров локальной сети в Интернет и преобразования их адресов в адрес внешнего интерфейса, от имени которого они будут иметь выход в глобальную сеть, достаточно в окне терминала или в консольном сеансе выполнить две команды:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Команды необходимо выполнять от имени пользователя root, который имеет административные привилегии. В Debian, Ubuntu и Linux Mint для этого достаточно в начале строки команды ввести sudo и пробел. Перед выполнением команды система запросит пароль пользователя.

В Linux Mint можно получить права администратора сразу для консольного сеанса. Для этого следует ввести команду su -. Дефис в команде пишется через пробел. После ввода пароля пользователя вы получите консольный сеанс администратора, в котором можно вводить указанные команды, как они приведены в примере.

Консольных сеансов в любой Linux не менее шести. Для вызова консольного сеанса необходимо нажать следующую комбинацию клавиш <Alt>+<Ctrl>+<Fn>, где n номер вызываемой консоли. Для возврата в графический режим нажмите <Alt>+<Ctrl>+<F7>.

Приведенные команды действуют до перезагрузки компьютера, и их необходимо вводить каждый раз при включении или после перезагрузки. Чтобы закрепить за компьютером функцию шлюза в Интернет, необходимо редактировать конфигурационные файлы. Материалов на эту тему в Интернете достаточно и при желании вы можете ознакомиться с ними, но легкого пути не ждите. Более простой путь — настройка в Linux Mint через графический интерфейс.

Предварительно необходимо установить программу Firestarter.

На рисунке (рис. 2.60) показано окно уже работающей программы.

Во время первого запуска программы запускается мастер настройки, который можно запустить и позднее по команде **Run Wizard** из меню **Firewall**. Основные вопросы мастера будут об интерфейсах. Какой сетевой адаптер подключен к Интернету, а какой к локальной сети. Если предварительно сетевые интерфейсы были настроены, то по завершении работы мастера будет включена маршрутизация меж-



ду сетевыми интерфейсами и компьютер, подключенный к интерфейсу local, сможет использовать подключение к Интернету основного компьютера.

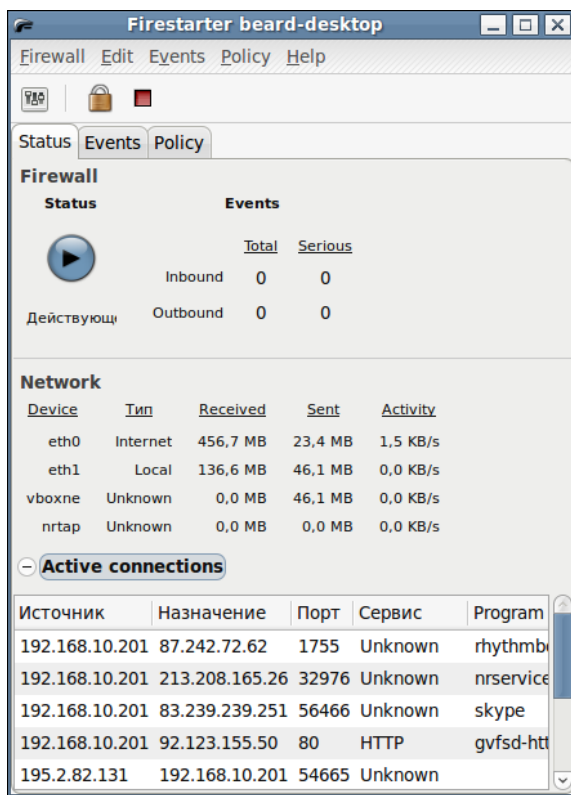


Рис. 2.60. Окно Firestarter

Теперь вы можете использовать общее подключение к Интернету в вашей сети. Но, имея возможность беспрепятственно бродить по Интернету с любого компьютера сети, следует подумать и о защите от тех опасностей, которыми нас не радует Интернет. То вирус, то непрошенные гости в нашем компьютере. Всякое бывает. Будем защищаться.

## ГЛАВА 3



# Защищаем сеть

Используя какую-либо технику, необходимо соблюдать правила ее эксплуатации. Иначе возможны непредвиденные неисправности и отклонения от штатных режимов работы. Компьютер, и прежде всего компьютер, включенный в сеть, также требует соблюдения правил эксплуатации. В числе прочих очень важным является обеспечение защиты операционной системы от воздействия компьютерных вирусов, вредоносных программ и вмешательства незарегистрированных на компьютере пользователей и злоумышленников. Частично заботу о защите компьютера берут на себя разработчики операционных систем, включая в их состав необходимые программы. Но эти программы должны быть правильно настроены, необходим регулярный контроль над их работой. Нередки случаи, когда пользователи ПК, настраивая работу каких-либо программ, временно снижают уровень защиты компьютера или вовсе отключают защиту, а затем забывают восстановить ее нормальное функционирование. Результатом этой безответственности становятся украденные логины, пароли, испорченные данные, а иногда и полная неработоспособность операционной системы.

В этой главе рассмотрены наиболее доступные средства защиты.

## Брандмауэр

Если компьютер подключен к Интернету, но система не имеет никакой защиты от доступа извне, то велика вероятность того, что кто-либо по злому умыслу или из любопытства попытается проникнуть к вам на компьютер. Последствия такого проникновения не предсказуемы. Проникновение возможно как в ручном режиме, так и автоматически с неблагонадежных сайтов. На ваш компьютер могут быть установлены программы-шпионы для сбора сведений о ваших интересах или программы, которые помимо вашей воли будут направлять вас на определенные сайты в Интернете. Для защиты компьютеров от подобных атак существуют программные средства — "*файерволы*" (*firewall*) или иначе *брандмауэры*.

## Брандмауэр Windows

Для того чтобы защитить компьютер от несанкционированного доступа к нему, в состав Windows XP SP2 и старше включено средство, которое закрывает доступ к компьютеру извне во всех случаях, кроме явно разрешенных пользователем. Брандмауэр настраивается системой автоматически при первом указании пользователем вида сети, в которую входит компьютер. В дальнейшем при желании можно изменить настройки защиты.

Получить доступ к настройкам Брандмауэра Windows можно, открыв из окна Центра обеспечения безопасности Windows окно **Брандмауэр Windows** (рис. 3.1), воспользовавшись соответствующим пунктом меню.

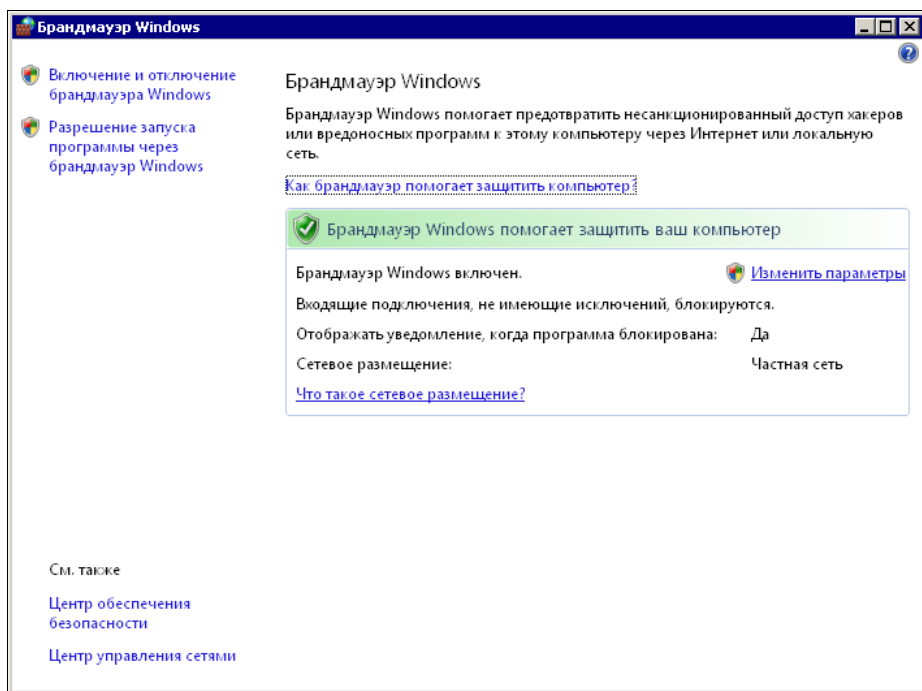


Рис. 3.1. Окно Брандмауэр Windows

Воспользовавшись ссылкой **Изменить параметры**, имеющейся в этом окне, можно открыть окно **Параметры брандмауэра Windows** (рис. 3.2), которое имеет три вкладки, на каждой из которых можно выполнить определенные настройки.

Так, на вкладке **Общие** можно выключить или включить брандмауэр Windows, выбрать режим **Блокировать все входящие подключения**, который может быть полезен при работе в неизвестных вам и небезопасных сетях.

На вкладке **Дополнительно** (рис. 3.3) можно указать те сетевые подключения, которые должны быть защищены брандмауэром. Вполне возможно, что одно из подключений используется вами для связи со вторым своим компьютером. Защищать себя от себя, возможно, вам не потребуется.

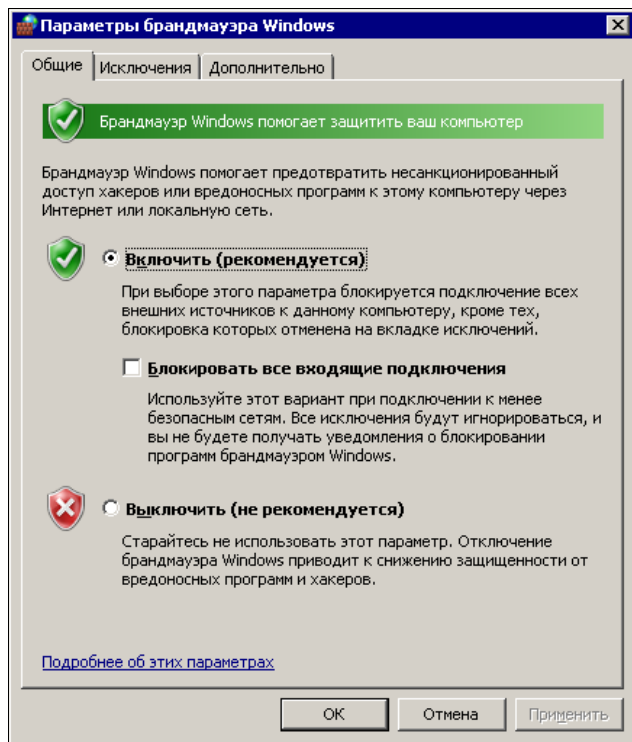


Рис. 3.2. Окно Параметры брандмауэра Windows, вкладка Общие

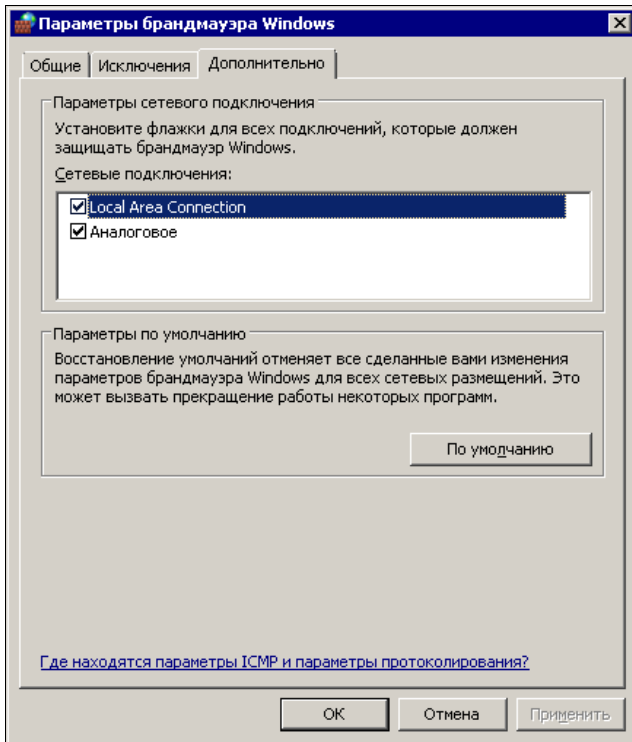


Рис. 3.3. Окно Параметры брандмауэра Windows, вкладка Дополнительно

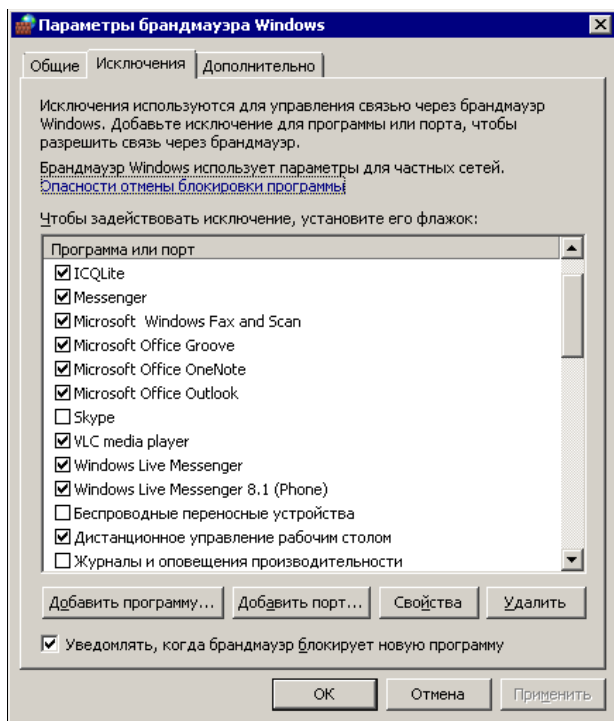


Рис. 3.4. Окно Параметры брандмауэра Windows, вкладка Исключения

На вкладке **Исключения** (рис. 3.4) можно указать программы или отдельные порты, к которым необходимо обеспечить беспрепятственный доступ из сети или Интернета. Автор использует, например, удаленный доступ к рабочему столу своего компьютера. Конечно, **Дистанционное управление рабочим столом** должно быть исключено из числа блокируемых внешних обращений к компьютеру.

Исключения вы можете добавлять самостоятельно, указав, например, порт, используемый программой (рис. 3.5). Но исходя из соображений безопасности, вы

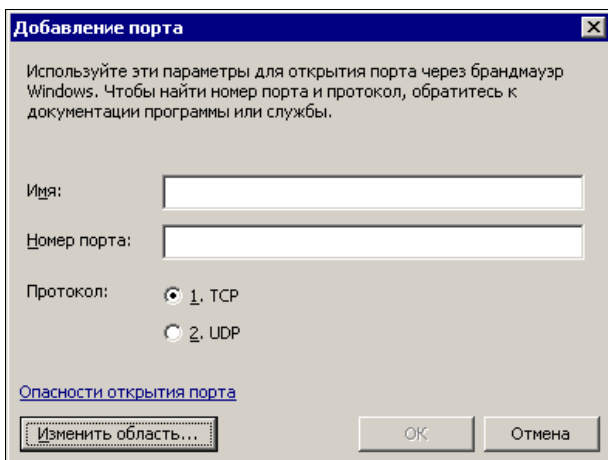


Рис. 3.5. Окно Добавление порта

можете ограничить число компьютеров, с которых будет возможен доступ к этому порту, указав конкретные значения разрешенных IP-адресов, воспользовавшись кнопкой **Изменить область**. Можно, конечно, разрешить доступ для всех или для определенной сети (рис. 3.6).

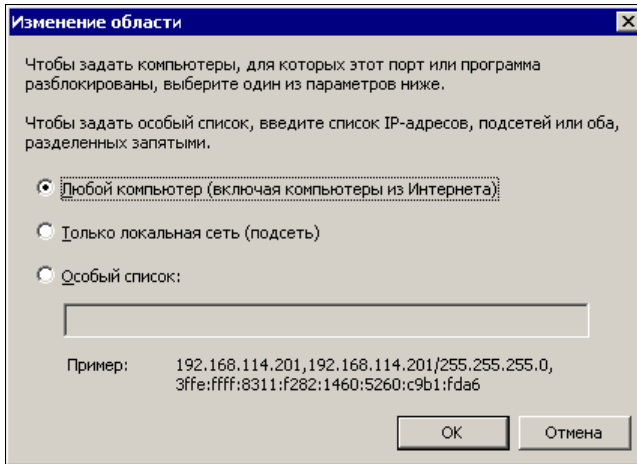


Рис. 3.6. Окно Изменение области

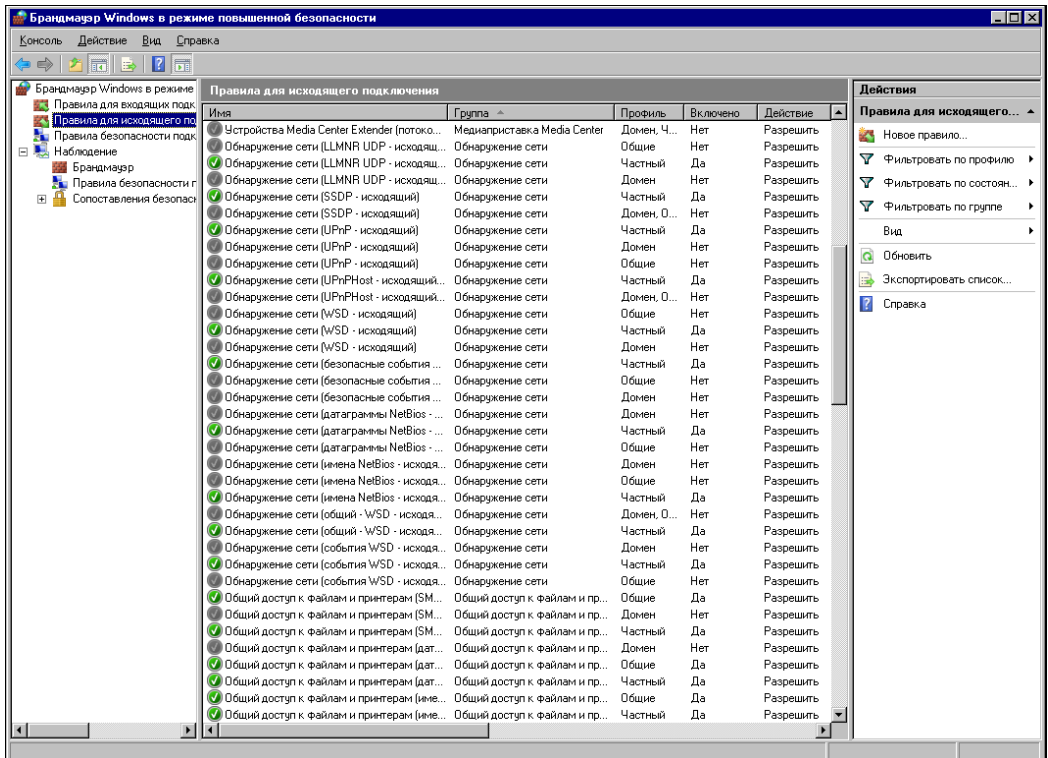


Рис. 3.7. Окно Брандмауэр Windows в режиме повышенной безопасности

Если вопросы безопасности для вас имеют очень серьезное значение, то через меню **Администрирование** в Панели управления можно открыть апплет **Брандмауэр Windows в режиме повышенной безопасности** (рис. 3.7). Здесь есть возможность очень тонкой настройки правил для входящих и исходящих пакетов.

## Файервол в Mandriva Linux

В Linux настройка защиты компьютера не сложнее, чем в Windows.

Откройте окно **Центр управления Mandriva Linux** и в левой ее части выберите **Безопасность** (рис. 3.8).

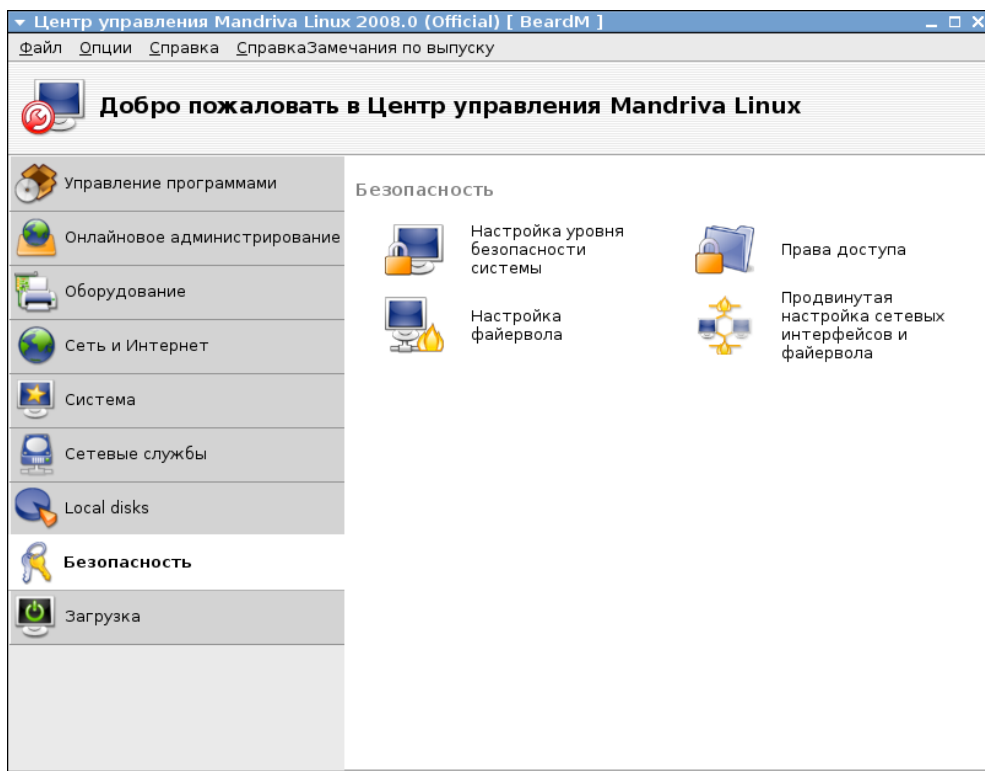


Рис. 3.8. Окно **Центр управления Mandriva Linux — Безопасность**

В правой части окна активизируйте утилиту **Настройка файервола**. В открывшемся одноименном окне (рис. 3.9) выберите службы, которым необходимо предоставить доступ к компьютеру. Если есть особые службы, отсутствующие в списке, можно указать номера портов и протоколов, через которые они работают.

Нажмите **ОК**, и в следующем окне (рис. 3.10) можно выбрать службы, обращение к которым будет сопровождаться сообщением.

В следующем окне (рис. 3.11) отметьте интерфейсы, которые необходимо защитить.

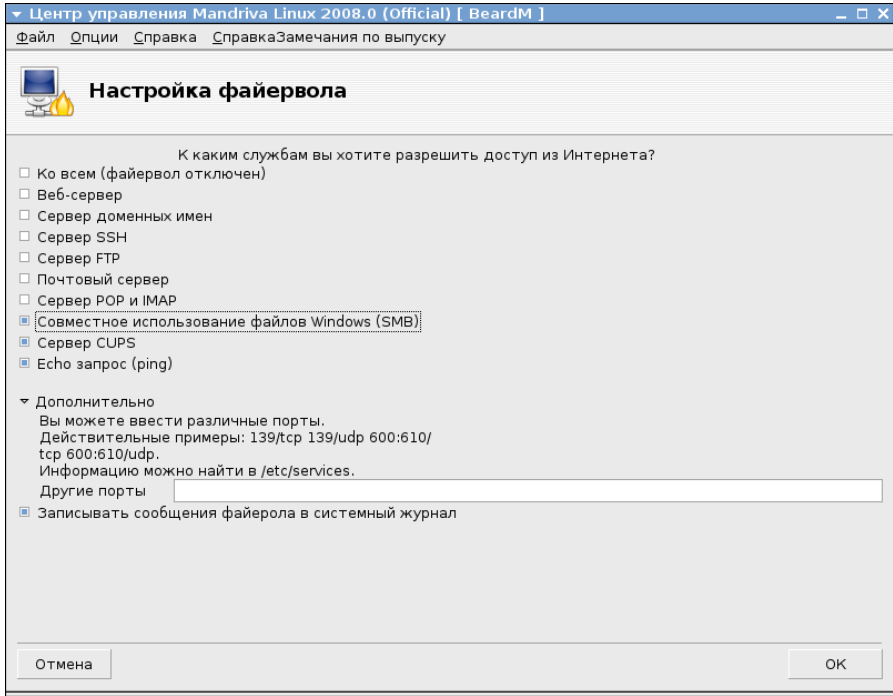


Рис. 3.9. Окно Центр управления Mandriva Linux — Настройка файервола (выбор служб)

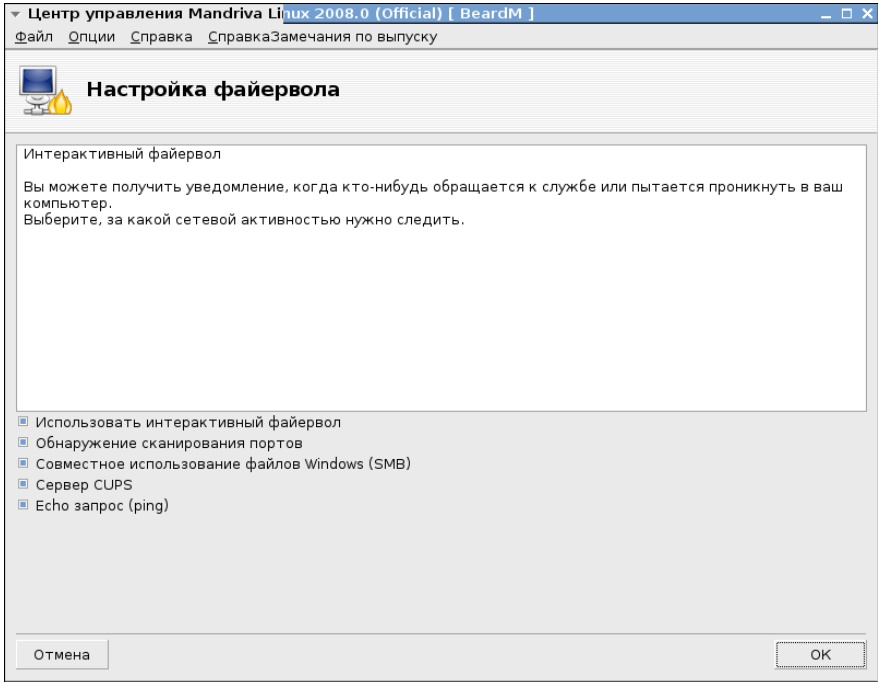


Рис. 3.10. Окно Центр управления Mandriva Linux — Настройка файервола (интерактивный файервол)



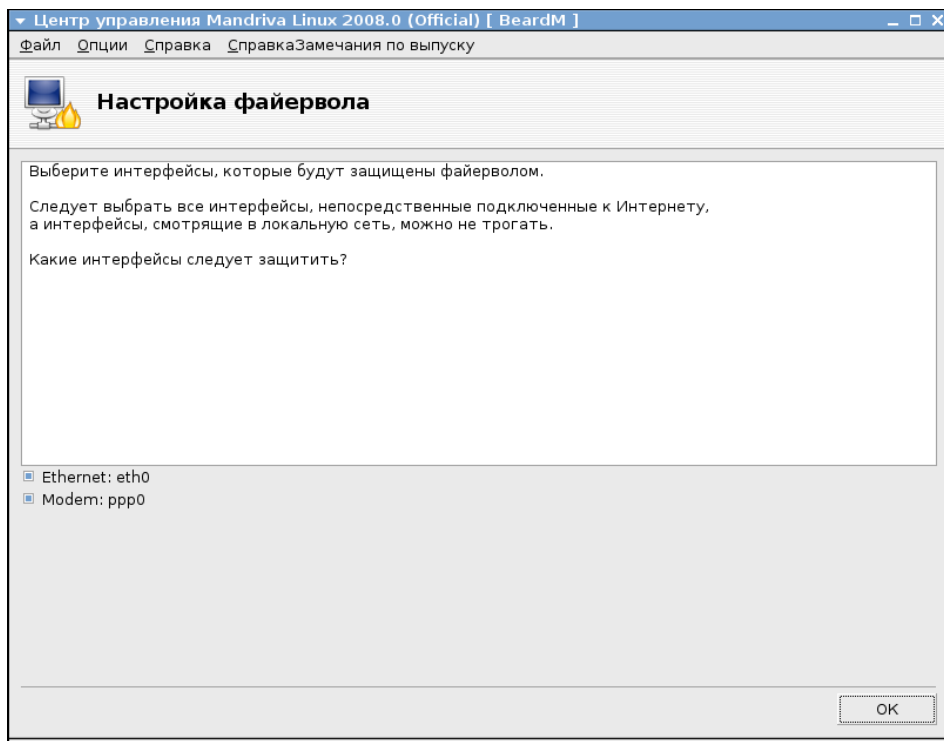


Рис. 3.11. Окно Центр управления Mandriva Linux — Настройка файервола (выбор защищаемых интерфейсов)

Файервол следует настраивать каждый раз, когда появляются новые программы или службы, требующие доступа к компьютеру из локальной сети или Интернета.

## Брандмауэр для Windows Comodo

По адресу в Интернете <http://www.personalfirewall.comodo.com> можно получить бесплатную программу *Comodo Firewall Pro*. Последняя версия программы 5.0. В распоряжении автора на момент написания этих строк была версия 3.0 (рис. 3.12), не имеющая русскоязычного интерфейса, как и все новые версии программы, но совместимая с Windows Vista.

Версия 2.4 (рис. 3.13) с русскоязычным интерфейсом, предназначенная для работы в Windows 2000/XP/2003, доступна по адресу <http://www.comss.ru/page.php?id=14>.

Интерфейсы и возможности версий программы отличаются довольно существенно. В последних версиях программы есть режим обучения. В качестве программы для защиты от сетевых вторжений вполне достаточно версии 2.4. Применяя эту программу, можно отключать брандмауэр Windows, выполнив все необходимые настройки в Comodo Firewall Pro. Сетевые правила легко добавляются, удаляются и редактируются. Конкретные рекомендации по настройке файервола давать сложно. Кто-то работает в безопасной сети, где только доверенные компьютеры, и защита



Рис. 3.12. Окно COMODO Firewall Pro (версия 3.0)

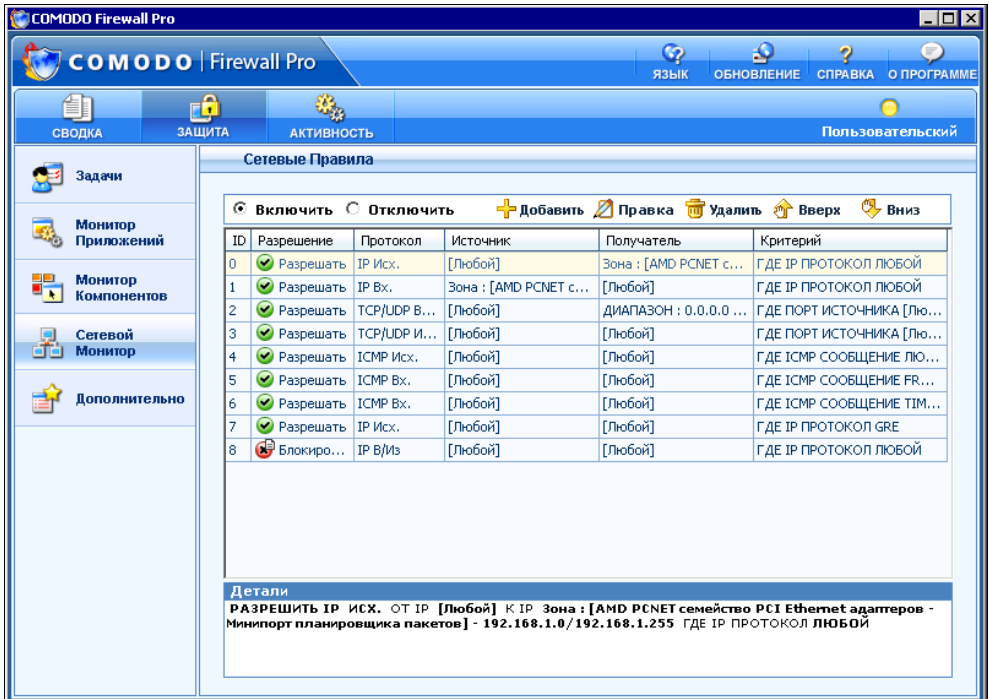


Рис. 3.13. Окно COMODO Firewall Pro (версия 2.4)

от вторжений из этой сети не требуется. Кто-то наоборот, обеспокоен возможностью атак на его компьютер с любой стороны и устанавливает самый высокий уровень защиты, когда перекрыты возможности обмена информацией с внешним миром по всем портам, адресам и протоколам, за исключением самых необходимых. Приведем небольшое описание функций программы, которые появились в новой версии.

#### Режим чистого ПК (Clean PC Mode)

При этом режиме все установленные на компьютере программы по умолчанию признаются безопасными. И только новые программы, пытающиеся получить права на управление компьютером, будут блокироваться, пока не получат на это ваше разрешение. Этот режим защищает от большинства вредоносных программ и руткитов. Полезно при установке Comodo Firewall Pro на новый компьютер (или после переустановки системы).

#### **ПРИМЕЧАНИЕ**

*Руткит (rootkit)* — это набор программ, которые модифицируют имеющиеся исполняемые файлы в системе. Данный процесс нарушает целостность базы доверия компьютера (Trusting Computer Base).

#### Defense+

Defense+ закрывает доступ к критическим системным файлам и блокирует вредоносные программы до того, как они получают шанс установиться.

#### Продвинутый движок сетевого файервола (Advanced Network Firewall Engine)

В новой версии появились новые системы и инструменты: скрытый режим (Stealth Mode), что делает ваш компьютер практически невидимым для вредоносных программ; автоопределитель безопасных зон; защита настроек Comodo Firewall Pro паролем; диагностика возможного конфликта системы с файерволом и многое другое...

#### Режим обучения (Training Mode)

Comodo Firewall Pro 3.0 больше не будет прерывать вашу работу беспочвенными сообщениями по поводу программ, которым вы доверяете. Режим "Train with Safe Mode" позволяет компьютеру запомнить безопасные приложения и тихо создать правила для них.

#### Увеличенная база данных программ

На сегодняшний день Comodo Firewall Pro распознает около миллиона программ по степени их безопасности. Перед установкой каждой из известных программ проверяются ее параметры, чтобы исключить возможность маскировки вредоносных программ под безопасные.

Установив и настроив эту программу, можно быть уверенным, что вредоносные программы не нарушат целостности операционной системы Windows.

## И снова Firestarter

В Linux есть прекрасно работающий Firewall, но настраивается он обычно путем правки конфигурационных файлов. Утилита Firestarter, с помощью которой мы превращали компьютер в шлюз Интернета, позволяет графическими средствами выполнить основные настройки Firewall в Linux.

На вкладке **Policy** (политики) окна утилиты Firestarter (рис. 3.14) можно определить правила для сетевого экрана. Для добавления правил достаточно вызвать контекстное меню щелчком правой кнопки мыши в выбранном разделе вкладки **Policy** и выбрать **Add Rule** — добавить правило.

Правила могут быть определены для входящего и исходящего трафика.

При выборе **Inbound traffic policy** (правил входящего трафика) в раскрывающемся списке редактирования **Editing** доступны следующие правила:

- Allow connections from host** — всегда разрешать подключение компьютерам. Здесь могут быть указаны как компьютеры локальной сети, так и хосты в Интернете. В сочетании с запрещающими политиками правила могут быть настроены очень гибко;
- Allow service** — всегда разрешать подключение сервисам. Здесь можно настроить разрешения подключений для различных сервисов, использующих известные порты для сетей и компьютеров с указанными IP-адресами, или для всех. Например, как указано на рисунке, открыть порты для работы торрентов (torrent) (порты 6881—6889) и подключения к DNS-серверу (порт 53);
- Forward service** (Сервис перенаправления). Можно указать по каким портам и к каким IP-адресам перенаправлять пакеты из Интернета. Например, если вам требуется получить доступ к рабочему столу компьютера внутри сети, необходимо указать перенаправляемый порт на IP-адрес этого компьютера.

При выборе **Outbound traffic policy** (правил исходящего трафика) в раскрывающемся списке редактирования **Editing** (рис. 3.15) и переключателя разрешения блокировки трафика по умолчанию — **Permissive by default, blacklist traffic** доступны следующие настройки правил:

- Deny connection to host** — запретить подключение к хосту. Здесь можно запретить компьютерам локальной сети подключение к определенным IP-адресам в Интернете;
- Deny connection from LAN host** — запретить подключение к компьютерам локальной сети. IP-адреса указанные в этом разделе будут всегда заблокированы для подключения к ним;
- Deny service** — запретить сервисы. Здесь можно указать службы интернета, которые запрещены для использования компьютерами локальной сети.

При выборе **Outbound traffic policy** (правил исходящего трафика) в раскрывающемся списке редактирования **Editing** (рис. 3.16) и переключателя **Restrictive by default, whitelist traffic** — запрещения для блокировки правил по умолчанию (рис. 3.16), можно указать разрешения для подключений к IP-адресам в Интернете,

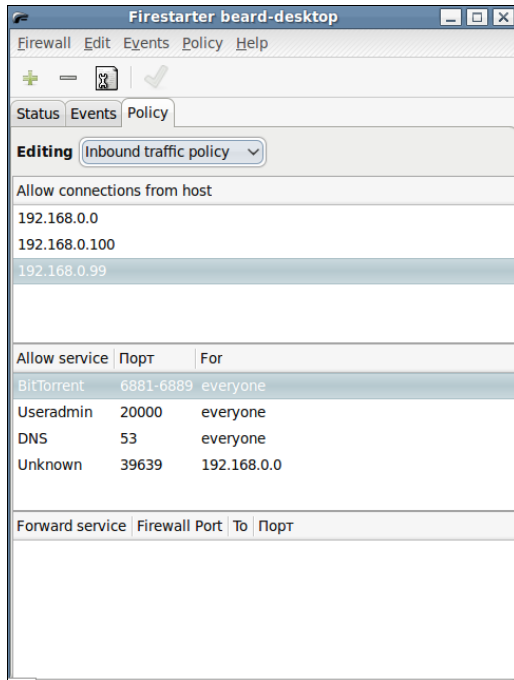


Рис. 3.14. Окно Firestarter, вкладка Policy

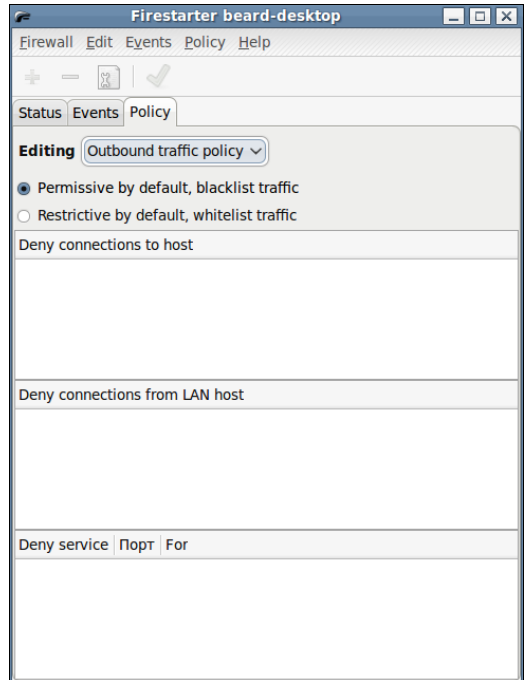


Рис. 3.15. Окно Firestarter beard-desktop, вкладка Policy, режим Outbound traffic policy, Permissive by default, blacklist traffic

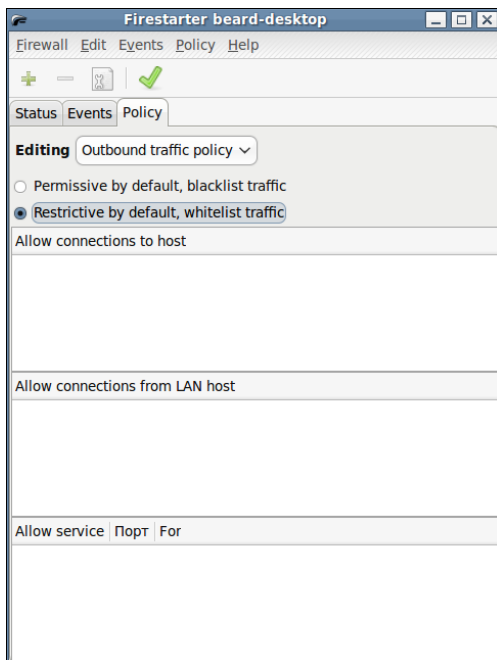


Рис. 3.16. Окно Firestarter beard-desktop, вкладка Policy, режим Outbound traffic policy, Restrictive by default, whitelist traffic

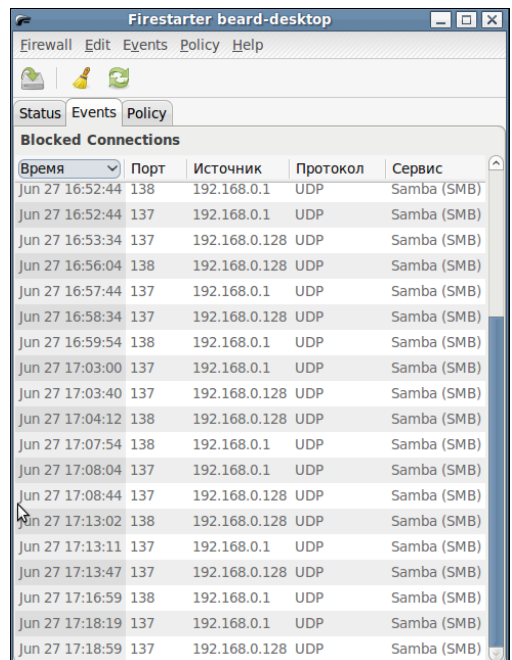


Рис. 3.17. Окно Firestarter beard-desktop, вкладка Events

компьютерам локальной сети или разрешения для применения сервисов и служб, использующих указанные порты, которые будут иметь приоритет над запрещениями.

После настройки необходимых правил на вкладке **Events** (события) (рис. 3.17) можно увидеть регистрируемые программой события во время работы сети.

Анализируя события, полученные утилитой Firestarter, можно оценить верность выполненных настроек Firewall.

## Антивирус

Для Linux существует около сотни вирусов. Еще не было вирусных эпидемий в среде пользователей Linux, но это не значит, что вирусы совершенно безопасны для пользователей этой операционной системы.

*"Linux способна оградить вас от вирусов и хакерских атак, но только в том случае, если вы поможете системе проявить ее лучшие свойства. Поэтому если вы только начинаете, следуйте простым правилам. Выполняйте всю повседневную работу от имени рядового пользователя, root-аккаунт<sup>1</sup> задействуйте только для администрирования системы. Удалите все ненужные программы, постарайтесь избавиться от программ неизвестного назначения, отключите все сервисы, которые вами не используются. Устанавливая программы, пользуйтесь только официальными файловыми архивами, а набравшись опыта, по возможности собирайте новые программы из исходников. Вот, пожалуй, и все. Забудьте про антивирусы и — приятной вам работы!"*

Это цитата со страницы <http://knoppix.ru/130306.shtml>.

Но в нашей сети есть и Windows, а для Windows написано несколько десятков тысяч вирусов. Конечно, можно соблюдать правила, приведенные только что и при работе в Windows (в Windows Vista эту возможность применять удобнее, чем в более старых версиях), но даже в этом случае опасность поражения вирусом в Windows весьма высока.

Это значит, что без антивирусной программы нам не обойтись. Известных антивирусных пакетов довольно много. Все они достаточно эффективно обнаруживают и уничтожают большинство вирусов. Многие имеют антивирусные мониторы, которые обнаруживают и обезвреживают вирусы "на лету". К сожалению, наиболее эффективные антивирусы нередко затрудняют работу пользователя, постоянно сообщая о подозрительных файлах, блокируя работу некоторых программ.

Имея в своей сети Linux, можно использовать ее высокий иммунитет к вирусным заражениям для повышения безопасности работы всей сети. Никто не мешает совершать "прогулки в Интернет" через Linux. Linux имеет простые средства для удаленного подключения к рабочему месту. Можно не отходя от машины с Windows подключаться к компьютеру под управлением Linux. Сохраненные файлы затем можно скопировать или перенести на свой компьютер. Но здесь уже требуется осторожность. Файлы должны быть проверены антивирусной программой. Ка-

---

<sup>1</sup> Root account — учетная запись суперпользователя.

кую же программу выбрать? Многие пользователи Windows хотели бы найти бесплатную антивирусную программу. И такая программа есть. Она не имеет ограничений по времени использования, обновляет свои базы через Интернет и легально совершенно бесплатна. Она не содержит антивирусных мониторов, но сканирует папки, диски, отдельные файлы, которые вы ей укажете. Для нашего случая очень подходящий вариант. Получить программу, которая называется *Clam AntiVirus*, можно, загрузив ее со страницы <http://ru.clamwin.com/content/view/18/46/>. Интересно, что существует портативная версия программы, которая не требует установки и может быть запущена с флэшки [http://portableapps.com/apps/utilities/clamwin\\_portable](http://portableapps.com/apps/utilities/clamwin_portable).

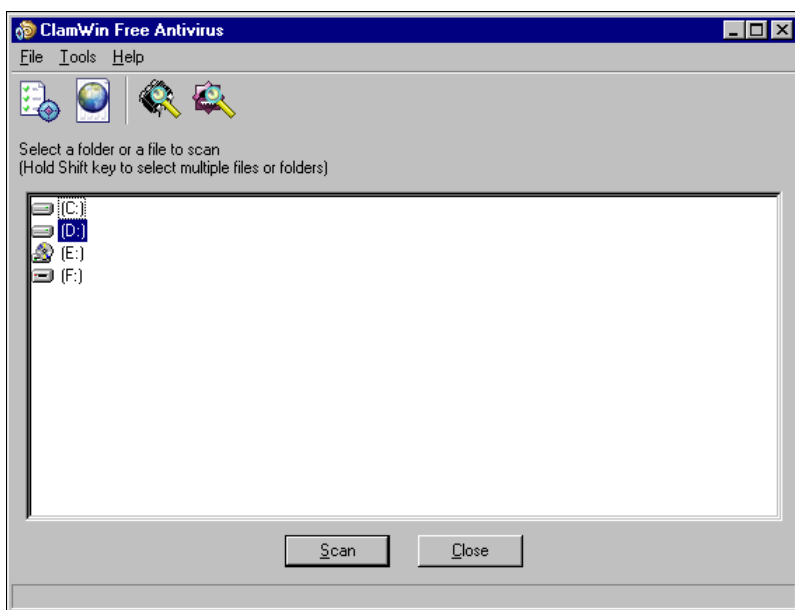


Рис. 3.18. Окно ClamWin Free Antivirus

Интерфейс программы английский, но очень простой (рис. 3.18). Четыре кнопки под заголовком окна позволяют (в порядке расположения) вызвать настройки программы, обновить антивирусные базы, сканировать память компьютера и выбранные файлы.

Программа существует и для Linux. При желании вы можете получить версии программы для других операционных систем со страницы <http://www.clamav.org/download/>.

## Avast!

Avast! — это еще одна бесплатная для домашнего применения антивирусная программа (рис. 3.19). Для ее легального использования требуется регистрация на сайте программы. Существует русскоязычный сайт <http://www.avast.ru>, где можно найти информацию и о коммерческих версиях программы.

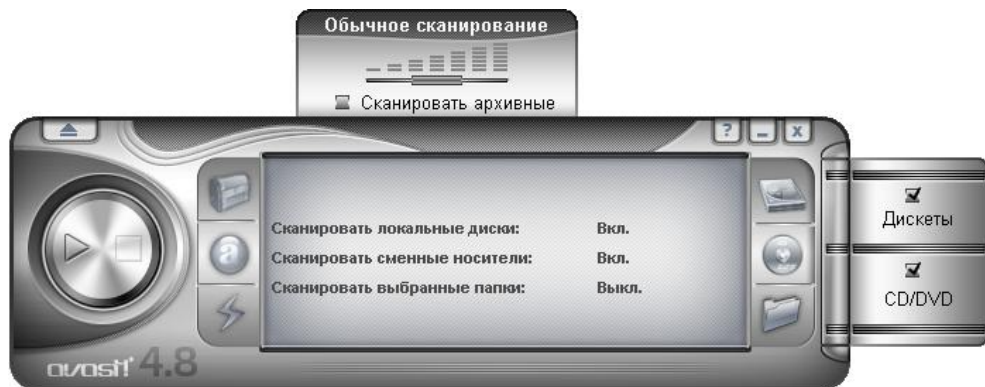


Рис. 3.19. Окно программы avast! 4.8

Работа с программой avast! не вызывает проблем даже у начинающих пользователей. Русскоязычный интерфейс, настройки по умолчанию, которые вполне подходят для повседневной обычной работы с компьютером, возможность как ручного режима работы, так и автоматического, когда сканирование файлов, программ, сетевой активности, электронной почты происходит "на лету".

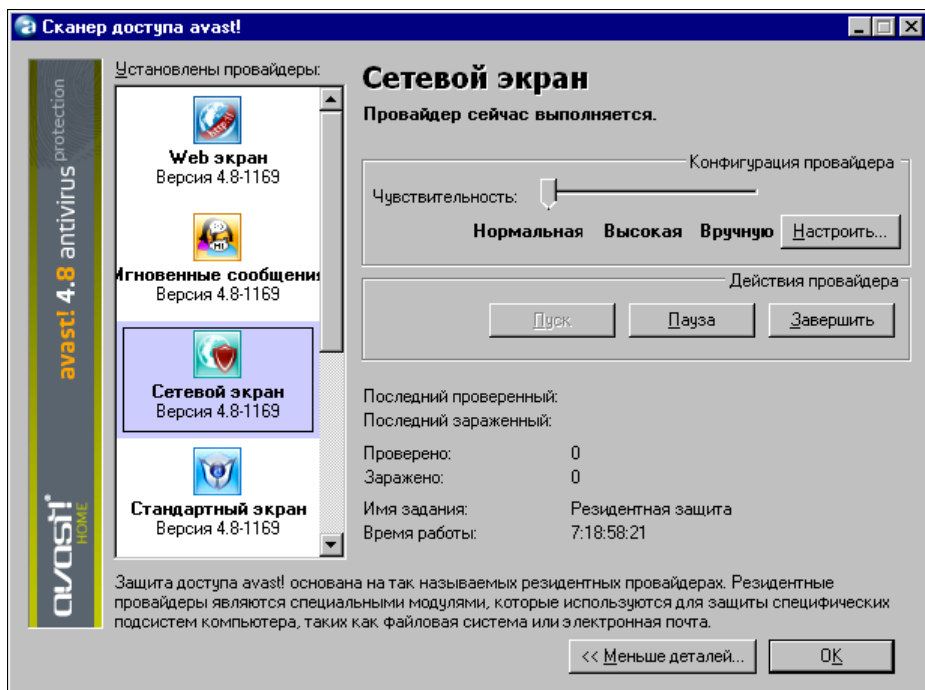


Рис. 3.20. Окно Сканер доступа avast!

Автоматическое сканирование осуществляют специальные модули — провайдеры, настройка которых может быть выполнена в окне **Сканер доступа avast!** (рис. 3.20).



## AnVir Task Manager

Программой AnVir Task Manager автор пользуется постоянно. Она является прекрасным дополнением к другим антивирусным программам, с которыми никогда не конфликтует. Для русскоязычных пользователей программа бесплатна. Но, если программа вам понравится, автор просит угостить его пивом.

AnVir Task Manager — это менеджер процессов и программ автозапуска с функциями антитрояна, *antispyware* и антивируса, позволяющий:

- видеть полную информацию о запущенных процессах, используемые файлы и путь к ним, команду запуска, использование памяти, диска и процессора, загруженные *dll*, созданные окна, потоки и идентификаторы процессов, счетчики производительности, информацию о версии файла;
- управлять файлами автозапуска Windows, отключать, редактировать записи в реестре и в папке "Автозагрузка". Отслеживать и блокировать попытки программ добавить себя в автозагрузку. В программу встроена база данных по 17000 автозагружаемым программам. Поддерживаются перекрестные ссылки между процессами и программами автозагрузки;
- удалить с зараженного компьютера вирусы и вредоносные программы, скрыто работающие на компьютере;
- ускорить время загрузки Windows за счет отключения ненужных программ и использования функции отложенного запуска программ автозапуска. Автоматически менять приоритет процессам или завершать процессы по заданному шаблону;
- анализировать информацию о текущей загрузке процессора и жесткого диска, которая динамически выводится в системный трей (*system tray*) и в строку состояния (*status bar*) в виде иконок и списка процессов, наиболее активно потребляющих ресурсы компьютера. Ведется журнал (*log*) созданных и завершенных процессов, созданных окон;
- запускать последние запущенные или избранные приложения через автоматически заполняемое меню в трее;
- управлять поведением окон программ.

Программа AnVir Task Manager имеет удобный пользовательский интерфейс, высокое быстродействие, небольшой размер дистрибутива. AnVir Task Manager является удобным инструментом для решения задач обеспечения безопасности и защиты, оптимизации быстродействия и использования ресурсов компьютера. AnVir Task Manager может заменить такие программы, как стандартный диспетчер задач Windows, Process Explorer и WinPatrol (<http://www.winpatrol.com/>).

Получить программу можно по адресу в Интернете [http://www.anvir.com/index\\_ru.htm](http://www.anvir.com/index_ru.htm).

Даже беглого взгляда на окно программы (рис. 3.21) достаточно, чтобы увидеть, что возможности программы очень широки. Последняя версия программы, имеющаяся у автора, появилась в марте 2008 года.

The screenshot displays the AnVir Task Manager application window. The main window title is "AnVir Task Manager [Версия для некоммерческого использования]". The interface includes a menu bar (Файл, Процессы, Вид, Инструменты, Помощь), a toolbar, and a main table listing system services. Below the table, there are three detailed panels: "База автозагрузки и сервисов" (Autostart and services database), "Анализ риска безопасности" (Security risk analysis), and "Свойства процесса" (Process properties).

Продукт	Уровень риска	Автозагрузка	ЦП %	Загрузка д...	Сеть: При...	Сет...	Ско...	Скор...	Использ. па...	Заго...
Automatic LiveUpdate Scheduler Service	Нулевой риск	Сервисы: План...	0	0					1 312 K	
AnVir Task Manager	Нулевой риск		22	1 Kb/s					10 908 K	A
ApmMsgFwd	Нулевой риск		0	0					1 836 K	
Alps Pointing-device Driver for Windows N...	Низкий риск		1	15 Kb/s					2 176 K	
Alps Pointing-device Driver	Нулевой риск	Реестр: Автос...	0	0					3 100 K	
Apple Mobile Device Service	Нулевой риск	Сервисы: Appl...	0	0					812 K	
Global Virtual Card Host	Низкий риск		0	1 Kb/s					19 176 K	
avast! service GUI component	Нулевой риск	Реестр: Автос...	2	0					10 032 K	C
avast! e-Mail Scanner Service	Нулевой риск	Сервисы: avast...	0	0					2 800 K	
avast! antivirus service	Нулевой риск	Сервисы: avast...	0	0					17 140 K	
avast! Web Scanner	Нулевой риск	Сервисы: avast...	0	0	1,23 МБ				36 028 K	

The "База автозагрузки и сервисов" panel shows details for "Alps Pointing-device Driver" (Apoint.exe) with a path to the registry and a description: "Touchpad software for laptop PC's. For instance it is found on the Panasonic and Sony Vaio machines and allows part of the touchpad to be used for...".

The "Анализ риска безопасности" panel shows a "Суммарный уровень риска: Нулевой" (Overall risk level: Zero).

The "Свойства процесса" panel shows details for the "Alps Pointing-device Driver" process (apoint.exe, PID 4412), including its path and start time (09.05.2008 18:11).

The status bar at the bottom indicates system resource usage: "Загрузка ЦП: 20% | anvir 22% | system 4% | Загрузка диска | C: 1% | D: 0% | aprtex 15 | Использов. памяти: 59% | Всего: 2045 Мб | 3 | Прием: 0 байт/с | Отправление: 0 байт/с | Пр...

Рис. 3.21. Окно AnVir Task Manager

Скорее всего, описанных программ вам будет достаточно для защиты своего компьютера в сети. При желании, конечно, можете поискать и другие программы, но в этой главе рассмотрены те, что достаточно эффективны, но распространяются бесплатно или находятся в составе операционной системы.



## ЧАСТЬ II

### Необычные решения в сети

Не всегда есть возможность создать локальную сеть по всем правилам. Либо для этого недостаточно средств, либо условия для объединения компьютеров какие-нибудь особенные, не позволяющие их выполнить стандартными средствами, применяемыми в кабельных локальных сетях. В следующих главах рассмотрены примеры объединения двух компьютеров не стандартными для обычных локальных сетей способами.



## ГЛАВА 4



# Соединяем удаленные компьютеры

Возможно, что у вас уже возникала идея объединить два компьютера в простейшую сеть. Но вы не нашли решения задачи, поскольку не всегда есть возможность проложить кабель между двумя узлами локальной сети. Возможно, например, что компьютеры расположены в соседних домах или в разных районах города, и расстояние между ними значительно превышает предельное для обычной кабельной сети на *витой паре*. Возможно, конечно, применение оптоволоконного кабеля, но ради объединения двух компьютеров в простую сеть затраты на прокладку такого кабеля слишком велики. В таких случаях можно использовать уже существующие каналы связи, например телефонную линию или Интернет. Обычно для этого требуется совсем не много. Более того, чаще всего оно уже у вас есть!

## Соединяем удаленные компьютеры через модем

Не вам первым пришла в голову такая идея! На просторах Интернета можно найти решение такой задачи, и не одно.

## Соединяем компьютеры под управлением Windows Vista

Современные операционные системы в наибольшей степени приспособлены для работы в сети. Настройка подключения к Windows Vista, пожалуй, упрощена до минимума. На компьютере, с которого производится подключение, необходимо создать обычное модемное сетевое подключение, аналогично тому, которое используется для подключения к Интернету. Если вы решили с работы подключиться к домашнему компьютеру по телефонной линии, то в свойствах подключения следует указать ваш домашний телефон. А на приемной стороне — на домашнем компьютере — следует настроить входящее подключение.

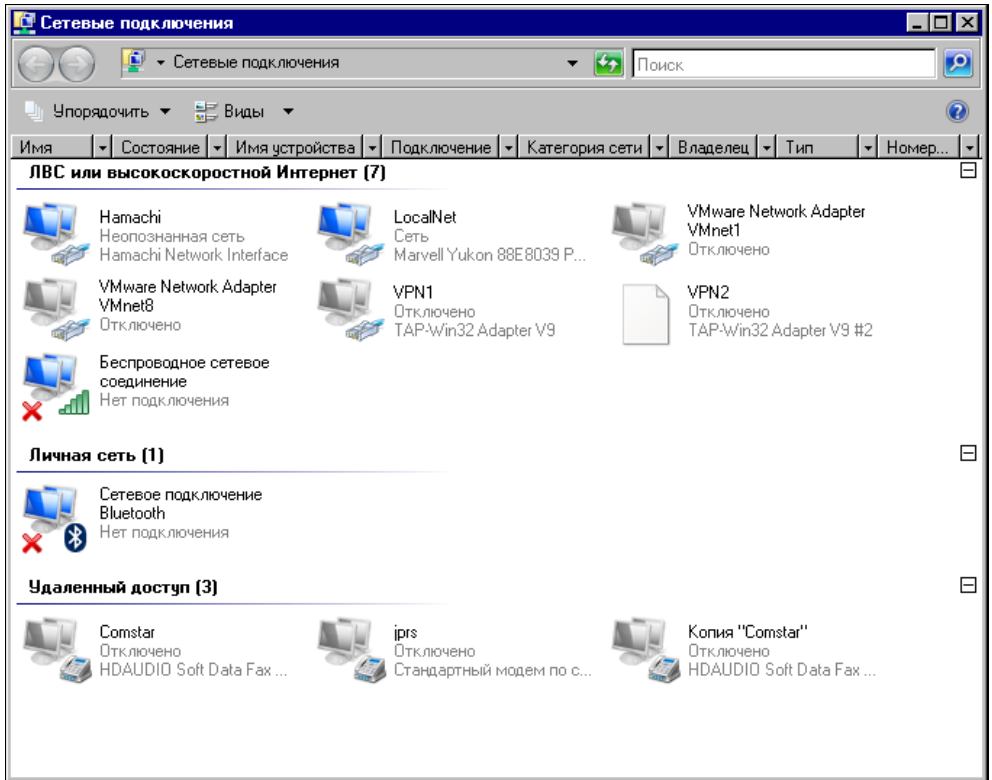


Рис. 4.1. Окно Сетевые подключения

Для этого выполните следующее:

1. Откройте **Панель управления | Сетевые подключения** (рис. 4.1).

#### **ПРИМЕЧАНИЕ**

Если вы не можете найти в панели управления значок **Сетевые подключения**, то открыть эту папку можно по следующему пути: **Панель управления | Центр управления сетями и общим доступом | Управление сетевыми подключениями**.

2. В меню **Файл** выберите команду **Новое входящее подключение**.

#### **ПРИМЕЧАНИЕ**

Если меню **Файл** не отображается, нажмите клавишу <Alt>.

Запустится мастер создания нового входящего подключения.

3. В окне **Разрешить подключения к этому компьютеру** (рис. 4.2) выберите пользователя, которому будет разрешен доступ к компьютеру.
4. В окне **Разрешить подключения к этому компьютеру** (выбор способа подключения) (рис. 4.3) выберите модем для входящего подключения.
5. В окне **Разрешить подключения к этому компьютеру — Программы для работы с сетью...** (рис. 4.4) укажите необходимые программы и протоколы.

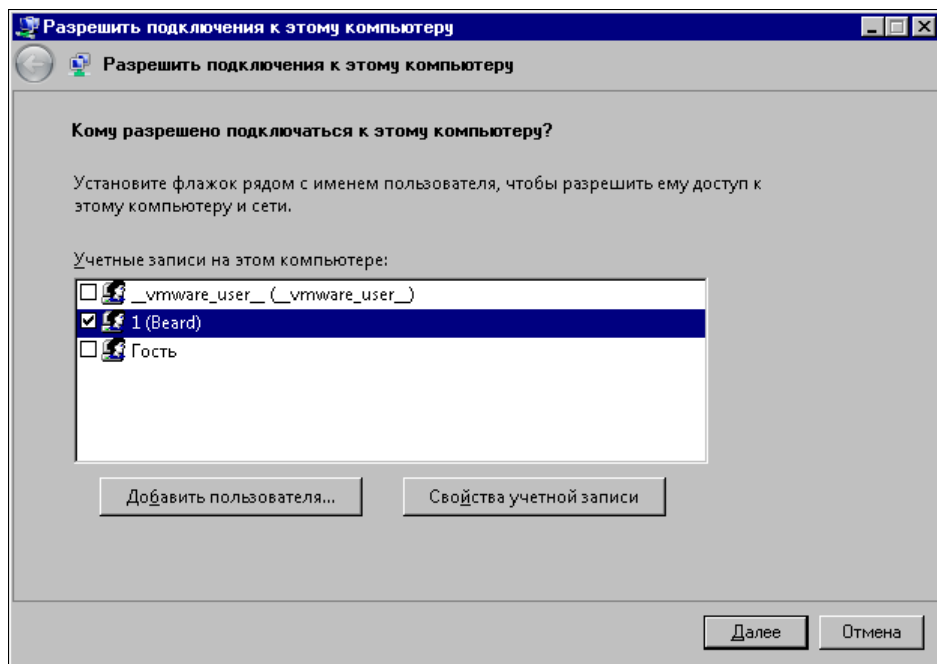


Рис. 4.2. Окно Разрешить подключения к этому компьютеру (выбор пользователя)

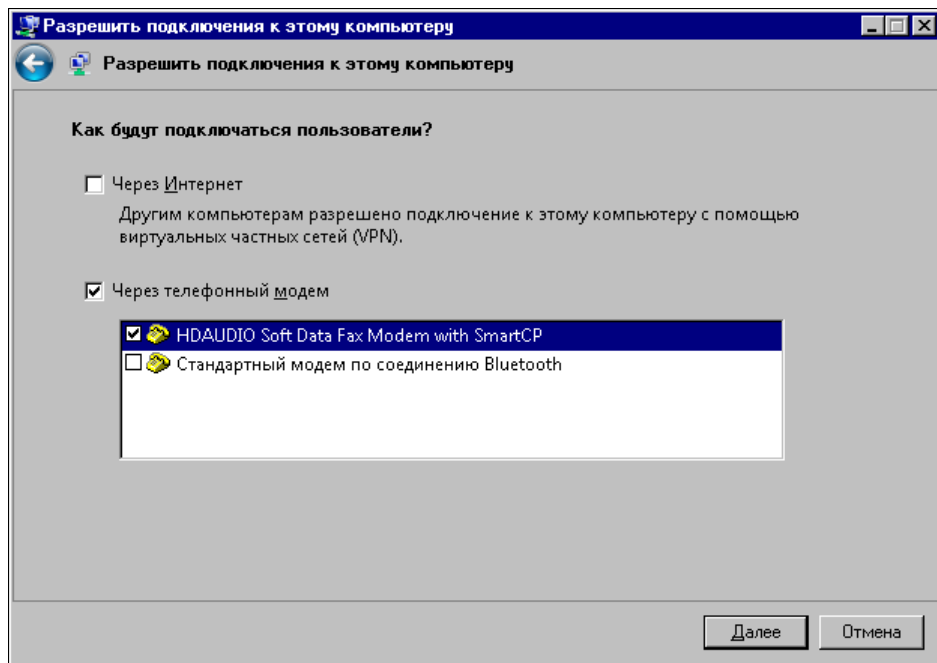


Рис. 4.3. Окно Разрешить подключения к этому компьютеру (выбор способа подключения)

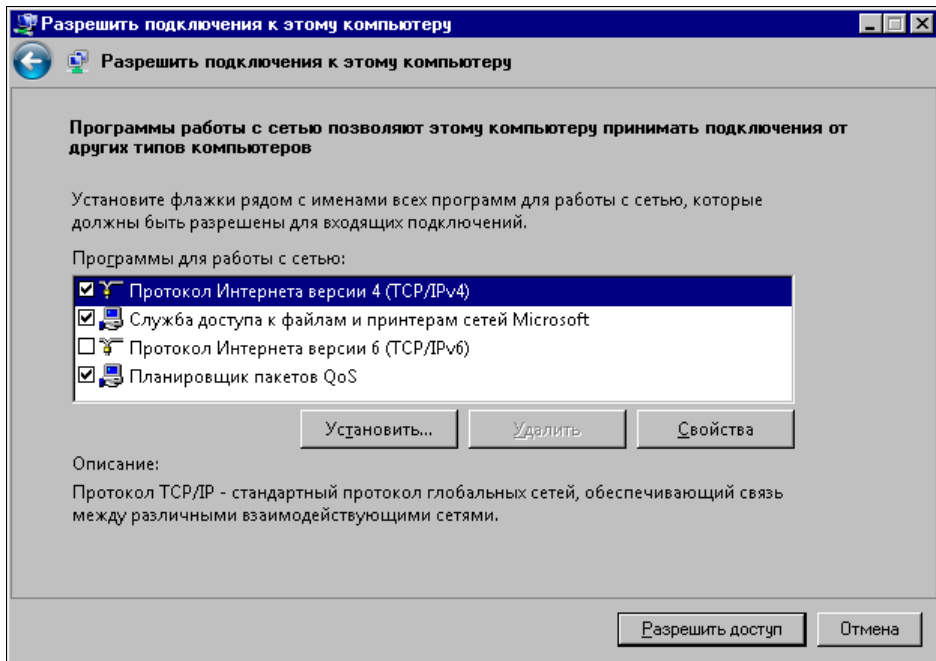


Рис. 4.4. Окно Разрешить подключения к этому компьютеру (выбор программ и протоколов)

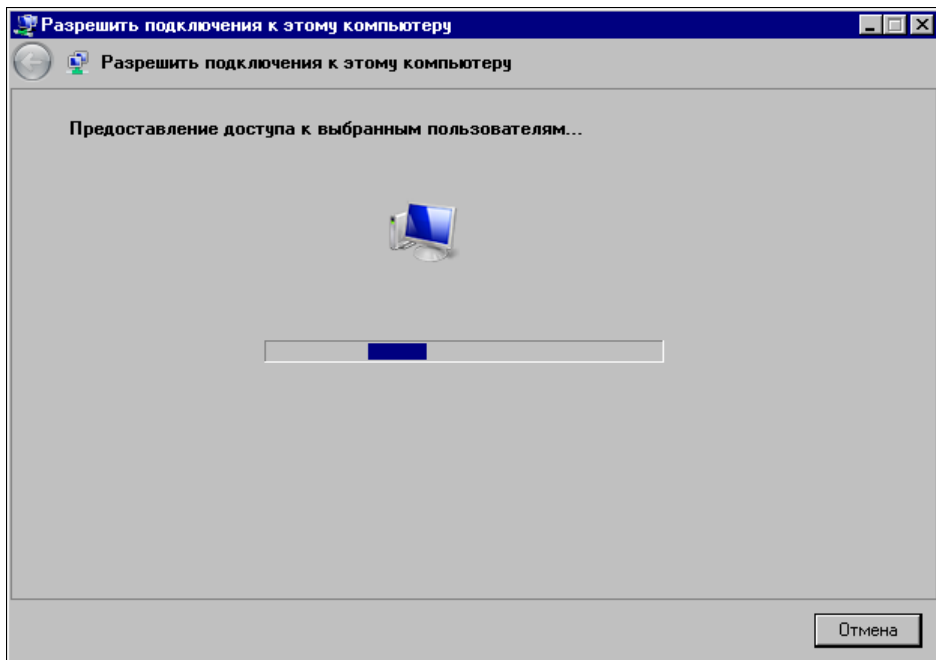


Рис. 4.5. Окно Разрешить подключения к этому компьютеру (предоставление доступа)





Рис. 4.6. Окно Разрешить подключения к этому компьютеру (завершение)

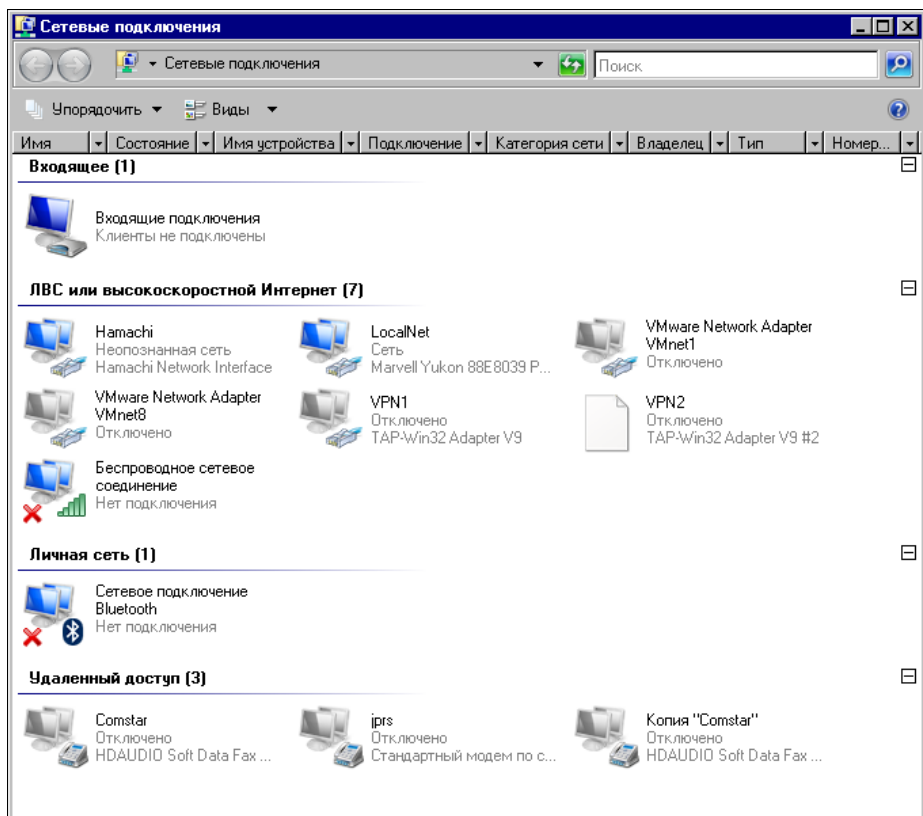


Рис. 4.7. Окно Сетевые подключения (новое входящее подключение)

6. В окне **Разрешить подключения к этому компьютеру — Предоставление доступа...** (рис. 4.5) ничего не надо делать. Мастер создает подключение.
7. В окне **Разрешить подключения к этому компьютеру — Выбранные пользователи теперь могут...** (рис. 4.6) можно распечатать или запомнить информацию, необходимую для подключения с другого компьютера.

Итак, подключение создано.

По завершении работы мастера вы увидите окно **Сетевые подключения** с новым разделом **Входящие** и с новым входящим подключением (рис. 4.7).

Теперь можно подключить модем компьютера к телефонной сети, и он будет готов к приему входящих подключений.

## Связь двух компьютеров через модем в Windows XP

Описанное в статье решение применимо, когда вы не имеете возможности решить задачу иным путем. У вас есть только два компьютера, два модема и телефонная линия. Несмотря на лаконичность поставленной задачи, возможны три варианта этого условия.

### **ВАРИАНТЫ ЗАДАЧИ**

1. Есть только два компьютера, два модема и телефонная линия.
2. Один из компьютеров подключен к локальной сети.
3. Один из компьютеров подключен к Интернету.

Естественно, что в каждом варианте задачи просматриваются три варианта результатов решения этой задачи.

1. Получаем доступ каждого компьютера друг к другу.
2. Получаем доступ в удаленную локальную сеть.
3. Получаем доступ в Интернет через удаленный компьютер.

Таким образом, вы можете поставить перед собой одну из трех целей (или все три сразу!) и достичь поставленной цели, решив описываемую задачу.

## Подготовка к соединению

Один из компьютеров, тот, к которому будем подключаться, назовем сервером, второй, с которого будем подключаться, — клиентом. Оба компьютера подключены к телефонной линии через модемы. Для установки связи между компьютерами необходимо, чтобы клиент позвонил на номер компьютера-сервера, а модем сервера в свою очередь "поднял трубку" и проверил логин и пароль звонящего пользователя. Если выполнение всех ранее перечисленных операций прошло без ошибок, то соединение состоится. А если нет, то вы где-то допустили ошибку.

## Настройка сервера

Компьютер-сервер, как мы уже выяснили, должен "ответить" на звонок клиента, для этого его нужно правильно настроить. Как это делается? А очень просто!

По следующей инструкции.

1. Если у вас меню **Пуск** в стиле Windows XP, то выполните следующие действия: нажмите кнопку **Пуск | Панель управления | Сетевые подключения | Создание нового подключения**.

Если меню **Пуск** в классическом стиле, то нажмите **Пуск | Настройка | Панель управления | Сетевые подключения | Создание нового подключения**.

После выполнения указанных действий запустится **Мастер новых подключений**, нажмите кнопку **Далее**.

2. Выберите **Установить прямое подключение к другому компьютеру** и нажмите кнопку **Далее**.
3. Выберите **Принимать входящие подключения** и нажмите кнопку **Далее**.
4. Выберите ваш модем и нажмите кнопку **Далее**.
5. Отметьте **Разрешить виртуальные частные подключения** и нажмите кнопку **Далее**.
6. В следующем окне **Выбор пользователя** у вас есть несколько вариантов продолжения настройки, рассмотрим их все по порядку.

- Можно выбрать из предлагаемого списка пользователей уже существующую учетную запись. Этот вариант приемлем, если на компьютере-сервере несколько учетных записей и клиент знает к одной из них логин и пароль. Такое бывает в тех случаях, когда клиент, к примеру, подключается из дома к своему рабочему месту.
- Можно заранее создать пользователя для подключения (см. дополнение "Создание новой учетной записи"). Этот вариант подходит, если подключения будут производиться часто и клиент хочет иметь на компьютере-сервере какие-либо права и собственные файлы.
- Можно создать нового пользователя здесь же. Для этого нажмите кнопку **Добавить** и заполните форму.
- И последний вариант — это выбрать учетную запись гостя. Этот вариант подходит тем, кто просто хочет поиграть с другом и ни на что более не претендует.

В свойствах учетной записи пользователя можно выбрать для него пароль или оставить его пустым (что и делается по умолчанию).

7. После того как вы определились с подходящим для вас вариантом, нажмите кнопку **Далее**.

## Выбор программ для работы с сетью

1. В свойствах компонента **Протокол Интернета (TCP/IP)** заранее установите IP-адреса для каждого компьютера.

По умолчанию IP-адрес выделяется автоматически, т. е. каждый раз при новом подключении он может меняться. Но если выбрать параметр **Указывать адреса TCP/IP явным образом**, то эта проблема исчезнет.

- Итак, отмечаем ранее указанный параметр и в поле **С**: пишем что-то вроде 125.125.125.125, а в поле **По**: 125.125.125.126. В итоге получаем два IP-адреса. Теперь IP-адрес сервера всегда будет 125.125.125.125, а IP-адрес клиента — 125.125.125.126.

Вы можете назначить серверу и клиенту и другие IP-адреса по своему выбору.

- Нажмите кнопку **Далее**.

А дальше-то и некуда. Все готово! Вот мы и настроили сервер. Теперь он готов принять звонок от клиента.

## Настройка клиента (вариант 1)

Компьютер-клиент должен дозвониться до сервера и пройти проверку имени и пароля, но для этого нужно правильно настроить сетевое подключение.

- Итак, делаем все то же самое, что и при настройке сервера на прием звонка, но только до запуска **Мастера новых подключений**.
- После запуска Мастера нажмите кнопку **Далее**.
- Есть два варианта продолжения настройки. Выбираем **Подключить к Интернету** и нажимаем кнопку **Далее**.
- Выбираем **Установить подключение в ручную** и нажимаем кнопку **Далее**.
- Выбираем **Через обычный модем** и нажимаем кнопку **Далее**.
- В поле **Имя поставщика услуг** вписываем любое имя (чтобы запомнить) и нажимаем кнопку **Далее**.
- В поле **Номер телефона** указываем тот, к которому подключен модем компьютера-сервера. Нажимаем кнопку **Далее**.
- Теперь заполняем форму, вводим имя пользователя и пароль, которые мы указали в настройках сервера.

Вот и все! Настройка подключения по первому варианту завершена!

## Настройка клиента (вариант 2)

Второй вариант не очень отличается от первого, но мы его все же рассмотрим. Описание начинаем с того места, где вы запустили **Мастер новых подключений**.

- Нажмите кнопку **Далее**.
- Теперь выбираем **Подключить к сети на рабочем месте** и нажимаем кнопку **Далее**.
- Выбираем **Подключение удаленного доступа** и нажимаем кнопку **Далее**.
- В поле **Организация** выбираем любое, понравившееся вам название. Затем нажимаем кнопку **Далее**.
- Номер телефона указываем тот, к которому подключен модем компьютера-сервера. Нажимаем кнопку **Далее**.

Готово!

### ЗАМЕЧАНИЕ

Обратите внимание на то, что имя и пароль пользователя мы не указывали. Их необходимо указать непосредственно перед звонком.

## Дополнение

Для подключения к удаленному компьютеру необходимо ввести имя и пароль пользователя. Это имя и пароль учетной записи на удаленном компьютере (сервере) или в сети, в которую входит удаленный компьютер.

Само собой, что такая учетная запись должна быть создана до первой попытки подключения.

Для создания учетной записи входим в **Панель инструментов | Учетные записи пользователей | Создание учетной записи** и вводим имя новой учетной записи (оно же и имя нового пользователя). Тип учетной записи напрямую зависит от ее назначения. Учетная запись с правами администратора предназначена для опытных пользователей и, само собой, администраторов компьютера. Пользователь с правами администратора может выполнять любые действия на компьютере. Обычный пользователь с учетной записью, имеющей ограниченные права, может изменять непосредственно свою учетную запись и окружающую его обстановку, но он не может повлиять на систему в целом.

Теперь следует разрешить новому пользователю вход через входящие подключения, или включить его в уже созданное (в свойствах подключения).

## Возможные неполадки

Если модем компьютера-сервера не отвечает на звонок клиента, то скорее всего причину стоит искать в настройках модема и еще стоит попробовать отключить из линии все телефоны.

Если модем клиента, начиная дозвон, "поднимает трубку" и не набирает номер, то стоит попробовать, в настройках модема, отключить опцию **Дождаться сигнала "линия свободна"**.

Бывает, что при подключении к серверу не удастся пройти регистрацию. Сервер не узнает пользователя или пароль. В этом случае можно создать на нем подключение аналогичное клиентскому и запустить **Мастер настройки домашний сети или сети малого офиса**, тот же мастер нужно запустить на компьютере-клиенте.

Ссылка: <http://www.oszone.net/3329/>.

## Соединяем компьютеры под управлением Windows 98

Не секрет, что до настоящего времени еще есть пользователи ПК, которые имеют компьютеры под управлением Windows 98. Многого, что могут новые операционные системы, эта ОС не умеет. Тем не менее она существует. Почему бы не использовать такие компьютеры для удаленного подключения? Простые сетевые за-

дачи, такие как передача файлов, например, вполне могут быть решены с помощью старых машин.

По ссылке <http://www.okobox.narod.ru/st1.htm> можно посмотреть статью "Компьютер — телефон — компьютер". В ней и описываются настройки, которые необходимо выполнить, чтобы компьютеры под управлением Windows 98 могли подключаться удаленно.

## Компьютер — телефон — компьютер

Здесь эта статья изложена в сокращенном виде.

Начинается статья с небольшого предисловия, в котором обозначается путь решения проблемы, с которой с большой вероятностью могут столкнуться пользователи, реализующие удаленное подключение. Проблема связана с тем, что при включении компьютера под управлением Windows 98 в локальную сеть подключение к нему может не получиться из-за необходимости вводить параметры учетной записи, подключающегося пользователя в необычном формате. Формат этот описан в справке по Windows 98, но описание так глубоко спрятано, что не каждому удается его найти.

### Небольшое предисловие

Если машина, к которой подключаемся, включена в сеть, то у нее может быть два входных пароля — один для входа в Windows или в сеть, а другой для доступа к ресурсам компьютера.

#### **ПРИМЕЧАНИЕ**

В новых операционных системах формат данных учетной записи не меняется в этих случаях.

Обычно при подключении требуется ввести *Имя\_пользователя* и *Пароль\_для\_входа\_в\_windows\_или\_в\_сеть*, но иногда компьютер-сервер требует указать домен, которого реально может и не быть. При этом авторизоваться можно, введя данные в следующем виде:

```
MSN/<имя_пользователя>  
Пароль_для_доступа_к_ресурсам
```

При этом поле для имени домена остается пустым.

Теперь, зная о "подводном камне", который может встретиться при реализации удаленного подключения, можно производить его настройку.

### Компьютер — машина универсальная

Имея телефонную линию и два модема, можно реализовать одну из важных функций персонального компьютера — связь с другими компьютерами.

С какой целью устанавливается такая связь?

Во-первых, просто для человеческого общения, т. е. для передачи текста, графики, речи удаленному абоненту и получения от него ответа. А также для передачи какой-либо телеметрической информации.

Во-вторых, для использования информационных ресурсов второго удаленного компьютера, пересылки файлов.

В-третьих, для доступа к программному обеспечению удаленной машины, удаленного администрирования.

И, в-четвертых, для использования вычислительной мощности двух удаленных машин (причем, как при работе в одиночку, так и при совместной работе двух операторов).

Как же установить такую связь? Сразу следует оговориться, что хакерские приемы такой связи мы рассматривать не будем, тем более что связь без выхода на просторы Интернета и даже без выхода в какую-либо компьютерную сеть существенно осложняет хакерское проникновение к вашей информации и вашему компьютеру.

Самым простым из доступных в Windows средств связи является программа HyperTerminal. Эта программа имеет собственные средства управления модемом и не требует ничего, кроме наличия модема и телефонной линии.

Если у вас нет этой программы, достаточно запустить установку Windows и в группе компонентов **Связь** выбрать **HyperTerminal**. Если программа установки попросит вставить диск с дистрибутивом Windows, вставьте его и HyperTerminal будет установлен.

С помощью HyperTerminal вы можете набрать номер телефона, и если на другом конце провода компьютер с модемом подключен к телефонной линии, а HyperTerminal находится в режиме ожидания, вы можете передать какие-либо файлы, перейдя в режим ожидания, получить файлы, если их передадут вам. Зная команды управления модемом, можно организовать текстовый диалог.

Есть и другие программы, обладающие более удобным интерфейсом и более широкими возможностями. Но в большинстве случаев эти программы, в отличие от HyperTerminal, требуют предварительно установленного подключения. Но и без применения дополнительного программного обеспечения установленное удаленное подключение двух компьютеров позволяет обмениваться файлами и выполнять другие сетевые задачи.

## Настройки

Итак, рассмотрим, как же настроить наш компьютер для организации удаленного подключения. Мы будем говорить об одном компьютере, предполагая, что он применяется и в качестве сервера, и в качестве клиента. Таким образом, выполнив все настройки на двух компьютерах, вы сможете использовать любой из них как в качестве сервера, так и в качестве клиента.

Прежде всего нужно через апплет **Установка и удаление программ** проверить наличие всех необходимых компонентов Windows в группе программ **Связь**.

Если в этой группе не установлены **Сервер удаленного доступа**, **Телефон** и **Удаленный доступ к сети**, то их необходимо установить с дистрибутивного диска Windows 98. После установки компонентов потребуется перезагрузка Windows. Так же можно установить HyperTerminal и NetMeeting, если вы предполагаете их использовать.

Затем в **Панели управления** дважды щелкните на значке **Сеть**. Необходимо установить, если еще не установлены **Клиент для сетей Microsoft**, протокол **NetBEUI**, протокол **TCP/IP**, **Служба удаленного доступа**. Для этого, нажимая кнопку **Добавить** и выбирая из списка производителей — **Microsoft**, выбираем необходимого клиента, протокол или службу. В свойствах **Клиента для сетей Microsoft** установите **Быстрый вход в сеть**. Остальные параметры можно оставить по умолчанию. Нажав кнопку **Доступ к файлам и принтерам** разрешите доступ к файлам и принтерам, выбрав соответствующие опции. На вкладке **Управление доступом** установите значение **На уровне ресурсов**. Посмотрите на вкладку **Идентификация** и запомните имя компьютера.

Теперь, войдя в **Мой компьютер**, откройте **Удаленный доступ к сети**.

В меню **Соединения** этого окна обратите внимание на пункт **Сервер удаленного доступа** (если вы не обнаружили этот пункт меню, прочтите статью сначала). Открыв этот пункт, вы можете разрешить или запретить удаленные подключения к вашему компьютеру. Разрешив удаленное подключение, придумайте и введите пароль для него. Запишите его и не потеряйте! Если модем у вас постоянно подключен к телефонной сети и нет возможности отключить питание модема (для встроенных модемов), то пока не разрешайте удаленные подключения, т. к. компьютер будет ожидать звонка, и на все входящие звонки будет отвечать. Если это обычный звонок, то звонящий услышит неприятный свист в телефонной трубке и положит ее, не дождавшись вашего ответа. Позже мы рассмотрим, как избежать такого неудобства. Теперь необходимо создать новое соединение. Задайте имя нового соединения и укажите для него номер телефона.

Затем на вкладке **Тип сервера** отметьте **Войти в сеть, NetBEUI, TCP/IP**, все остальные вкладки снимите.

Обеспечьте доступ к дискам вашего компьютера. Для этого, щелкнув правой кнопкой на иконке требуемого диска в папке **Мой компьютер**, выбираем пункт **Доступ** и отмечаем **Общий ресурс**, заполняем поле для сетевого имени, придумаем его. Тип доступа отметим — **Полный**, придумаем и введем пароль для доступа к диску. После этого изображение диска в папке **Мой компьютер** изменится, приобретя "поддерживающую руку".

Все настройки необходимо повторить на втором компьютере, с которым вы собираетесь соединиться. Только соединение должно создаваться другое, соответствующее номеру телефона для первого компьютера. Теперь, открыв **Мой компьютер** на втором компьютере, откройте **Удаленный доступ к сети**. Выбрав из меню **Соединения** пункт **Сервер удаленного доступа**, разрешите удаленные подключения к компьютеру. Разрешив удаленное подключение, вы исключите возможность звонить по телефону голосом по номеру, к которому подключен удаленный компьютер.

Если телефон все же нужен, можно заставить компьютер включать разрешение на удаленные подключения по расписанию, скачав программку *ServerOK* по адресу <http://serverok.newmail.ru> и заставив встроенный в Windows планировщик задач включать разрешение на доступ в заранее заданное время. Рекомендации по настройке программы *ServerOK* есть на посвященном ей сайте.



## Пришла пора подключаться

Подключив модем к телефонной линии и включив его питание, открываем уже созданное соединение и даем команду **Подключиться**, нажав соответствующую кнопку. Предварительно можно ввести пароль для подключения к удаленному компьютеру или ввести его по требованию компьютера позже. Когда соединение установится, щелчком правой кнопкой значок **Сетевое окружение**, что на рабочем столе, и выберем **Найти компьютер**. В появившемся окне через некоторое время появится значок компьютера, с которым установлена связь.

Далее с удаленным компьютером можно работать, как в обычной сети.

## Комментарии

Просматривая сообщения пользователей ПК в Интернете, можно встретить немало вопросов по поводу подключения к удаленному компьютеру через модем. Часть этих вопросов связана с тем, что никакая статья или сообщение на форуме не может вместить в себя все тонкости и нюансы, которые могут встретиться при реализации конкретного подключения.

## Микрофильтры и сплиттеры

К примеру, вы решили подключиться к удаленному компьютеру, который подключен к Интернету посредством ADSL-модема. Во многих городах России этот способ выхода в Интернет становится все доступнее.

В такой ситуации одна и та же телефонная линия применяется как для входящего подключения, так и для подключения к Интернету. Конечно, в самой операционной системе это два совершенно разных соединения...

Но и физически они должны быть разными. Вот здесь и возникает иногда ошибка. Куда подключать обычный модем?

Для подключения ADSL-модема необходимо, чтобы все другие устройства подключались к телефонной линии через *сплиттер* (*splitter*) или микрофильтр. Если ваш ADSL-модем стоит у вас на столе (или висит на стене рядом со столом), телефонная линия тоже подведена к столу, то, подключая обычный модем, легко упустить из виду необходимость установки сплиттера или микрофильтра. При этом что-нибудь обязательно работать не будет, скорее всего, — обычный модем.

### Надо помнить

Всегда помните, что ADSL-модем подключается к телефонной линии напрямую, все остальное должно быть соединено через сплиттер или микрофильтр.

## Шлюз для доступа в Интернет

Еще одна распространенная ошибка. Если у вас уже работает подключение к удаленному компьютеру, но не удастся использовать его подключение к Интернету, то проверьте, указан ли адрес удаленного компьютера в качестве основного шлюза для подключаемого компьютера?

### **Надо помнить**

Во всех случаях, когда подключение к Интернету происходит через промежуточное устройство, будь то маршрутизатор, специальный сервер или просто удаленный компьютер, необходимо указать в настройках подключения адрес этого устройства в качестве основного шлюза.

Если вы подключаетесь к другой сети, то тоже должен быть шлюз для перехода в эту сеть. IP-адрес шлюза всегда соответствует диапазону адресов вашей сети.

## **DNS**

Это тоже может привести к неработоспособности подключения, если цель была — выход в Интернет. Если на компьютере, который непосредственно подключен к Интернету, указаны адреса DNS-серверов, то это не значит, что подключаемый компьютер их тоже узнает.

### **Надо помнить**

Каждый компьютер должен самостоятельно обнаруживать IP-адреса по их символьным представлениям. Для этого он обязан самостоятельно обращаться к DNS-серверам, адреса которых вы можете ему подсказать.

Знаюки, конечно, могут сказать, что есть другой способ передачи адресов DNS-серверов компьютеру. Да, они правы. Но в этом случае в вашей сети должен работать DHCP-сервер, который знает адреса DNS-серверов и передает их рабочим станциям. Но в этом случае вам нужно подсказать адреса DNS-серверов DHCP-серверу. Но компьютеру, не включенному в сеть, неоткуда взять DHCP-сервер.

## **IP-адреса**

Выбирая IP-адреса для компьютеров, тоже следует принять во внимание некоторые ограничения. Если один из компьютеров имеет подключение к Интернету, то адреса для подключения компьютер-компьютер необходимо выбирать из диапазона, допустимого для локальных сетей. Удобно, например, применять адреса вида 192.168.X.Y с маской подсети 255.255.255.0, где X соответствует адресам сетей, а Y — адресам машин в этих сетях. Если сеть, в которую входит одна из подключаемых машин, имеет адреса 192.168.X1.Y, то адреса настраиваемых подключений должны быть 192.168.X2.Y. Таким образом, адреса подключений должны принадлежать другой подсети.

### **Надо помнить**

Каждый сетевой адаптер, установленный на компьютер, должен иметь самостоятельный IP-адрес, соответствующий самостоятельной подсети. Причем, под сетевым адаптером в данном случае понимается любое устройство для подключения к какой-либо сети. Это может быть и модем, и виртуальный сетевой адаптер.

Тема подключения к удаленному компьютеру достаточно популярна. Многие пользователи, проверив свой вариант подключения, часто делятся опытом с другими. Так, например, имеется ссылка <http://infocity.kiev.ua/os/content/os376.phtml> на

статью, в которой рассмотрен вариант подключения к компьютеру под управлением Windows 2000. Процедура настройки практически совпадает с процедурой для ОС Windows XP. Но все же нюансы могут быть. Кроме того, эта статья имеет продолжение, в котором рассматриваются варианты использования удаленного подключения.

## Соединяем компьютеры через Интернет

Вы спросите: зачем? Что ж, возможно, что у вас такой необходимости еще не возникало. Но многие администраторы сетей имеют возможность работать со своей сетью издалека. Зачем ехать для решения проблемы через многие километры, когда можно просто подключиться к сети через Интернет. Конечно, одно важное условие должно выполняться — и ваш компьютер, и сеть должны быть подключены к Интернету. Причем, желательно, чтобы сеть была всегда подключена к Интернету.

Но, возможно, вас заинтересует другой случай. Вы по ICQ или по E-mail договариваетесь о времени подключения и, имея обычные модемы, объединяете ваши компьютеры в маленькую локальную сеть, несмотря на расстояние, которое их разделяет.

### ПРИМЕЧАНИЕ

Обратите внимание, что разговор идет не об удаленном доступе к рабочему столу, а об объединении удаленных компьютеров в сеть.

Вообще говоря, вариантов для объединения компьютеров в сеть в Интернете много. Есть очень сложные способы, есть попроще, но совсем простых не существует. Нередко такую услугу предлагают провайдеры Интернета. Но нас интересует максимально простой способ.

Прежде всего, следует обратить внимание на то, что найти компьютер в Интернете может быть не просто. Большинство провайдеров выдают выходящим в Интернет машинам динамические IP-адреса, которые меняются при каждом новом подключении. Это затрудняет подключение к такому компьютеру. Но не делает невозможным. Помощь можно получить от имеющихся в Интернете сервисов, которые позволяют определить текущий IP-адрес компьютера и найти его по символическому имени. Один из самых удобных сервисов такого рода можно найти по адресу <http://dyndns.org>.

Более подробное описание сервиса приведено в *главе 22*.

Остается найти средство, позволяющее создать сетевое соединение через Интернет.

По собственному опыту могу утверждать, что в данном случае лучше всего подойдет пакет OpenVPN (<http://openvpn.net/index.php/downloads.html>).

К сожалению, мне не удалось найти в Интернете лаконичное описание настройки этой программы для двух компьютеров под управлением Windows. Создана была эта программа, как кроссплатформенная, и применяется по большей части в мире Linux. Тем не менее, ее с успехом можно применять и для Windows-систем. Приведу здесь собственное описание настройки сети из двух компьютеров, "протянутой" через Интернет. Описание построено на основе материалов с сайта проекта

OpenVPN и собственных экспериментов, которые завершились созданием постоянно действующего соединения двух компьютеров. Операционная система для обеих машин должна быть не ниже Windows 2000. Реально опробована работа сети, соответствующей описанию, на Windows XP и Windows Server 2003.

## OpenVPN

Серверная и клиентская части программы ничем не отличаются, кроме нескольких строчек в файле конфигурации программы. После установки программы на компьютере появляется виртуальный сетевой адаптер. Для нового адаптера автоматически создается и новое подключение, которое следует сразу переименовать в короткое и понятное имя, т. к. в файлах конфигурации программы OpenVPN нужно указать имя этого подключения. 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 4.1 и 4.2.

### Листинг 4.1. Local.ovpn — файл конфигурации для клиента OpenVPN

```
# имя компьютера, к которому осуществляем доступ
# приведен пример имени, созданного при использовании сервиса DynDNS
remote myserver.homeip.net
# порт, через который осуществляется связь (любой свободный)
port 35000
# указание на роль компьютера в VPN
proto tcp-client
dev tap
ifconfig 192.168.116.2 255.255.255.0
# имя подключения
dev-node vpn
secret key.txt
ping-restart 60
ping-timer-rem
persist-key
resolv-retry 86400
ping 10
comp-lzo
verb 4
mute 10
```

### Листинг 4.2. 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 192.168.116.2 255.255.255.0
```

Эта строка устанавливает IP-адрес для подключения `vpn` 192.168.116.2, 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 команду `ping` по адресу сервера, к которому делается попытка подключения. В локальном файле конфигурации указывается имя сервера (параметр `remote`). Связь имени и IP-адреса должна быть обеспечена любым из доступных способов.

OpenVPN-сервер, запущенный на сервере сети, ожидает попыток подключения извне. При удачной попытке сетевое VPN-подключение (Virtual Private Network — виртуальная частная сеть) 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 с помощью пункта меню программы **Generate a static OpenVPN key** (Создать статический ключ) на одном из компьютеров и передан на другой любым доступным способом. Важно, чтобы на обеих машинах были копии одного и того же файла. 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. Признаком установившегося соединения 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. При установившейся связи в сетевом окружении удаленного компьютера появится сервер (если компьютеры имеют одинаковое имя рабочей группы или домена). Для входа на него требуется ввести имя пользователя и пароль учетной записи, имеющейся на сервере.

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) **Запрос 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.

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.

Защищенный канал связи, создаваемый в Интернете, работает через порт, который мы зададим в файлах конфигурации OpenVPN, этот порт должен быть открыт. В примере показано применение порта 35000, но можно выбрать любое значение, неиспользуемое на вашем сервере. Если есть сомнения в том, что выбранный вами порт открыт на каком-либо участке предполагаемого канала, его можно изменить.

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.

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 VPN-соединения откройте сетевое окружение на рабочей станции. Вы должны увидеть компьютер, к которому производилось подключение.

Если вместо сообщения Initialization Sequence Completed на экране будет появляться Initialization Sequence Completed with Errors, то работа с сетевыми ресурсами может быть затруднена или невозможна. В этом случае следует проверить качество соединения и правильность настроек.

Если вам удалось настроить OpenVPN и получить доступ к удаленному компьютеру, то при желании вы можете запустить службу OpenVPN, которая появилась в перечне служб операционной системы после установки программы. Теперь связь будет устанавливаться автоматически при каждом совместном выходе в Интернет обоих компьютеров.

Число подключений, созданных с помощью OpenVPN, может быть практически любым. Потребуется только создать необходимое число виртуальных сетевых адаптеров, а затем запускать соответствующее количество экземпляров программы.

Один экземпляр программы может обслужить одну пару компьютеров.

## Hamachi

Программу Hamachi можно найти по адресу <https://secure.logmein.com/products/hamachi/vpn.asp>. От OpenVPN она отличается тем, что может работать через маршрутизаторы и сетевые экраны без их дополнительных настроек.

После регистрации на сайте вы сможете, загрузив и установив программу, создать собственную виртуальную сеть. Эта программа для создания соединения между компьютерами использует специальный сервер в Интернете. Сервер позволяет создавать прямой туннель между компьютерами, а при невозможности создания такого туннеля проложить его путь через сервер. Практически подключения с помощью этой программы возможны вне зависимости от способа подключения к Интернету. Программа существует как в коммерческой версии, так и в бесплатном варианте, возможностей которого вполне достаточно для небольшого числа объединяемых компьютеров.

*LogMeIn Hamachi* — это служба VPN, которая без труда настраивается за 10 минут и обеспечивает безопасный удаленный доступ к вашей сети отовсюду, где можно подключиться к Интернету. Служба взаимодействует с существующим брандмауэром и не требует дополнительной настройки. Hamachi — это первое приложение, успешно объединяющее несвязанные сетевые технологии в один мощный пакет, обеспечивающий прямую связь между одноранговыми узлами.

После установки программы можно создать новую сеть, которая не совсем похожа на настоящую локальную. Отличие в том, что IP-адреса компьютеров в этой сети самостоятельные, не связанные маской подсети. Такая сеть это, скорее, видимая через интерфейс программы (рис. 4.8) группа компьютеров, объединенная общими учетными данными. Тем не менее, все необходимые для локальной сети качества имеются.

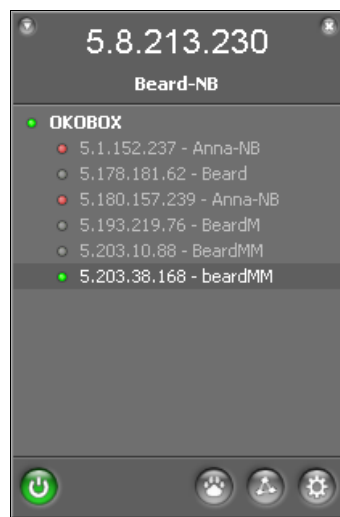


Рис. 4.8. Окно программы Hamachi

Программа может быть установлена в двух вариантах — в режиме оказания помощи клиентам сети, и в режиме подключения к своим компьютерам. Здесь описан второй вариант. Подключение клиентов сети производится с подключаемого компьютера через сайт программы. В бесплатном варианте можно создать до четырех сетей по шестнадцать клиентов в каждой. Активные в данный момент компьютеры отмечены зеленой точкой. В контекстном меню строки клиента в окне программы можно выбрать пункт **Просмотреть папки**. При этом откроется окно **Сеть** — *<IP-адрес>* (рис. 4.9), в котором будут показаны доступные по сети папки на удаленном компьютере. Все, как в обычной локальной сети.

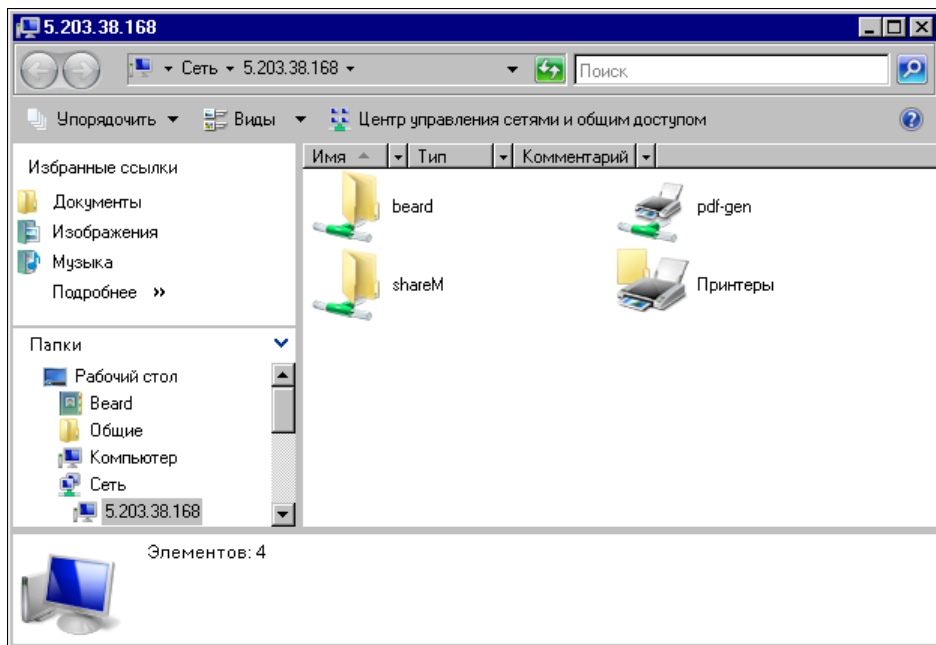


Рис. 4.9. Окно Сеть — 5.203.38.168

Если возникли проблемы с соединением, можно в контекстном меню выбрать пункт **Проверить доступность**. Откроется окно командной строки (рис. 4.10), в котором будет показан результат команды ping по адресу клиента.

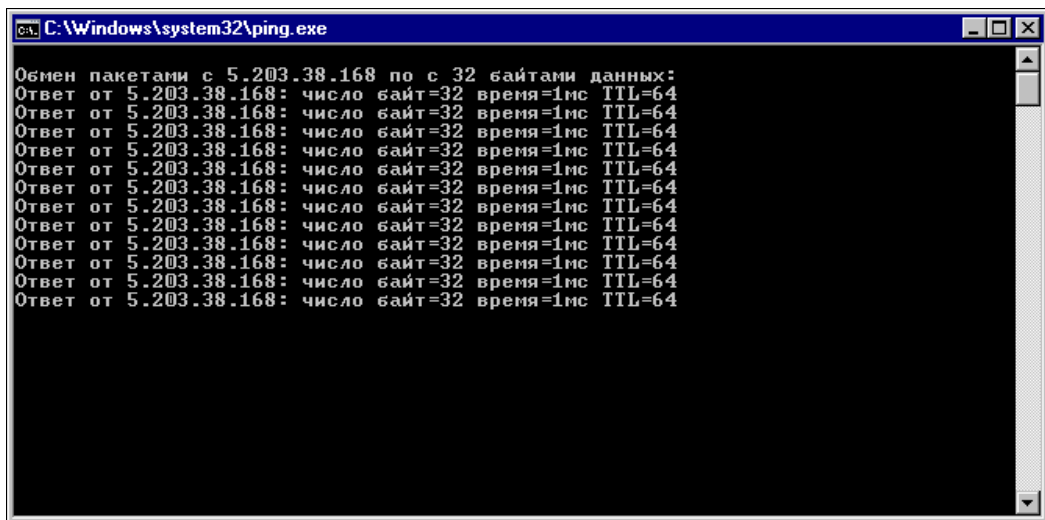


Рис. 4.10. Окно командной строки с результатами проверки 5.203.38.168

Команда выполняется до закрытия окна командной строки. По результатам выполнения команды ping можно решать проблему недоступности. Обычно, если



подключение к Интернету есть и на клиентской машине обеспечен доступ к ресурсам, все работает достаточно надежно.

На данный момент клиент Hamachi работает в Windows 2000, XP, 2003 и Vista. Существуют консольные версии Hamachi для Linux и OS X. На странице загрузки программы <https://secure.logmein.com/products/hamachi/vpn.asp> можно получить и версию для Linux (hamachi-0.9.9.9-linux). В примере, приведенном ранее, клиентский компьютер как раз под управлением этой ОС. Для Linux программа запускается в консольном режиме. После загрузки программы следует выполнить следующие команды:

1. `su`.
2. `<пароль пользователя root>` — работаем от имени администратора.
3. `make install` — из каталога с дистрибутивом программы.
4. `/sbin/funcfg` — создается виртуальный сетевой адаптер.
5. `Exit` — входим в режим обычного пользователя.
6. `hamachi-init` — (пишется без пробелов) генерируются ключи для идентификации в системе.
7. `hamachi start` — запускаем программу.
8. `hamachi login` — входим в систему (регистрация на сервере Hamachi).
9. `hamachi go-online <network>` — входим в сеть с именем созданной сети `<network>`.
10. `hamachi list` — просматриваем доступные в нашей сети машины.

Теперь можно подключаться к сетевым ресурсам других членов сети.

Для остановки программы существует команда `hamachi stop`. При повторном запуске регистрация на сервере произойдет автоматически. Выполнив команду `hamachi` без параметров, можно увидеть справку по работе с программой. Также в каталоге с дистрибутивом находится файл `Readmy`, в котором помещено описание работы с программой (на английском языке).

## NeoRouter

Программа NeoRouter появилась относительно недавно. 20 октября 2008 года прошла информация о выходе версии 0.92. Теперь на сайте <http://www.neorouter.com/> доступна версия 1.1.1. Программа позволяет очень быстро настроить виртуальную частную сеть (VPN) как между двумя удаленными компьютерами, так и создать виртуальную сеть, которая может содержать до 253 компьютеров. В бесплатной версии такая сеть может быть только одна, но в большинстве случаев это ограничение не существенно.

Единственное условие, которое необходимо выполнить для нормальной работы программы, — это установка ее серверной части на доступный из Интернета компьютер или маршрутизатор. Есть версия программы для Tomato, OpenWrt, Fonera — операционных систем для маршрутизаторов и точек доступа.

Для того чтобы компьютер был доступен из Интернета, он должен иметь реальный внешний IP-адрес. Если адрес выделяется провайдером динамически, то можно использовать сервис DynDNS и подключаться к компьютеру по символьному имени. Для всех остальных участников сети способ подключения к сети Интернет не имеет значения. Ни сетевые экраны, ни NAT (Network Address Translation — трансляция сетевых адресов) подключениям не мешают.

При объединении в виртуальную сеть всего двух компьютеров, на одном из них должна быть установлена как клиентская, так и серверная часть NeoRouter.

В описании программы, имеющемся на сайте, сказано, что необходима регистрация виртуального домена. На самом деле, если вы используете статический IP-адрес или динамический в сочетании с сервисом DynDNS на сервере NeoRouter, в регистрации нет необходимости.

Программа имеет версии под все популярные 32- и 64-битные операционные системы, такие как Windows, Linux (Debian, Ubuntu, Suse, Fedora, CentOS), Mac OS. Все данные, передаваемые через виртуальную сеть, шифруются через SSL.

Несмотря на необходимость наличия сервера NeoRouter, соединения между клиентами сети устанавливаются напрямую. Это значит, что скорость соединения между клиентами не зависит от скорости соединения сервера с сетью Интернет.

При установке NeoRouter устанавливает виртуальный адаптер, которому при подключении к виртуальной сети присваивается уникальный IP-адрес вида 10.0.0.\*.

Так же NeoRouter устанавливает собственные системные сервисы для клиентской и серверной части, которые после первого подключения к сети запоминают домен (или IP-адрес), логин и пароль. При последующем запуске системы уже не понадобится запускать клиентскую часть NeoRouter (NeoRouter Network Explorer) — сервисы установят подключение сами. При этом если сервер не запущен, то сервис просто будет с определенной периодичностью опрашивать сервер NeoRouter, пока не дожидается подключения. Если есть возможность установки более чем одного сервера, тогда клиент будет опрашивать их по очереди, пока не обнаружит действующий.

Не имеет значения, какие операционные системы используются на сервере и клиентах. Клиенты и серверы для разных ОС полностью совместимы.

## NeoRouter Configuration Explorer

Установка программы NeoRouter Configuration Explorer не представляет никакой сложности. Поэтому рассмотрим уже установленные компоненты программы и их настройки. Серверная часть программы — NeoRouter Configuration Explorer (рис. 4.11) обязательно настраивается один раз после установки. В дальнейшем вы можете "забыть" об этом компоненте программы. На вкладке **General** (см. рис. 4.11) отображены данные о программе, ее состоянии и параметры, которые вы зададите при установке или последующей настройке — IP-адрес или доменное имя, порт, который будут использовать клиенты для подключения. Номер порта лучше оставить по умолчанию. В этом случае клиентам не придется изменять его.

На вкладке **User Accounts** (рис. 4.12) вы можете добавлять и удалять пользователей, назначать им права администратора или обычного пользователя. Обычный

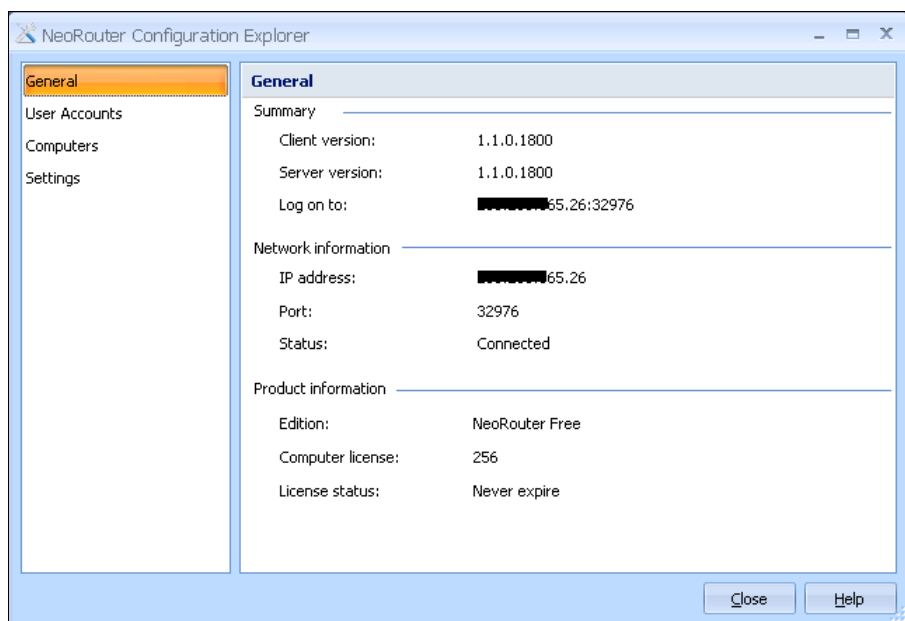


Рис. 4.11. Окно NeoRouter Configuration Explorer, вкладка General

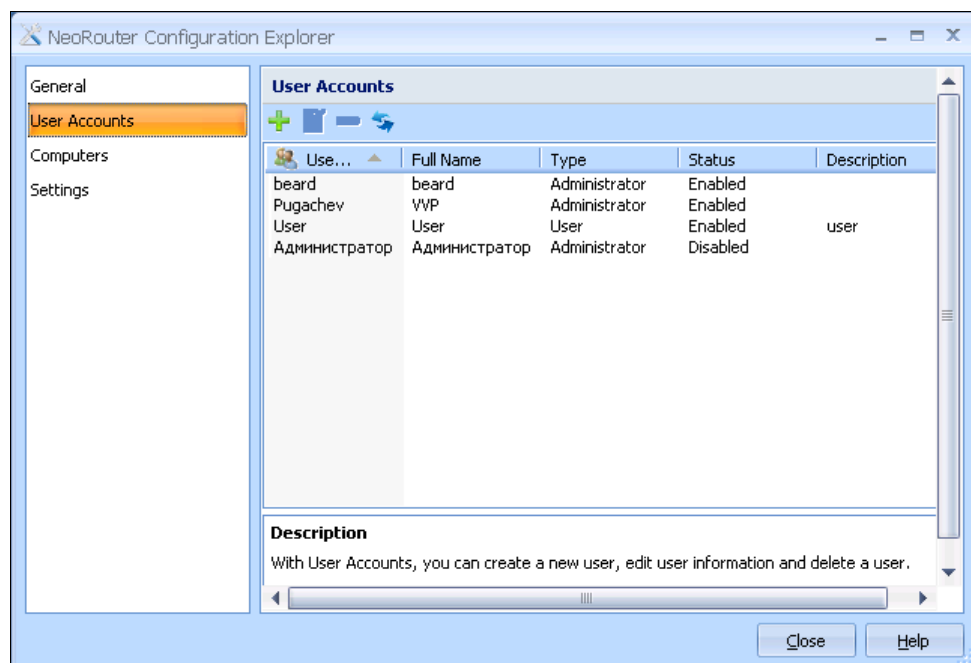


Рис. 4.12. Окно NeoRouter Configuration Explorer, вкладка User Accounts

пользователь не имеет возможности самостоятельно добавить свой компьютер в сеть или удалить другой. Администратор может увидеть еще не включенный в сеть, но подключившийся к серверу компьютер и ввести его в сеть. Эту операцию администратор может выполнить как из окна NeoRouter Configuration Explorer, так и из окна своей клиентской части программы.

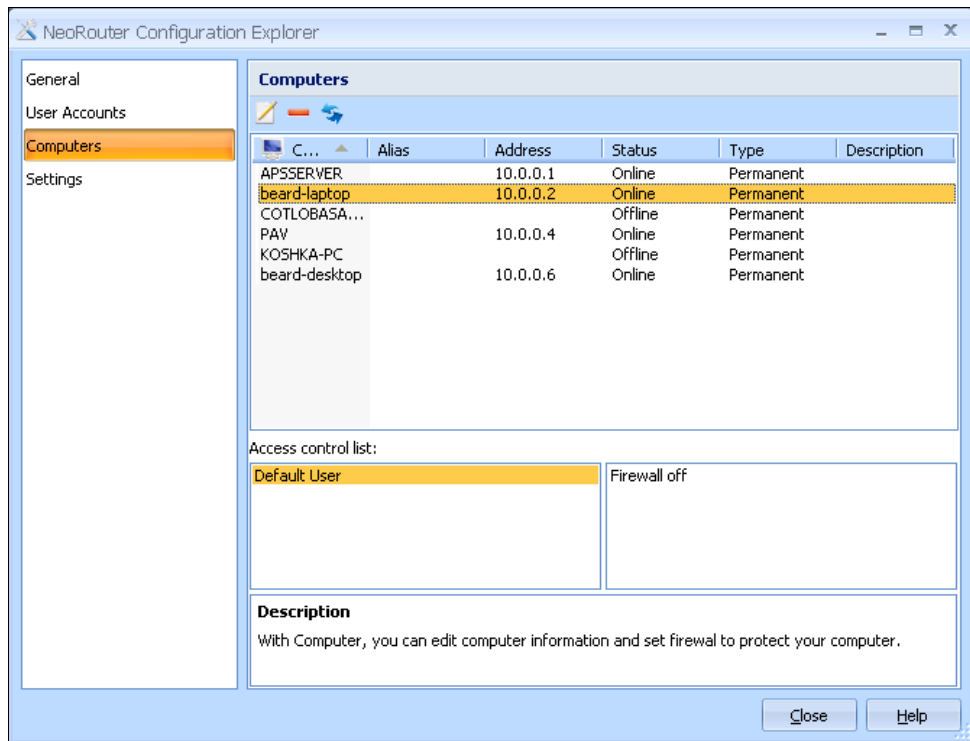


Рис. 4.13. Окно NeoRouter Configuration Explorer, вкладка Computers

На вкладке **Computers** (рис. 4.13) отображены подключенные и отключенные компьютеры виртуальной сети.

На вкладке **Settings** (рис. 4.14) можно указать имя домена виртуальной сети (поле **Current domain**). Если вы используете подключение по статическому адресу и не регистрируетесь на сайте <http://www.neorouter.com/>, то имя может быть любым. Здесь также можно поменять при необходимости номер порта, настроить DHCP-сервер виртуальной сети, изменить адрес и маску всей виртуальной сети. Для обычной работы можно не менять ничего.

Клиентская часть программы NeoRouter Network Explorer (рис. 4.15) отображает компьютеры сети. Если вы имеете права администратора, то посредством пункта меню **Computers** вы имеете возможность подключать к сети другие подключившиеся к серверу компьютеры.

При первом запуске программы NeoRouter Network Explorer спрашивает доменное имя сервера (можно ввести его IP-адрес), имя пользователя и пароль. Имя для

обычных пользователей можно использовать одно, например User, как в этом примере.

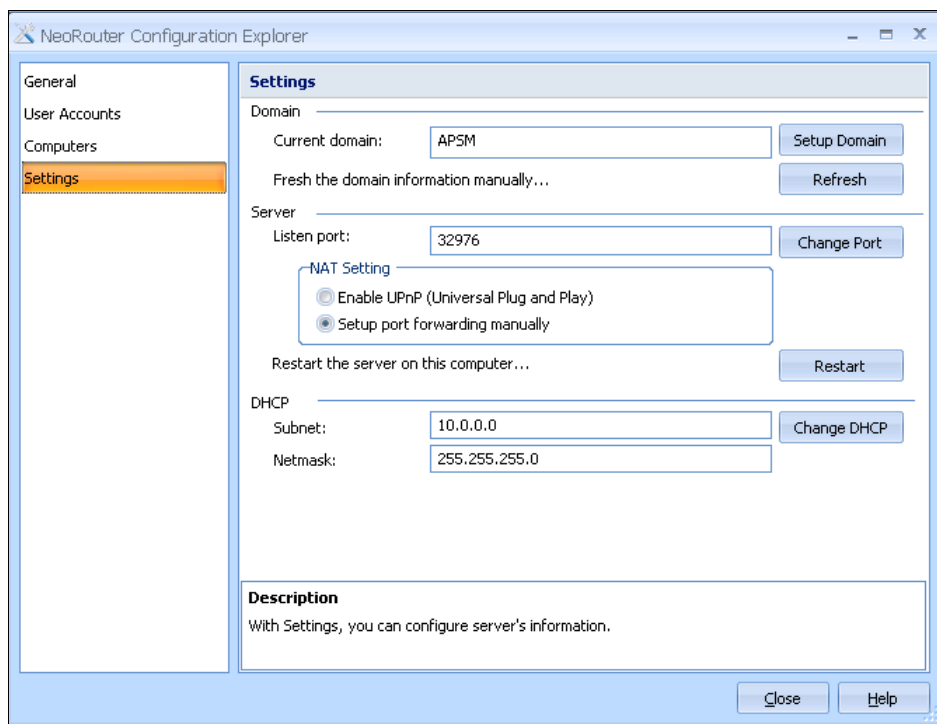


Рис. 4.14. Окно NeoRouter Configuration Explorer, вкладка Settings

На рис. 4.16 приведен вид окна терминала Linux с текстовым выводом NeoRouter Network Explorer для Linux. В качестве подсказки выведены команды, которые можно использовать. Первые две команды — `addcomputer` (добавить компьютер) и `deletecomputer` (удалить компьютер) — применяются чаще всего. Другие команды вам могут и не понадобиться совсем, но при желании можете почитать о них в документации, доступной на сайте, или поэкспериментировать с ними самостоятельно.

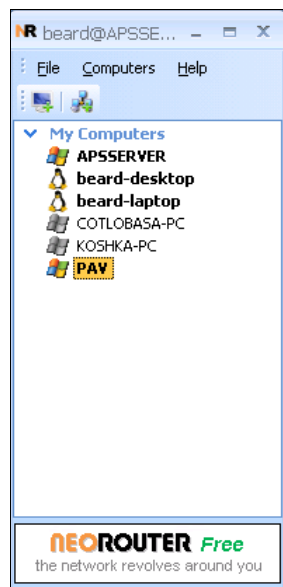
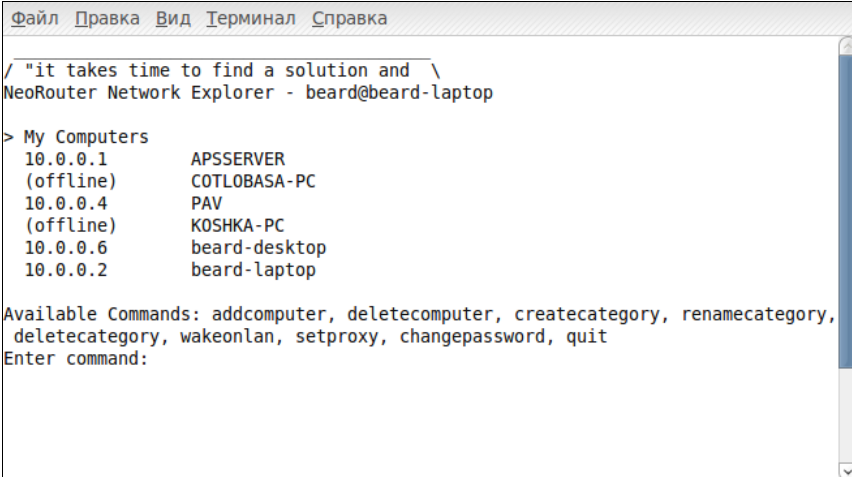


Рис. 4.15. Окно клиентской часть программы NeoRouter Network Explorer



```
Файл Правка Вид Терминал Справка
/ "it takes time to find a solution and \
NeoRouter Network Explorer - beard@beard-laptop

> My Computers
10.0.0.1      APSSERVER
(offline)   COTLOBASA-PC
10.0.0.4      PAV
(offline)   KOSHKA-PC
10.0.0.6     beard-desktop
10.0.0.2     beard-laptop

Available Commands: addcomputer, deletecomputer, createcategory, renamecategory,
deletecategory, wakeonlan, setproxy, changepassword, quit
Enter command:
```

Рис. 4.16. Окно программы NeoRouter Network Explorer для Linux

Чтобы опробовать программу, совсем не обязательно иметь подключение к Интернету. Для начала можно установить и серверную и клиентскую части на одном компьютере, ознакомиться на практике с возможностями настроек программы, а потом установить клиентскую часть на втором компьютере сети и подключиться с него к серверу. После удачного добавления второго компьютера в сеть вы получите зашифрованное подключение внутри локальной сети. Теперь вы можете закрыть все порты, кроме используемого программой, но получить доступ как к файловым ресурсам, так и к удаленному рабочему столу второго компьютера.

## ГЛАВА 5



# Маршрутизация

Локальная сеть с выходом в Интернет использует маршрутизацию для обеспечения подключения к Интернету всех или нескольких компьютеров сети. Нередко возникает задача предоставить доступ для компьютеров вашей сети к компьютерам другой сети. Это могут быть сети двух соседних квартир, домов или офисов. Решить такую задачу можно несколькими путями — рассмотрим наиболее распространенные из них.

## Сетевой мост

Сетевой мост — одно из самых простых для применения средств объединения сетей. В то же время есть некоторые особенности этой технологии, которые не позволяют начинающему пользователю получить положительный результат в целом ряде случаев. В Интернете и в справке Windows можно найти немало сведений о сетевом мосте, но подробно описанных примеров совсем не много. Видимо не часто есть условия для реализации этой технологии в практике обычных пользователей. Но когда такая ситуация возникает, сетевой мост настраивается достаточно просто и помогает решить задачу объединения сегментов сети. В отличие от других технологий, сетевой мост, не требуя специальных настроек сети, может передавать любые пакеты между сетями, позволяя всем включенным в мост сетям иметь общее подключение к Интернету. Наиболее дешевый и простой способ объединения сетей — программный сетевой мост. Возможность его создания встроена в современные операционные системы, такие как Windows XP, Windows Server 2003, Windows Vista и Windows 7. Данный пример выполнялся в среде Windows Server 2003. Важно и то, что сетевой мост позволяет объединить сети практически в неограниченном числе. Сколько сетевых адаптеров может быть подключено к компьютеру, столько подсетей можно и объединить. Причем, адаптеры эти могут быть как обычными сетевыми картами, так и Wireless-адаптерами, подключаемыми через USB-интерфейсы, и даже виртуальными. Правда, не все виртуальные адаптеры можно включать в сетевой мост. Так, мне не удалось подключить к мосту виртуальный адаптер виртуальной машины VMware. Может быть, что-то делалось не

так, но не получилось. Зато виртуальный адаптер клиента OpenVPN — средство для создания виртуальной сети — подключился без проблем.

На рис. 5.1 показаны условные обозначения, использованные при описании объединенных сетей, рассмотренных далее.

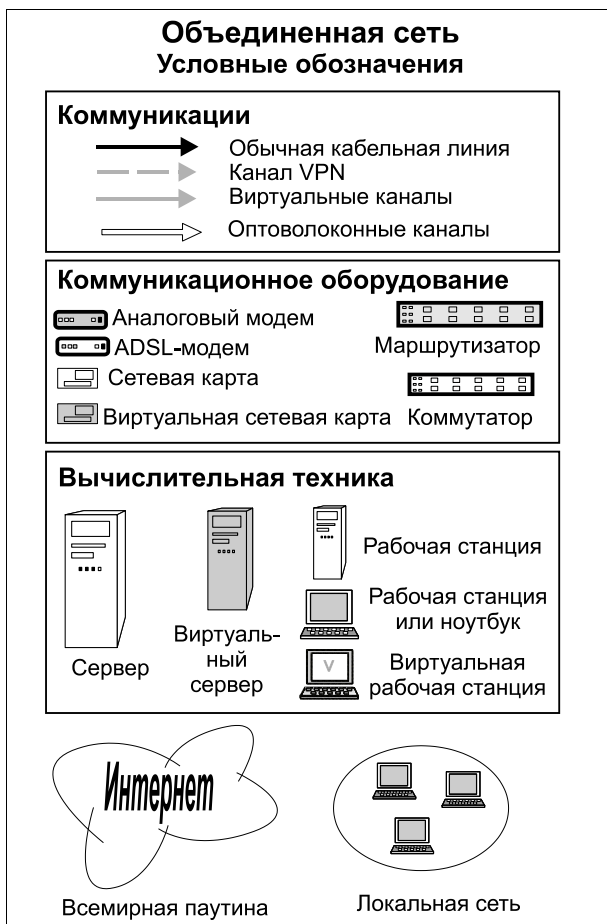


Рис. 5.1. Объединенная сеть (Условные обозначения)

На рис. 5.2 показана домашняя часть большой сети, представляющей собой объединение нескольких мелких и крупных сетей.

Объединенная сеть имеет масштабы крупного города, и частью этой большой сети является маленькая домашняя сеть, показанная на рисунке. В этой небольшой сети работают несколько пользователей, которые решают не только домашние, но и достаточно масштабные задачи. Для этого, кроме обычного подключения к локальной сети и к Интернету, им потребовалось подключение к сети организации (рис. 5.3). В этой сети находится сервер (на рисунке обозначен цифрой 3), через который осуществляется обмен файлами, и иногда проводится совместная работа над этими файлами. Сеть имеет свой контроллер домена (2), работают в ней не



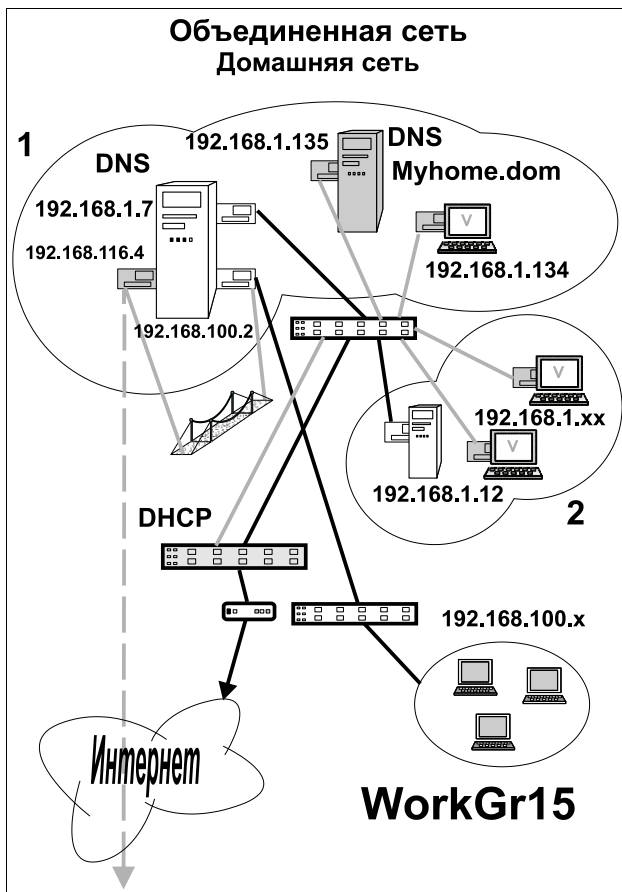


Рис. 5.2. Объединенная сеть (Домашняя сеть)

один десяток пользователей (1), имеет выход в Интернет. Домашняя сеть тоже имеет приличный выход в Интернет через ADSL-модем (Стрим<sup>1</sup>). Для организации канала между этими сетями, находящимися на расстоянии более сорока километров, было решено организовать VPN (виртуальную частную сеть). На сервере сети WorkGr15.dom (здесь и далее так будем называть сеть организации) был установлен сервер VPN, а в домашней сети (ее имя Myhome.dom) установили клиент VPN. Эти программы самостоятельно обнаруживают друг друга и с физического сервера (1) сети Myhome.dom можно в любой момент подключиться к серверу предприятия. Но только с сервера, который ради экономии средств и повышения защищенности от возможных воздействий со стороны пользователей не оборудован монитором и клавиатурой. Требовалось обеспечить возможность работы с этим сервером для группы пользователей WorkGr15. Имя этой группы в нашем описании не содержит суффикса ".dom". В отличие от пользователей WorkGr15.dom, компьютеры которых

<sup>1</sup> Стрим — это высокоскоростной домашний интернет-канал со свободным телефоном. Для его получения абонент должен приобрести контракт и комплект стрим-оборудования.

входят в домен, компьютеры WorkGr15 входят в рабочую группу с таким же именем. Это позволяет в сетевом окружении WorkGr15 видеть компьютеры WorkGr15.dom. Компьютеры WorkGr15 изначально имели адреса вида 192.168.100.X с маской 255.255.255.0, и были подключены через коммутатор к сетевому адаптеру физического сервера (1) с адресом 192.168.100.3. Клиент VPN имеет виртуальный сетевой адаптер с адресом 192.168.116.3. Причем для виртуальной сети была выбрана маска 255.255.255.248, которая позволяет использовать лишь шесть IP-адресов.

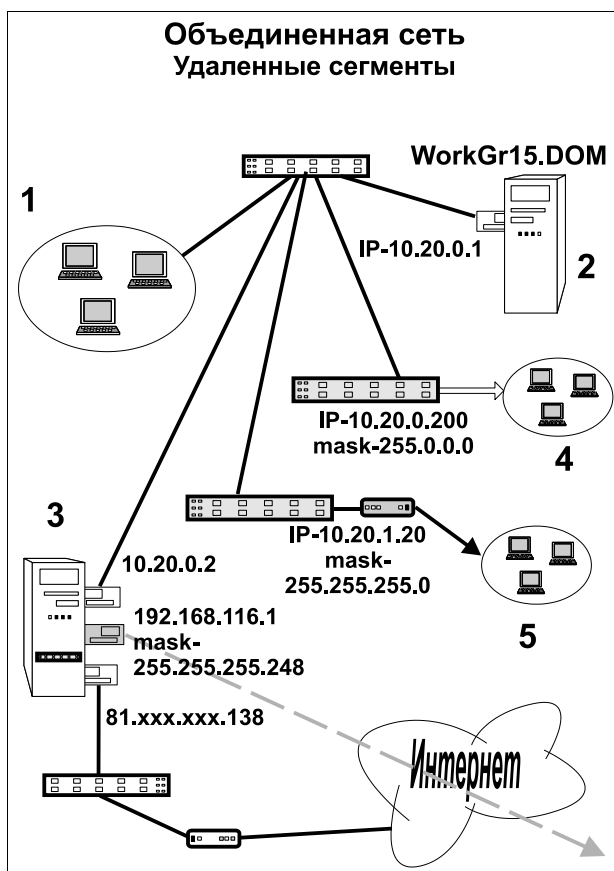


Рис. 5.3. Объединенная сеть (Удаленные сегменты)

Остается обеспечить возможность подключения группы WorkGr15 к виртуальной сети, в которой работает необходимый этой группе сервер. Вот эту задачу и решим с помощью организации моста, который на рисунке так и изображен, как маленький подвесной мост.

На рис. 5.4 показано окно сетевых подключений физического сервера сети Myhome.dom. Два подключения **Local Area Connection 2** и **vpndom** были выбраны мышью при нажатой клавише <Ctrl>, после чего из контекстного меню был выбран пункт **Настроить мост**. Собственно, в этом и состоит вся основная работа. Мост

создается автоматически, а значки выбранных подключений в окне **Сетевые подключения** помещаются вместе со значком сетевого моста в один раздел.

Если для сетевого моста нет доступного DHCP-сервера, как в данном случае, то через некоторое время система сама назначит ему IP-адрес, который использовать вы не сможете. Поэтому надо, дождавшись завершения автоматической процедуры присвоения IP-адреса, заменить его на правильный. В данном случае правильным будет адрес из числа разрешенных для нашей VPN-сети. Мы установили его равным 192.168.116.4.

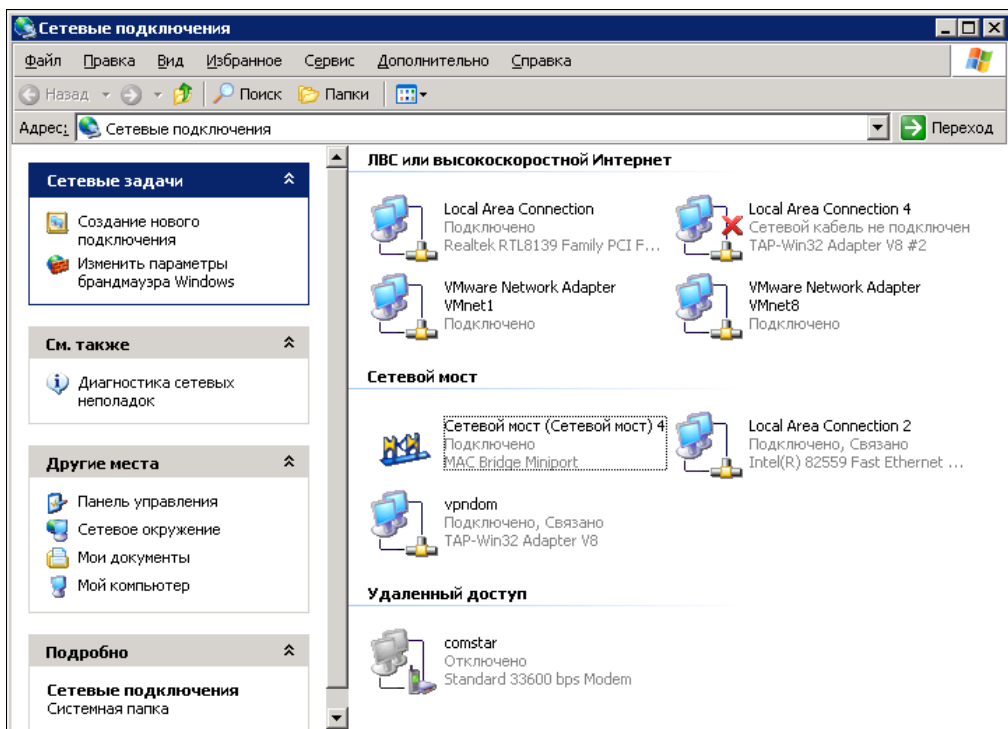


Рис. 5.4. Окно **Сетевые подключения** физического сервера сети Myhome.dom

Теперь параметры включенных в мост сетевых адаптеров увидеть и изменить нельзя. Но обращение к ним со стороны компьютеров сети, как и ранее, остается возможным. Адрес сетевого моста не должен совпадать с адресом любого включенного в него адаптера.

Если не возникло ошибок, все адаптеры остались в рабочем состоянии, и система не отключила их, пометив красным крестом, то можно переходить к рабочей станции из группы WorkGr15. На всякий случай только вспомним, что в сети VPN у нас доступно шесть IP-адресов. Один занят сервером VPN, другой сетевым адаптером клиента, третий присвоен сетевому мосту. Осталось три адреса, которые можно присвоить трем рабочим станциям из группы WorkGr15.

На рабочей станции ее сетевому адаптеру осталось добавить еще один адрес, например, 192.168.116.3. Теперь она может работать в сети 192.168.100.0 и в сети

192.168.116.0. Войдя в сетевое окружение на этой рабочей станции, мы увидим значки компьютеров сети WorkGr15.dom, которые находятся в группе WorkGr15. Кроме этой группы в сетевом окружении мы должны видеть и группу домашней сети Myhome. Но в ней будет доступен только сервер до тех пор, пока мы не включим в сетевой мост на сервере еще один сетевой адаптер **Local Area Connection**. Но в данном конкретном случае такой необходимости не было.

По следующим ссылкам вы найдете дополнительную информацию о настройке сетевого моста, в частности, для предоставления общего доступа к Интернету:

- <http://www.ixbt.com/comm/prac-small-lan5.shtml>;
- <http://www.isranet.info/main/content/view/141/7/>;
- [http://www.nbu.gov.ua/inet/lan/page/page\\_4.html](http://www.nbu.gov.ua/inet/lan/page/page_4.html).

## Настраиваем маршрутизацию в Windows XP

Эта задача тоже может возникнуть в сетевой практике. Собственно, один из вариантов исключения маршрутизации в Windows XP — это использование компьютера для организации общего доступа к Интернету. Данная процедура предусмотрена разработчиками системы и автоматизирована с помощью мастера. Еще вариант маршрутизации, рассмотренный в предыдущей главе, — сетевой мост. Но в данный момент нас интересуют несколько иные задачи. Мы разбираем проблемы, связанные с объединением сетей.

### Указываем маршруты

Представьте себе ситуацию, когда в вашей сети несколько маршрутизаторов, которые ведут в разные сети. К тому же есть шлюз в Интернет, который используется всеми компьютерами сети. Такая ситуация реально показана на рис. 5.2 для сети WorkGr15.dom. Пользователи сети (1) должны в зависимости от выполняемых задач подключаться к сети (4) или сети (5).

Windows XP имеет в своем составе достаточно средств для решения задач маршрутизации и диагностики сети.

Для того чтобы указать системе дополнительный маршрут, есть команда `route`. Выполняется она из командной строки и в зависимости от параметров, применяемых вместе с ней, может добавлять или удалять маршруты или просто показать таблицу маршрутов, существующую в системе. Возможно создание как временных маршрутов, когда после перезагрузки и после перехода в спящий режим маршрут стирается из памяти машины, так и постоянных, когда информация о них записывается в реестр, и компьютер может их использовать без необходимости повторного выполнения команды.

Перед добавлением какого-либо маршрута есть смысл посмотреть на уже существующие в системе маршруты. Для этого достаточно выполнить следующие действия: **Пуск** | **Выполнить**, ввести `cmd` и нажать клавишу <Enter>. При этом просто

откроется окно командной строки. Теперь в окне командной строки следует ввести команду `route print`.

На экран будет выведена информация о существующих маршрутах (рис. 5.5).

```
C:\Documents and Settings\Administrator>route print

IPv4 таблица маршрута
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ..... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x10005 ...00 13 d4 90 25 f4 ..... Marvell Yukon 88E8053 PCI-E Gigabit Ethernet
Controller
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0        192.168.1.1     192.168.1.11   20
127.0.0.0         255.0.0.0     127.0.0.1       127.0.0.1      1
192.168.1.0       255.255.255.0 192.168.1.11    192.168.1.11   20
192.168.1.11     255.255.255.255 127.0.0.1       127.0.0.1      20
192.168.1.255    255.255.255.255 192.168.1.11    192.168.1.11   20
192.168.60.0     255.255.255.0 192.168.60.1    192.168.60.1   20
192.168.60.1     255.255.255.255 127.0.0.1       127.0.0.1      20
192.168.60.255  255.255.255.255 192.168.60.1    192.168.60.1   20
192.168.182.0   255.255.255.0 192.168.182.1   192.168.182.1  20
192.168.182.1   255.255.255.255 127.0.0.1       127.0.0.1      20
192.168.182.255 255.255.255.255 192.168.182.1   192.168.182.1  20
224.0.0.0        240.0.0.0     192.168.1.11    192.168.1.11   20
224.0.0.0        240.0.0.0     192.168.60.1    192.168.60.1   20
224.0.0.0        240.0.0.0     192.168.182.1   192.168.182.1  20
255.255.255.255  255.255.255.255 192.168.1.11    192.168.1.11   1
255.255.255.255  255.255.255.255 192.168.60.1    192.168.60.1   1
255.255.255.255  255.255.255.255 192.168.182.1   192.168.182.1  1
Основной шлюз:      192.168.1.1
=====
Постоянные маршруты:
Отсутствует

C:\Documents and Settings\Administrator>
```

Рис. 5.5. Информация о существующих маршрутах в окне командной строки

В таблице маршрутов, приведенной на рисунке, можно увидеть, что кроме системных маршрутов, которые никуда из компьютера не выводят, работает маршрут в Интернет (первая строка таблицы). Он отличается тем, что сетевой адрес и маска сети состоят из нулей. Указан адрес маршрутизатора (шлюза) и адрес интерфейса, через который компьютер имеет доступ в Интернет.

Теперь посмотрите на рис. 5.6. На нем приведено окно командной строки другого компьютера, на котором была выполнена команда

```
route add -p 10.0.0.0 mask 255.0.0.0 10.15.0.254 metric 2
```

которая требует создания маршрута в сеть 10.0.0.0 с маской 255.0.0.0 через шлюз 10.15.0.254. Параметр `-p` указывает на необходимость записи маршрута в реестр, чтобы при перезагрузках он сохранился, а `metric 2` указывает системе, что в сеть 10.0.0.0 можно попасть, пройдя два маршрутизатора.

Первая строка таблицы маршрутов также говорит о возможности выхода в Интернет с этого компьютера, а вторая строка показывает установленный новый маршрут. Под таблицей маршрутов указано, что маршрут постоянный, т. е. он записан в реестре и не пропадет при перезагрузке. Интересно, что по информации из этой таблицы можно предположить, что на этом компьютере есть сетевой адаптер, который в настоящее время не подключен к сети. Это адаптер с адресом 169.254.14.88.

```

C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Версия 5.00.2195]
(C) Корпорация Майкрософт, 1985-2000.

C:\Documents and Settings\Admin>route print
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x10000003 ...00 02 b3 b0 58 00 ..... Intel(R) PRO Adapter
0x10000004 ...00 02 b3 b0 57 b5 ..... Intel(R) PRO Adapter
=====
Активные маршруты:
Сетевой адрес          Маска сети             Адрес шлюза            Интерфейс              Метрика
-----
0.0.0.0                0.0.0.0               10.15.0.198           10.15.0.199            1
10.0.0.0               255.255.255.0        10.15.0.254           10.15.0.199            2
10.15.0.0              255.255.255.0        10.15.0.199           10.15.0.199            1
10.15.0.199           255.255.255.255     127.0.0.1             127.0.0.1              1
10.255.255.255       255.255.255.255     10.15.0.199           10.15.0.199            1
127.0.0.0             255.0.0.0            127.0.0.1             127.0.0.1              1
169.254.0.0           255.255.0.0         169.254.14.88         169.254.14.88          1
169.254.14.88        255.255.255.255     127.0.0.1             127.0.0.1              1
169.254.255.255     255.255.255.255     169.254.14.88         169.254.14.88          1
224.0.0.0             224.0.0.0            10.15.0.199           10.15.0.199            1
224.0.0.0             224.0.0.0            169.254.14.88         169.254.14.88          1
255.255.255.255     255.255.255.255     169.254.14.88         169.254.14.88          1
Основной шлюз:        10.15.0.198
=====
Постоянные маршруты:
Сетевой адрес          Маска           Адрес шлюза            Метрика
-----
10.0.0.0              255.0.0.0       10.15.0.254            2
C:\Documents and Settings\Admin>_

```

Рис. 5.6. Окно командной строки после добавления нового маршрута

Назначение маршрутов таким способом полезно не только для обеспечения доступа рабочих станций в какую-либо сеть, но и для обеспечения взаимодействия серверов объединяемых сетей. Например, если необходимо, чтобы DNS-сервер получал обновленную информацию от DNS-сервера другой сети, следует обеспечить доступность второго сервера.

Если требуется указывать временные маршруты достаточно часто, то можно подготовить пакетные файлы с командами добавления маршрутов и использовать их при необходимости. В качестве завершающей команды в файл следует записать `pause`. Эта команда предотвратит закрытие окна командной строки сразу после выполнения команд и даст вам возможность убедиться, что все выполнено без ошибок, или, наоборот, увидеть ошибки добавления маршрута.

Данные, приведенные на рис. 5.6, соответствуют компьютеру из объединенной сети. На рис. 5.3 это сервер, помеченный цифрой 2.

## Делаем маршрутизатор из Windows XP

Возможна также ситуация, когда компьютер под управлением Windows XP необходимо сделать маршрутизатором, т. е. этот компьютер установлен на границе сетей и обеспечивает доступ из одной сети в другую. Для того чтобы это стало реальным, требуется обеспечить возможность маршрутизации по всем сетевым интерфейсам компьютера, как это сделано в серверных операционных системах. Для этого нужно совсем немного.

Найдите в реестре ключ `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`, а в нем параметр `IPEnableRouter`. Если этого параметра нет, то создайте его с типом данных `REG_DWORD` и присвойте ему значение, равное 1. Это

значение включает маршрутизацию пакетов TCP/IP для всех сетевых подключений, установленных на данном компьютере.

После выполнения этих действий можно указывать маршруты через интерфейсы самого компьютера, заставив его работать в качестве маршрутизатора.

### **ВАЖНО!**

Компьютер-маршрутизатор должен работать только в маршрутизируемых сетях. Нельзя, например, подключать этот компьютер еще и к Интернету (если Интернет — не одна из маршрутизируемых сетей). В свойствах соединений не надо указывать основной шлюз. Все шлюзы необходимо добавлять командой `route add` из командной строки.

Для контроля правильности и работоспособности созданных маршрутов воспользуйтесь командами `tracert` и `netstat`. Команды командной строки могут иметь много полезных параметров. О них можно узнать, указав параметр `/?` или `-?` после команды. Параметры позволяют отобразить данные наиболее удобным для нас образом. На рис. 5.7 показан результат выполнения команды `netstat` с параметрами `-an -p tcp`. Параметры позволили отобразить числовые значения IP-адресов и исключить показ сведений о подключениях по всем сетевым протоколам, кроме TCP.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\administrator.MH2003S>netstat -an -p tcp

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      0.0.0.0:21            0.0.0.0:0          LISTENING
TCP      0.0.0.0:53            0.0.0.0:0          LISTENING
TCP      0.0.0.0:135           0.0.0.0:0          LISTENING
TCP      0.0.0.0:445           0.0.0.0:0          LISTENING
TCP      0.0.0.0:554           0.0.0.0:0          LISTENING
TCP      0.0.0.0:1025          0.0.0.0:0          LISTENING
TCP      0.0.0.0:1031          0.0.0.0:0          LISTENING
TCP      0.0.0.0:1036          0.0.0.0:0          LISTENING
TCP      0.0.0.0:1037          0.0.0.0:0          LISTENING
TCP      0.0.0.0:1755          0.0.0.0:0          LISTENING
TCP      0.0.0.0:3389          0.0.0.0:0          LISTENING
TCP      0.0.0.0:8098          0.0.0.0:0          LISTENING
TCP      127.0.0.1:1039        0.0.0.0:0          LISTENING
TCP      169.254.161.5:139    0.0.0.0:0          LISTENING
TCP      192.168.1.7:139      0.0.0.0:0          LISTENING
TCP      192.168.1.7:3389     192.168.1.11:2410  ESTABLISHED
TCP      192.168.1.7:3433     192.168.1.133:1026 ESTABLISHED
TCP      192.168.1.7:3434     192.168.1.133:1026 ESTABLISHED
TCP      192.168.1.7:3833     81.133.133.133:5050 ESTABLISHED
TCP      192.168.1.7:3901     192.168.1.133:389  CLOSE_WAIT
TCP      192.168.1.7:4223     192.168.1.133:445  TIME_WAIT
TCP      192.168.100.7:139    0.0.0.0:0          LISTENING
TCP      192.168.116.2:139    0.0.0.0:0          LISTENING
TCP      192.168.116.2:139    0.0.0.0:0          LISTENING
TCP      192.168.116.2:3884   10.15.0.76:445     ESTABLISHED
TCP      192.168.116.2:4136   10.15.0.183:445    ESTABLISHED
TCP      192.168.116.2:4176   10.15.0.199:445    ESTABLISHED
TCP      192.168.188.1:139    0.0.0.0:0          LISTENING
TCP      192.168.232.1:139    0.0.0.0:0          LISTENING
  
```

Рис. 5.7. Окно командной строки с результатом выполнения команды `netstat -an -p tcp`

В данном случае компьютер может иметь доступ к нескольким сетям. В настоящее время установлены соединения между интерфейсами в состоянии `ESTABLISHED`. Причем известно, что адрес `81.133.133.133` (адрес изменен) соответствует реально-

му IP-адресу удаленного компьютера в Интернете. Другие соединения установлены по адресам локальных сетей. Скорее всего, этот компьютер не сможет работать маршрутизатором между сетями 192.168.1.0 и 192.168.116.0, поскольку имеет подключение к Интернету и, соответственно, основной шлюз 192.168.1.1. Попытка любого подключения из сети в сеть через этот компьютер должна завершиться неудачей, поскольку все пакеты будут направляться в шлюз по умолчанию — основной шлюз. Но, отключив этот компьютер от Интернета, можно настроить маршрутизацию между тремя сетями — 192.168.1.0, 192.168.100.0 и 192.168.116.0. Сеть 192.168.100.0 сейчас не имеет связи с этим компьютером, интерфейс 192.168.100.7 слушает сеть (LISTENING) и готов принять подключение, если оно будет установлено.

В сложных случаях не ленитесь проводить эксперименты. На компьютере из примера удалось настроить маршрутизацию из сети 192.168.100.0 в сеть 10.15.0.0! Как вариант настройки маршрутизации — организация сетевого моста, рассмотренная ранее в *этой главе*. Это компьютер из сети, показанной на рис. 5.2.

Таким образом, разбирая результаты выполнения диагностических команд, можно сделать выводы о правильности текущих и возможностях будущих настроек.

Далее приведен перечень команд, которые могут пригодиться при возникновении проблем при создании маршрутов. Эти команды позволяют провести диагностику маршрутов и иногда оптимизировать их.

### **ПРЕДУПРЕЖДЕНИЕ**

Настраивая подключения к удаленным компьютерам через Интернет, вы, скорее всего, будете отключать Firewall и/или брандмауэр на подключаемых машинах. После завершения настроек *не забудьте восстановить защиту!* По возможности используйте нестандартные порты для таких подключений. Это существенно уменьшит вероятность взлома ваших компьютеров "доброжелателями".

- ❑ Команда `route` — отображает таблицу IP-маршрутизации и добавляет или удаляет маршруты IP. Это основная команда при работе с маршрутизатором.
- ❑ Команда `netstat` — отображает активные подключения TCP, порты, прослушиваемые компьютером, статистику Ethernet, таблицы IP-маршрутизации, статистику IPv4 (для протоколов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP через IPv6 и UDP через IPv6).
- ❑ Команда `ipconfig` — отображает текущие значения конфигурации сети TCP/IP, обновляет или освобождает адреса, назначенные сервером DHCP, а также отображает, регистрирует или освобождает имена DNS.
- ❑ Команда `ping` — отправляет сообщения с эхо-запросами по протоколу ICMP, чтобы проверить правильность настройки TCP/IP и доступность узла TCP/IP.
- ❑ Команда `hostname` — отображает имя узла.
- ❑ Команда `nbtstat` — отображает сведения о текущих соединениях NetBIOS поверх TCP/IP, обновляет кэш имен NetBIOS и отображает зарегистрированные имена и код области.



- ❑ Команда `pathping` — отображает путь к узлу TCP/IP и сообщает о потерях данных на каждом маршрутизаторе по пути следования пакета.
- ❑ Команда `tracert` — отображает путь узла TCP/IP.

Некоторые подробности о маршрутизации можно прочитать по следующим ссылкам:

- ❑ <http://www.computerbooks.ru/books/OS/Book-Windows-XP/Glava20/Index0.htm>;
- ❑ <http://www.netdocs.ru/articles/Making-Sense-Windows-Routing-Tables.html>;
- ❑ [http://home.mark-itt.ru/manual/iprouter\\_nt.htm](http://home.mark-itt.ru/manual/iprouter_nt.htm).

## Настраиваем маршрутизацию в Linux Mint

Современные версии Linux имеют графические интерфейсы для настройки различных параметров системы. Маршрутизация не исключение. Одна из программ, которая по умолчанию установлена в Linux Mint и во многих других версиях Linux, — NetworkManager. Интерфейс программы доступен по пути **Menu | Центр управления | Интернет и сеть | Сетевые соединения** (рис. 5.8).

Открыв окно **Сетевые соединения**, выполните следующие действия:

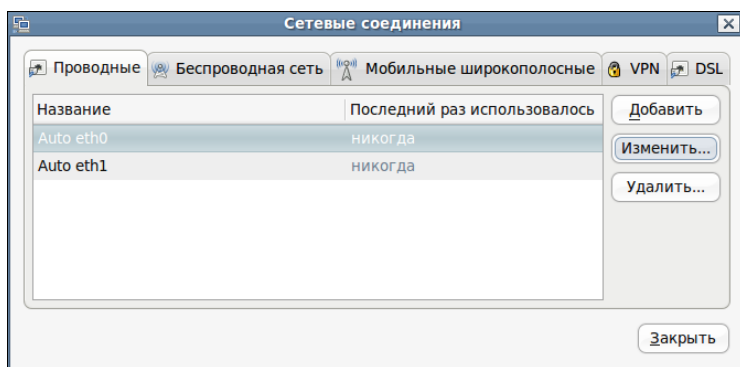
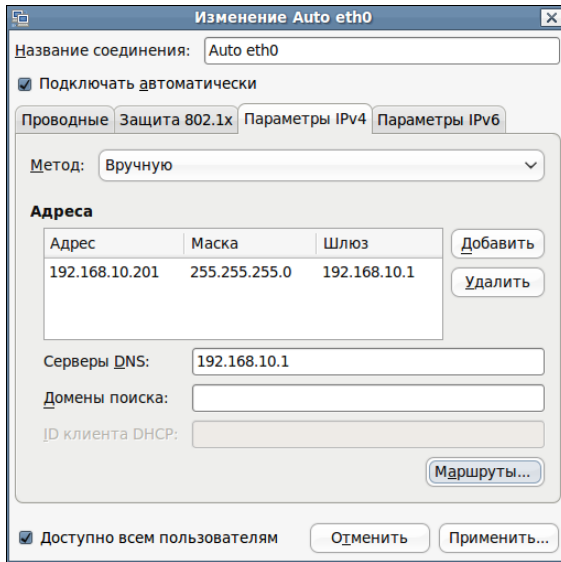


Рис. 5.8. Окно **Сетевые соединения** (интерфейс программы NetworkManager)

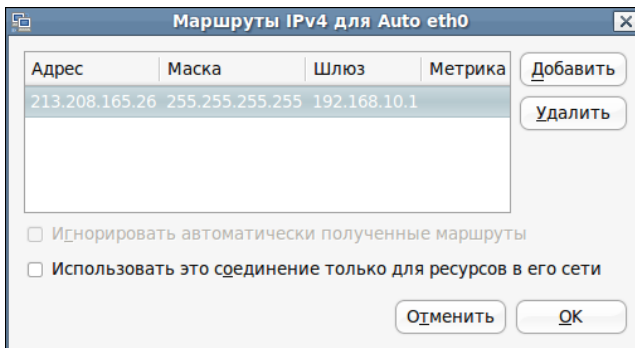
1. В окне **Сетевые соединения** выберите строку сетевого адаптера, для которого вы хотите установить статический маршрут (в примере Auto eth0), и нажмите кнопку **Изменить**. Откроется окно **Изменение Auto eth0** (рис. 5.9).
2. В окне **Изменение Auto eth0** нажмите кнопку **Маршруты**. Откроется окно **Маршруты IPv4 для Auto eth0** (рис. 5.10).
3. В окне **Маршруты IPv4 для Auto eth0** нажмите кнопку **Добавить** и введите адрес цели маршрута, маску адреса цели маршрута и шлюз для достижения цели.

Поле **Метрика** можно заполнить, если вы знаете число шагов до цели. Если цель находится в Интернете, то лучше это поле оставить пустым. Система сама определит метрику.

4. Остается нажать кнопки **ОК**, **Применить**, **Заккрыть**, последовательно закрывая окна в порядке, обратном открыванию.



**Рис. 5.9.** Окно  
Изменение Auto eth0



**Рис. 5.10.** Окно Маршруты IPv4 для Auto eth0

Все, маршрут создан. Если у вас есть два подключения к сети Интернет, то узел с адресом нашей цели маршрута будет доступен только через соединение Auto eth0. Это может быть полезно, если одно подключение к сети Интернет медленное, но безлимитное, а другое быстрое, но трафик дорогой. Вы можете выбрать оптимальный путь до цели, определяя, что важнее при ее достижении, скорость или экономия денег.

Указание статических маршрутов может быть полезно и для решения задач в локальных сетях.

Для указания маршрута в Linux можно обойтись и без графического интерфейса. Достаточно в окне терминала или в консольном сеансе ввести команду:

```
route add -net 192.168.20.0 netmask 255.255.255.248 gw 192.168.1.1
```

Эта команда добавит статический маршрут в сеть 192.168.20.0/29 через шлюз с IP-адресом 192.168.1.1.

### ПРИМЕЧАНИЕ

В примере встречается указание маски двумя способами. Чтобы легко переводить значение маски из одного формата записи в другой, установите программу `ipcalc` командой `sudo apt-get install ipcalc`. Эта программа выполняется в терминале. Введя команду `ipcalc 192.168.20.0 255.255.255.248`, вы получите такой вывод:

```
beard@beard-laptop ~ $ ipcalc 192.168.20.0 255.255.255.248
Address: 192.168.20.0      11000000.10101000.00010100.00000 000
Netmask: 255.255.255.248 = 29 11111111.11111111.11111111.11111 000
Wildcard: 0.0.0.7        00000000.00000000.00000000.00000 111
=>
Network: 192.168.20.0/29  11000000.10101000.00010100.00000 000
HostMin: 192.168.20.1    11000000.10101000.00010100.00000 001
HostMax: 192.168.20.6    11000000.10101000.00010100.00000 110
Broadcast: 192.168.20.7  11000000.10101000.00010100.00000 111
Hosts/Net: 6              Class C, Private Internet
```

В строке `Netmask` значение маски представлено сразу в трех вариантах.

## Применяем аппаратные маршрутизаторы и модемы

Модем и маршрутизатор, работая вместе, могут обеспечить связь двух удаленных на значительное расстояние сетей. Иногда это единственно возможный способ организовать взаимодействие удаленных сетей. Обычно для того, чтобы осуществить такое взаимодействие, требуется *выделенная линия*, а проще — прямой провод.

## Настраиваем связь по выделенной линии

Сразу следует отметить, что модемная связь в наше время может быть установлена между сетями в случаях, когда другого способа нет или когда модемной скорости вполне достаточно, или как временный вариант, чтобы не тратить средства на организацию более быстрого канала связи при отладке взаимодействия между сетями. Описанный в этой главе вариант связи проработал достаточно долго, пока не был заменен значительно более дорогим оптоволоконным каналом. Но работал надежно, соединяя сети на расстоянии более десяти километров. Выделенная линия представляла собой "прямой провод", проходящий через телефонный узел. По этому каналу связи круглосуточно передавались небольшие объемы информации.

На рис. 5.3 показана небольшая локальная сеть, помеченная цифрой 4. Из сети `WorkGr15.dom` в эту небольшую сеть можно попасть через маршрутизатор и модем. На рисунке не показано, но в сети 4 тоже установлен модем и маршрутизатор. Такая цепочка устройств и кабель или телефонная линия между ними позволяют связать две сети, когда это необходимо. Рассмотрим, как это можно настроить.

К сожалению, в отличие от настроек Windows, здесь нет вариантов, которые можно просто повторить, если не иметь точно такого же оборудования. Маршрутизаторы различных производителей имеют свои особенности и свои интерфейсы настроек и администрирования. Часто к ним требуются дополнительные платы расширения, чтобы обеспечить работу по тем или иным протоколам. В сети WorkGr15.dom применяется маршрутизатор фирмы Allied Telesyn AR410 для обеспечения связи с сетью 4. Причем, несмотря на то, что есть удобный выход в Интернет, связь по некоторым причинам осуществляется через модемы Zixel U-336E Plus по выделенной линии. Эти модемы, как и многие другие, позволяют автоматически устанавливать связь "модем — модем" сразу после включения (команды для этого описаны в документации на модем). При этом появляется канал связи, который можно использовать для маршрутизации между сетями. Маршрутизатор AR410 с помощью платы AT-AR024-00 (приобретается дополнительно), обеспечивающей работу с асинхронным портом, подключен к модему. Другой порт маршрутизатора включен в нашу сеть. Портam назначены IP-адреса, соответствующие допустимым в двух сетях. После первичной настройки маршрутизатора, которая осуществляется с помощью любого компьютера, на котором установлено прилагаемое к маршрутизатору программное обеспечение, и подключаемого к маршрутизатору специальным кабелем, его администрирование возможно через Web-интерфейс. В специальных файлах конфигурации указываются имена пользователей, их полномочия и пароли. Подключаясь через Web-интерфейс к маршрутизатору, необходимо авторизоваться. Кроме Web-интерфейса, для управления маршрутизатором можно применять Telnet. Открыв соответствующие порты для доступа из Интернета и направив их на адрес маршрутизатора, можно получить доступ к управлению им из Интернета. При попытке подключения через Web-интерфейс вам будет предложено авторизоваться (рис. 5.11).

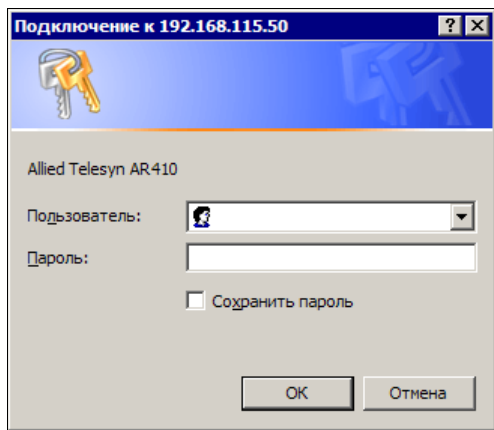


Рис. 5.11. Окно Подключение к <адрес маршрутизатора>

После авторизации будет показано главное окно с информацией о маршрутизаторе (рис. 5.12), из которого с помощью обычного для интернет-браузера меню можно получить доступ ко всем настройкам маршрутизатора.

На рис. 5.13 показано окно редактора файлов конфигурации с фрагментом раздела IP configuration, где описаны все необходимые маршруты.

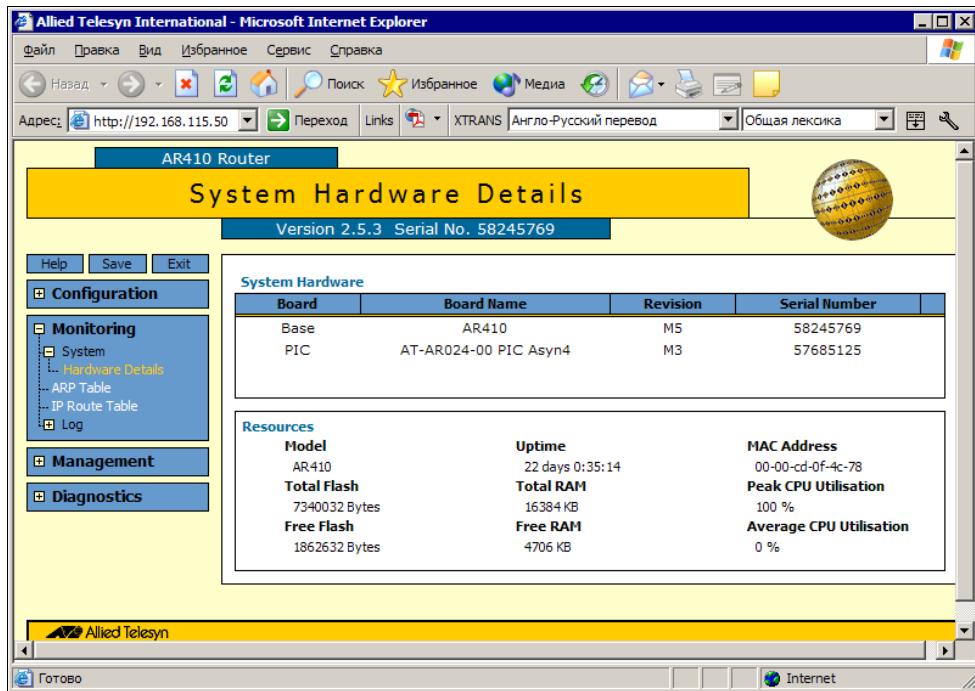


Рис. 5.12. Окно интернет-браузера с информацией о маршрутизаторе

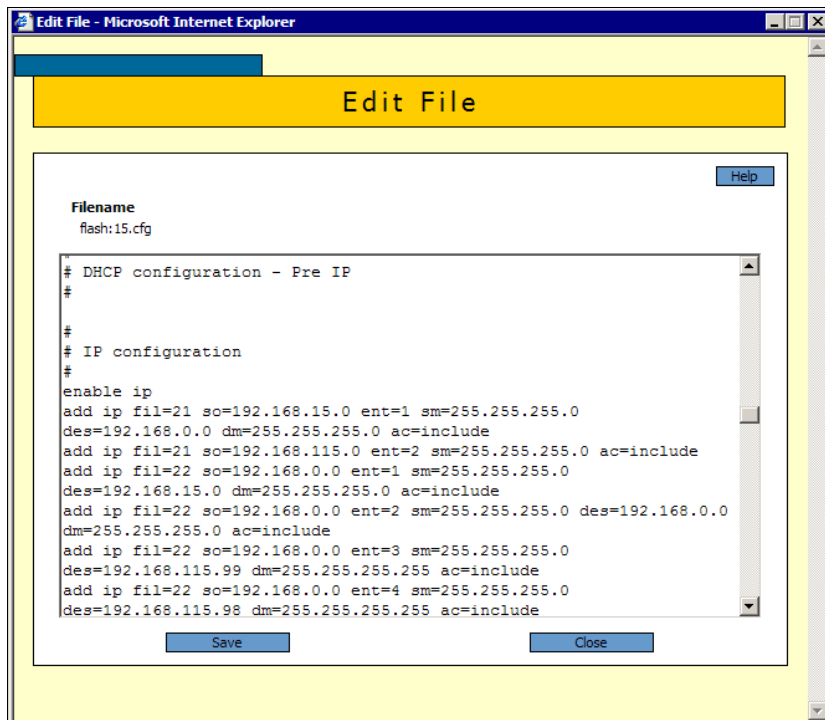
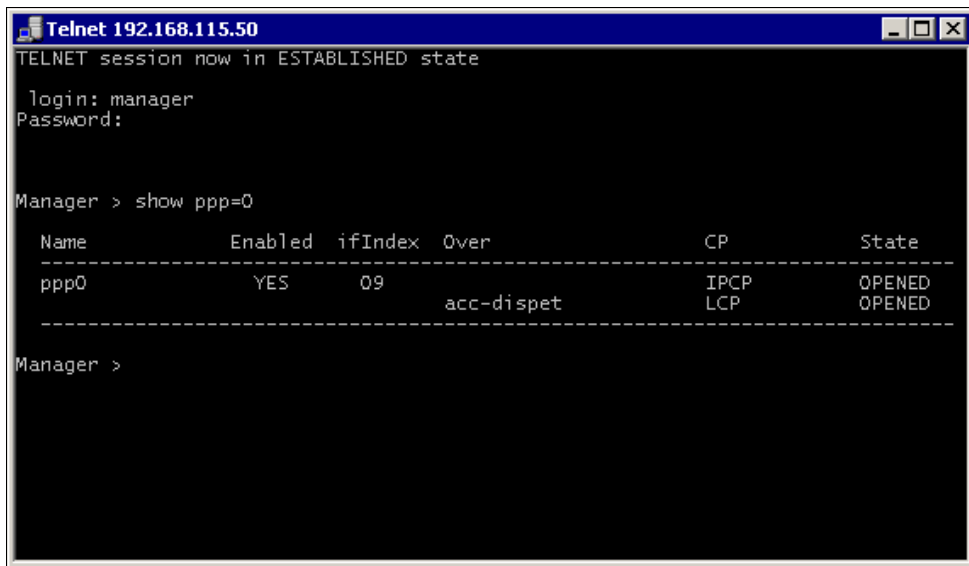


Рис. 5.13. Окно Edit File

Описание необходимых команд и их синтаксис приведены в описании маршрутизатора на прилагаемом к нему компакт-диске. При необходимости, можно удаленно перезагрузить маршрутизатор, пользуясь Web-интерфейсом или Telnet (рис. 5.14).



```

Telnet 192.168.115.50
TELNET session now in ESTABLISHED state

login: manager
Password:

Manager > show ppp=0

Name           Enabled  ifIndex  Over          CP           State
-----
ppp0           YES      09       acc-dispet    IPCP         OPENED
               LCP         OPENED
-----
Manager >

```

Рис. 5.14. Окно Telnet сеанса связи с маршрутизатором

Показанное на рис. 5.14 окно позволяет убедиться в том, что маршрутизатор включен, и все необходимые соединения установлены.

Теперь рассмотрим суть способа обеспечения безопасности подключения.

Обеспечение безопасности на стороне внешней сети — задача ее администратора. Поэтому рассмотрим решение задачи только на одной стороне.

На рис. 5.15 схематически показана организация подключения.

Если во внутреннюю сеть обеспечен доступ из внешней сети, то существует вероятность того, что ресурсы внутренней сети, доступные для всех ее пользователей, будут доступны и для случайного пользователя внешней сети. В нашем случае требовалось исключить такую возможность, но не усложнять политику доступа к ресурсам внутри сети.

Для ограничения доступа к ресурсам сети было использовано свойство IP-адресов в сетях — маска подсети, а также невозможность прямого подключения к компьютерам сети, к которой не указаны явно маршруты.

На рис. 5.13 показано окно с фрагментом содержания файла IP-настроек маршрутизатора, в котором описаны сети и адреса, допустимые для подключения. Выберем из всех строк только те, что касаются решения поставленной задачи. Символом # обозначим комментарии, которые не обязательны в файле конфигурации и не используются маршрутизатором. Реально эти комментарии отсутствуют в файле и приведены только в книге. Описываемая часть файла конфигурации представлена в листинге 5.1.

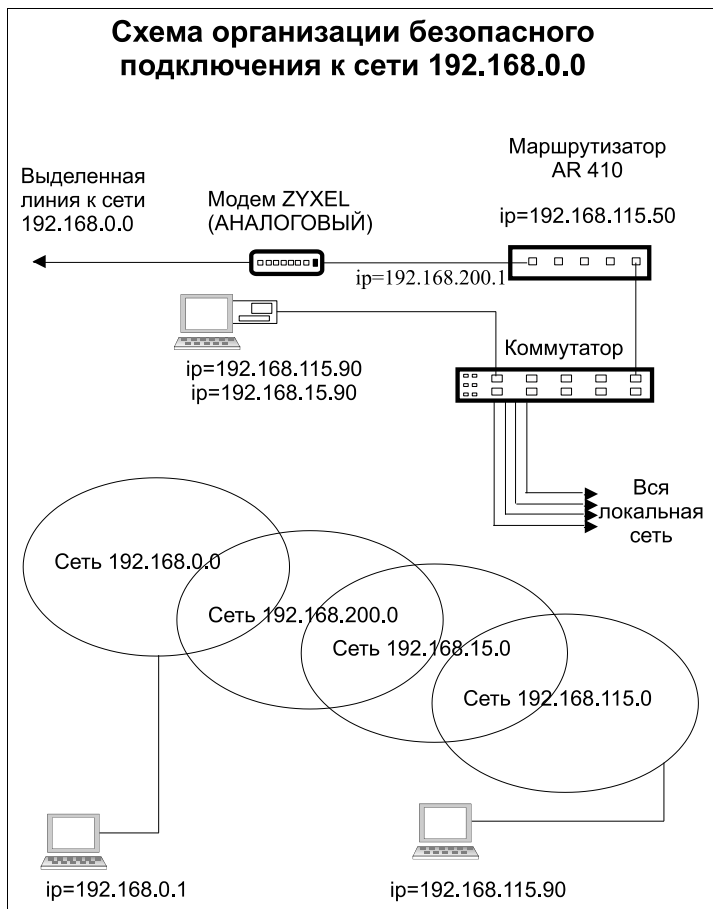


Рис. 5.15. Схема организации безопасного подключения к сети 192.168.0.0

**Листинг 5.1. Фрагмент файла конфигурации маршрутизатора**

```
# - разрешение сети 192.168.15.0 подключаться к сети 192.168.0.0
add ip fil=21 so=192.168.15.0 ent=1 sm=255.255.255.0 ↵
des=192.168.0.0 dm=255.255.255.0 ac=include
# - разрешение сети 192.168.115.0 подключаться к сети 192.168.0.0
add ip fil=21 so=192.168.115.0 ent=2 sm=255.255.255.0 ac=include
# - разрешение сети 192.168.0.0 подключаться к сети 192.168.15.0
add ip fil=22 so=192.168.0.0 ent=1 sm=255.255.255.0 ↵
des=192.168.15.0 dm=255.255.255.0 ac=include

# - разрешение сети 192.168.0.0 подключаться к сети,
# состоящей из единственного адреса - 192.168.115.99
add ip fil=22 so=192.168.0.0 ent=3 sm=255.255.255.0 ↵
des=192.168.115.99 dm=255.255.255.255 ac=include
```

```
# - разрешение сети 192.168.0.0 подключаться к сети, состоящей
# из единственного адреса - 192.168.115.98 (фактически, это разрешение
# компьютеру 192.168.115.98 получать информацию из сети 192.168.0.0)
add ip fil=22 so=192.168.0.0 ent=4 sm=255.255.255.0 ↵
des=192.168.115.98 dm=255.255.255.255 ac=include
# - назначение порту маршрутизатора, смотрящему во внутреннюю сеть,
# адреса 192.168.115.50
add ip int=vlan3 ip=192.168.115.50 fil=21
# - назначение порту маршрутизатора, смотрящему во внешнюю сеть, адреса
# 192.168.200.1 (по договоренности с администратором внешней сети)
add ip int=ppp0 ip=192.168.200.1 fil=22
# - назначение маршрута в сеть 192.168.0.0 на адрес 192.168.0.20
# (по договоренности с администратором внешней сети)
add ip rou=192.168.0.0 mask=255.255.255.0 int=ppp0 next=192.168.0.20
# - назначение маршрута в сеть 192.168.15.0 на любой ее адрес
add ip rou=192.168.15.0 mask=255.255.255.0 int=vlan3 next=0.0.0.0
# - указание адреса DBS-сервера
add ip dns prim=192.168.115.15
```

Кроме того, выполнено назначение сетевым адаптерам компьютеров, участвующих в общении с внешней сетью 192.168.0.0, дополнительных IP-адресов, принадлежащих вымышленной сети 192.168.15.0. У сетевых адаптеров, принадлежащих этой сети, два адреса: один из сети 192.168.15.0, другой из сети 192.168.115.0.

В результате применения этих настроек маршрутизатор позволяет из внешней сети "видеть" только строго определенные для этого компьютеры нашей сети (и то по дополнительным IP-адресам). Вход в сеть 192.168.115.0 для пользователя внешней сети невозможен (отдельные адреса этой сети выделены для доступа из внешней сети, как отдельные сети).

Учитывая необходимость авторизации в домене для доступа к ресурсам сети, доступ в нашу сеть из внешней сети практически невозможен. Доступ к разрешенным для этого ресурсам из нашей сети во внешнюю обеспечен администратором внешней сети. Для этого используется компьютер, не входящий в домен внешней сети, что позволяет обеспечить к нему доступ из любой внешней сети. Для этого необходимо лишь установить соответствующие разрешения.

Конечно, безопасность подключения к внешней сети обеспечена не только собственно маршрутизацией и организацией специфического адресного пространства. Важны и другие компоненты защиты, такие как сложные пароли для доступа к настройкам маршрутизатора по telnet-протоколу или через Web-интерфейс.

Возможно, что в вашем случае будет применен иной способ маршрутизации, например, с использованием дополнительного компьютера с серверной операционной системой или компьютера с Windows XP. Применение описанного принципа безопасной связи с другой сетью возможно в любом варианте реализации маршрутизации. Можно и упростить маршрутизацию, обеспечив безопасность средствами серверной операционной системы, например.



При создании описанного канала связи были применены модемы Zixel U-336E Plus по причине их надежности и приспособленности для организации связи по выделенной линии. Но могут применяться и другие модемы. Следует только иметь в виду, что Win-модемы, которые могут работать только под управлением операционной системы, невозможно заставить работать самостоятельно, как в этом примере. Для организации канала связи с их помощью придется в качестве маршрутизаторов использовать компьютеры, к которым они подключены.

## Настраиваем доступ через Интернет

Как-то перед автором была поставлена задача объединения двух сетей: СЕТЬ1 (192.168.1.1/24) и СЕТЬ2 (192.168.0.1/24) через Интернет. Причем, необходимо было выполнить такое условие:

Реальное подключение рабочих станций к Интернету из СЕТИ1 должно выполняться через СЕТЬ2. Более того, в целях экономии СЕТЬ1 получила от провайдера только внутренний адрес 10.255.0.6 и не имела возможности выйти в Интернет, СЕТЬ2 получила внутренний адрес 10.255.0.2 и динамический адрес для выхода в Интернет.

Вот здесь возможности маршрутизации аппаратными средствами показали себя с самой выгодной стороны. Для решения задачи были использованы два маршрутизатора AT AR415S. Несмотря на наличие Web-интерфейса у этих маршрутизаторов, файлы конфигурации готовились в текстовом редакторе. Листингах 5.2 и 5.3 приведены конфигурации маршрутизаторов с необходимыми комментариями, которые предваряются символом "#". Значения некоторых параметров заменены понятным пояснением.

### Листинг 5.2. Конфигурация маршрутизатора СЕТЬ1

```
# System configuration
set system name="NET1"

# User configuration
# Здесь указаны параметры подключения администратора к маршрутизатору
set user securedelay=600
add user=admin pass=<Значение пароля>
priv=securityOfficer lo=yes
set user=admin telnet=yes netmask=255.255.255.255
set user=manager pass=<Значение пароля> priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
enable user rso

#Адреса сетей, из которых возможен доступ администратора к маршрутизатору
add user rso ip=10.255.0.4 mask=255.255.255.252
add user rso ip=10.255.0.0 mask=255.255.255.252
add user rso ip=192.168.150.0 mask=255.255.255.0
add user rso ip=192.168.0.0 mask=255.255.255.0
add user rso ip=192.168.1.0 mask=255.255.255.0
```

```

#Адрес Интернета, с которого возможен доступ администратора к маршрутизатору
add user rso ip=XXX.XXX.XXX.XXX mask=YYY.YYY.YYY.YYY
##### #
# Назначаются порты для локальной сети. Сеть провайдера будет подключена к Eth0
# VLAN general configuration
create vlan="lan" vid=2
# VLAN port configuration
add vlan="2" port=1-4
##### #
# Для защиты сетевого трафика используем VPN с каналом L2TP через PPP
# L2tp configuration
enable l2tp
enable l2tp server=both
add l2tp call="tunnel" rem="tunnel" ip=10.255.0.2 ty=virtual prec=in
# PPP-tunnel configuration
create ppp=1 over=tnl-tunnel
set ppp=1 bap=off username="chap" password="chap"
##### #
# IP configuration
enable ip
enable ip remote
enable ip dnsrelay
#Здесь указаны адреса DNS-серверов (192.168.0.15 находится в СЕТИ 2)
add ip dns prim=192.168.0.15 seco=195.34.32.116
# Назначение адреса интерфейсу, обращенному в локальную сеть
add ip int=vlan2 ip=192.168.1.50
# Назначение адреса интерфейсу, обращенному в сеть провайдера
add ip int=eth0 ip=10.255.0.6 mask=255.255.255.252
# Назначение адреса вспомогательному интерфейсу
add ip int=ppp1 ip=192.168.150.2
set ip loc ip=192.168.1.50
##### #
# Маршрут через шлюз провайдера ко всем возможным целям
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=10.255.0.5 pref=8
# Вспомогательный маршрут через сеть провайдера
add ip rou=10.255.0.2 mask=255.255.255.255 int=eth0 next=10.255.0.5 pref=1
#Маршрут для трафика VPN
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp1 next=192.168.150.1 pref=4
##### #
# Настройка Firewall
enable firewall
create firewall policy="net1"
enable firewall policy="net1" icmp_f=unre,ping,sour,timee
add firewall policy="net1" int=vlan2 type=private
add firewall policy="net1" int=eth0 type=public
add firewall policy="net1" int=ppp1 type=private

```

```

# Разрешаем доступ к маршрутизатору по Telnet
add firewall policy="net1" ru=11 ac=allo int=eth0 prot=tcp po=23
ip=192.168.1.50 gblip=10.255.0.6 gblp=23
# Разрешаем доступ в Интернет отдельным компьютерам сети
add firewall policy="net1" ru=12 ac=allo int=vlan2 prot=ALL ip=0.0.0.0
add firewall policy="net1" ru=14 ac=allo int=vlan2 prot=TCP port=80
ip=192.168.1.11
add firewall policy="net1" ru=15 ac=allo int=vlan2 prot=TCP port=80
ip=192.168.1.22
# Всем остальным запрещаем
add firewall policy="net1" ru=16 ac=allo int=vlan2 prot=TCP port=80
ip=192.168.1.1-192.168.1.254

# Настройка VPN
add firewall policy="net1" ru=17 ac=non int=eth0 prot=ALL

add firewall policy="net1" ru=18 ac=non int=vlan2 prot=ALL
ip=192.168.1.1-192.168.1.254
set firewall policy="net1" ru=18 rem=192.168.0.0-192.168.0.254
add firewall policy="net1" ru=19 ac=allo int=ppp1 prot=ALL ip=0.0.0.0
##### #
##### #
# NTP configuration
#VNIIIFTRI, Moscow region, Russia (ntp1.imvp.ru)
enable ntp
set ntp utc=+04:00:00
add ntp peer=62.117.76.142
##### #
# GUI configuration
disable gui
# Получаем данные от DHCP-сервера сети СЕТЬ2
# BOOTP configuration
enable bootp relay
add bootp relay=192.168.0.15

```

### Листинг 5.3. Конфигурация маршрутизатора СЕТЬ2

```

# Конфигурация маршрутизатора СЕТЬ2
set system name="NET2"
# User configuration
set user securedelay=3600
add user=admin pass=<Значение пароля> priv=securityOfficer lo=yes
set user=admin telnet=yes netmask=255.255.255.255
set user=manager pass=<Значение пароля> priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
enable user rso
add user rso ip=10.255.0.4 mask=255.255.255.252
add user rso ip=10.255.0.0 mask=255.255.255.252

```

```

add user rso ip=192.168.150 mask=255.255.255.0
add user rso ip=192.168.0.0 mask=255.255.255.0
add user rso ip=192.168.1.0 mask=255.255.255.0

#Доступ к маршрутизатору с адреса в Интернете
add user rso ip=XXX.XXX.XXX.XXX mask=YYY.YYY.YYY.YYY
##### #

# В локальную сеть обращены порты 2-4 (vlan2), а в Интернет port1 (vlan3)
create vlan="lan" vid=2
create vlan="Internet" vid=3
# VLAN port configuration
add vlan="2" port=2-4
add vlan="3" port=1
##### #
# Параметры подключения к Интернету
create ppp=0 over=vlan3-any
set ppp=0 over=vlan3-any lqr=off echo=on iprequest=on username="Имя
пользователя" password="пароль"
##### #

#Настройка VPN через L2TP
enable l2tp
enable l2tp server=both
add l2tp call="tunnel" rem="tunnel" ip=10.255.0.6 ty=virtual prec=in
# PPP-tunnel configuration
create ppp=1 over=tnl-tunnel
set ppp=1 bap=off username="chap" password="chap"
##### #

# IP configuration - настройка IP-адресов и фильтров
enable ip
enable ip remote
enable ip dnsrelay
add ip dns prim=192.168.0.15 seco=195.34.32.116
add ip fil=101 so=192.168.0.0 sm=255.255.255.0 ent=1 des=192.168.1.0
dm=255.255.255.0 policy=3
add ip int=vlan2 ip=192.168.0.50
add ip int=eth0 ip=10.255.0.2 mask=255.255.255.252
add ip int=ppp0 ip=0.0.0.0
add ip int=ppp1 ip=192.168.150.1
set ip loc ip=192.168.0.50
##### #

# Маршруты в Интернет и VPN
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0 pref=8
add ip rou=10.255.0.6 mask=255.255.255.255 int=eth0 next=10.255.0.1 pref=4
add ip rou=192.168.1.0 mask=255.255.255.0 int=ppp1 next=192.168.150.2 pref=7
##### #
# Настройка Firewall
enable firewall
create firewall policy="net2"
enable firewall policy="net2" icmp_f=unre,ping,sour,timee
disable firewall policy="net2" tcpsetupproxy

```

```

add firewall policy="net2" int=vlan2 type=private
add firewall policy="net2" int=eth0 type=private
add firewall policy="net2" int=ppp0 type=public
add firewall policy="net2" int=ppp1 type=private
##### #
# Здесь включаем NAT при выходе в Интернет для каждой сети
add firewall policy="net2" nat=enhanced int=vlan2-0 gblin=ppp0
add firewall policy="net2" nat=enhanced int=ppp1 gblin=ppp0
##### #
add firewall policy="net2" ru=21 ac=allo int=eth0 prot=tcp po=23
ip=192.168.0.50 gblip=10.255.0.2 gblp=23
add firewall policy="net2" ru=22 ac=allo int=ppp0 prot=tcp po=23
ip=192.168.0.50 gblip=0.0.0.0 gblp=23
add firewall policy="net2" ru=22 ac=allo int=ppp1 prot=tcp po=23
ip=192.168.0.50 gblip=192.168.150.1 gblp=23
add firewall policy="net2" ru=23 ac=allo int=ppp0 prot=tcp po=23
ip=192.168.150.2 gblip=0.0.0.0 gblp=20023
#Office-to-office VPN
add firewall policy="net2" ru=54 ac=non int=vlan2 prot=ALL
ip=192.168.0.1-192.168.0.254
set firewall policy="net2" ru=54 rem=192.168.1.0-192.168.1.254
add firewall policy="net2" ru=55 ac=allo int=ppp1 prot=ALL
#Internet Access
add firewall policy="net2" ru=60 ac=allo int=vlan2 prot=ALL
ip=192.168.0.1-192.168.0.70
add firewall policy="net2" ru=61 ac=deny int=vlan2 prot=ALL
ip=192.168.0.1-192.168.0.254
##### #
# NTP configuration
#VNIIPTRI, Moscow region, Russia (ntp1.imvp.ru)
enable ntp
set ntp utc=+03:00:00
add ntp peer=62.117.76.142
##### #
# GUI configuration
disable gui

```

## Ссылки

Ссылки по теме:

- [http://www.opennet.ru/base/net/nt\\_leased.txt.html](http://www.opennet.ru/base/net/nt_leased.txt.html);
- <http://forums.gameguru.ru/board-hardware/action-display/num-1156266077/>;
- [http://www.ixbt.com/comm/ras\\_w95.html](http://www.ixbt.com/comm/ras_w95.html);
- [http://gizmodo.ru/2005/09/18/svjaz\\_po\\_modemu/](http://gizmodo.ru/2005/09/18/svjaz_po_modemu/);
- <http://v90.kiev.ua/faq/ats.html>.

## ГЛАВА 6



# Используем старый компьютер в сети

Техника развивается, появляются новые модели компьютеров. Чем больше вы стремитесь не отстать от прогресса, тем... больше рискуете стать обладателем устаревшего оборудования. Если кто-то не спешил приобрести компьютер во времена DOS (теперь не все пользователи ПК знают об этой операционной системе), то в самом худшем случае на его компьютере установлена Windows 95. Если же вы или ваши старшие родственники стремились идти в ногу со временем, то вполне вероятно, что у вас осталась машина, которая не в состоянии работать под управлением Windows. Возможно, что это компьютер вашего старшего брата или отца. Стоит эта машина, никто ее не включает, обновить железо сложно (ситуация имеет место для старых компьютеров HP Vectra, например), продать нельзя (никому не нужна), а выбросить жалко.

## Компьютер под DOS в вашей сети

Но старый компьютер еще может принести пользу. Во-первых, совершенно не вредно получить представление о возможностях старых операционных систем, а во-вторых, возможности старого компьютера могут оказаться полезными в новой сети. Зачем нагружать лишними задачами ваш рабочий компьютер или приобретать для их решения новую машину, если вполне еще может поработать старая заслуженная рабочая станция?

Для того чтобы все описываемые действия можно было выполнить пользователям, которые не знакомы с ОС, более старыми, чем Windows 98, мы рассмотрим MS-DOS 7.1, которая входит в состав Windows 98. Несложно, выполнив команду `sys c:`, перенести эту систему на винчестер с загрузочной дискеты Windows 98. Вы можете применить и другие версии DOS, под управлением которых работают ваши компьютеры, например free DOS (<http://www.freedos.org/>) или PTS DOS (<http://www.phystechsoft.ru/ptsdos/>). 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, работающем под управлением DOS. Можно использовать встроенный в Windows 9x редактор Edit.com.

Условимся, что каталог, в который устанавливается MS-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 6.1—6.4.

### Листинг 6.1. 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 6.2. Файл Config.sys

```
[menu]
menuitem=D, Use Net ; В этом разделе создается меню для
menuitem=C, No net  ; выбора 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
bufferhigh=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 6.3. 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 6.4. 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- А "
;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 Арахна
c:\drv\pktdrv\hprclanp 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 DOS-станции. В процессе установки сетевого программного обеспечения файл будет изменяться автоматически, но его окончательный вид должен быть таким, как в листинге 6.4. Кроме приведенных файлов вам могут понадобиться и другие. В табл. 6.1—6.3 приведен примерный перечень файлов, которые можно скопировать с загрузочной дискеты и из каталога \Windows\Command в соответствии с их размещением на диске, полученном командой DIR.

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: каталог \DISTRIB и поместите туда полученные файлы. Эти файлы позволят включить рабочие станции под управлением DOS в сеть.

**Таблица 6.1.** Содержимое диска C:\

Название файла или папки	Размер файла, байтов	Описание
COMMAND.COM	95 202	Командный процессор
NC <ПАПКА>		Norton Commander
NET <ПАПКА>		Каталог 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>		Системный каталог
MSDOS.SYS	116	Файл MS-DOS
CONFIG.SYS	432	Файл MS-DOS
LOGO.SYS	129 078	Заставка
AUTOEXEC.BAT	869	Файл MS-DOS

**Таблица 6.2.** Содержимое папки C:\DISTRIB

Название файла или папки	Размер файла, байтов	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 6.3. Содержимое папки C:\DOS7

Название файла или папки	Размер файла, байтов	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

## Установка Microsoft Network Client version 3.0 for MS-DOS

### ПРИМЕЧАНИЕ

Этот клиент может работать и в других DOS, автор использовал его с PTS DOS, например.

Перед началом установки проделайте следующее:

1. Создайте каталоги: \DISTRIB\DISK1 и \DISTRIB \DISK2.
2. Скопируйте в них файлы dsk3-1.exe и dsk3-2.exe.

3. Распакуйте файлы, запустив их на выполнение.
4. Перейдите в каталог `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 клавишу `<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 клавишу `<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 потребуются скорректировать сетевую конфигурацию компьютера. Клавишами со стрелками выберите **Change Network Configuration** и нажмите клавишу `<Enter>`.
12. На следующем экране (рис. 6.1) 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 для выбора необходимого действия.
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 поместить курсор на имя сетевого протокола, перейти в нижнее окно с помощью клавиши `<Tab>` и выбрать команду **Add protocol**. Нам потребуется добавить два протокола: `Microsoft TCP/IP` и `Microsoft NetBEUI`. Протокол, который предлагался по умолчанию, следует удалить (команда **Remove**).
14. Теперь необходимо настроить протокол `Microsoft TCP/IP`. Установив курсор на имя протокола, в нижнем меню выберите команду **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.

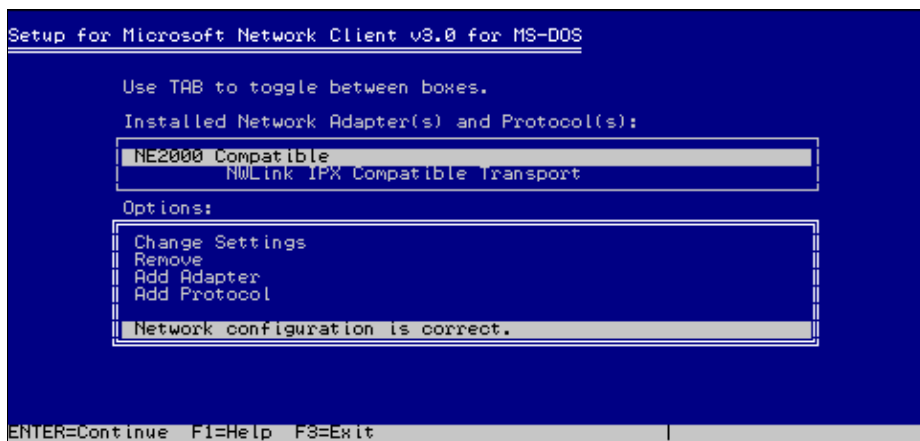


Рис. 6.1. Один из экранов программы Setup for Microsoft Network Client v3.0 for MS-DOS

### **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 команду **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 выбора команды **The listed options are correct** начнется процесс копирования файлов, по завершении которого компьютер выдаст запрос на перезагрузку. Если в дисковом диске 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, нажмите клавишу <Enter>. Или наберите другое имя и тоже нажмите клавишу <Enter>.

Появится строка "Type your password:" ("Напечатайте ваш пароль:"). Введите пароль. Вместо букв будут выводиться звездочки, затем нажмите клавишу <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 клавишу <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 прошло 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 `netshag.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 6.5 и 6.6, 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 6.5. 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]
NBSSessions=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 6.6. Файл System.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
dosphotkey=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=tcdrv.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.

## Настройки DHSP и WINS на сервере Windows 2000 Server

Протокол TCP/IP, который используется рабочей DOS-станцией, несколько отличается от того, который применяется сервером Windows 2000. В связи с этим настройка сервера для общения с Microsoft Network Client version 3.0 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 DOS-станции.
2. Нажмите кнопку **Пуск**.
3. Выберите **Программы | Администрирование | DHCP**. Откроется окно **DHCP** (рис. 6.2).
4. Раскройте папку **Область**, соответствующую адресам вашей сети, выделите папку **Арендованные адреса** и в списке справа найдите адрес рабочей DOS-станции (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 DOS-станции в соответствии с новым значением адреса и перезагрузите ее.

- Выделите папку **Резервирование**, щелкните правой кнопкой мыши и выберите пункт **Создать резервирование**.

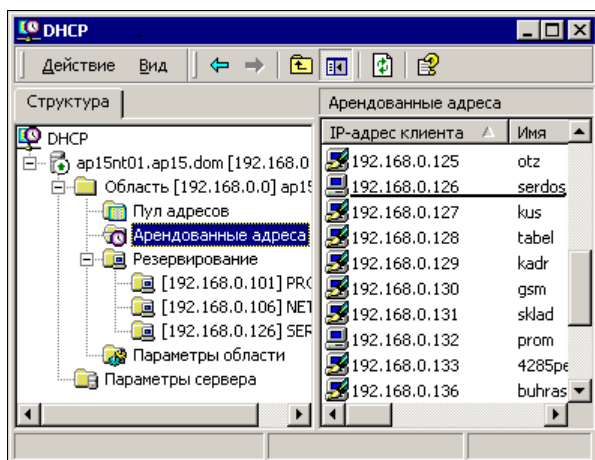


Рис. 6.2. Окно DHCP

- В открывшемся окне введите имя рабочей станции, ее IP-адрес и при необходимости комментарий.
- Нажмите кнопку **Добавить**.
- Закройте окно **DHCP**.
- Нажмите кнопку **Пуск**.
- Выберите **Программы | Администрирование | WINS**. Откроется окно **WINS** (рис. 6.3).
- Выделите папку **Активные регистрации**.

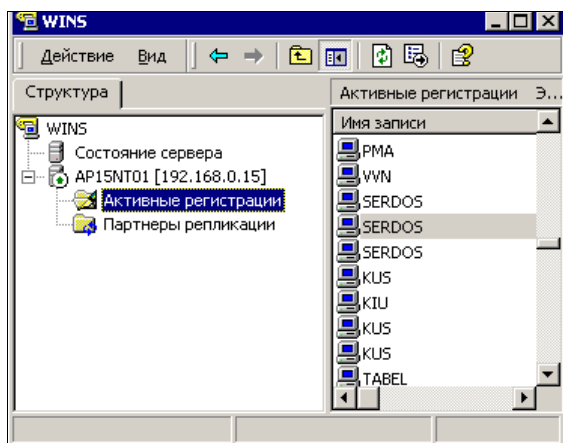


Рис. 6.3. Окно WINS

12. Щелкните правой кнопкой мыши и выберите команду 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 DOS-станции, достаточно внимательно посмотреть на строки, появляющиеся на экране в процессе загрузки с установленным Microsoft Network Client v3.0 for MS-DOS.
14. Нажмите кнопку **ОК**.

Теперь IP-адрес рабочей DOS-станции не будет изменяться по воле сервера и при установке программного обеспечения, которое требует указания адреса компьютера, и вы будете уверены, что вводите действительный адрес. Компьютеры сети, не использующие сервис, предоставляемый сервером, также смогут подключаться к рабочей DOS-станции и предоставлять ей свои ресурсы.

К сожалению, немного программ осталось в Интернете для ОС MS-DOS. Но если у вас есть архивы с такими программами, они еще могут поработать в вашей сети. Ведь MS-DOS может многое, даже прогулки в Интернете для нее не проблема. Посмотрите материалы по следующим ссылкам, чтобы убедиться в этом:

- <http://www.okobox.narod.ru/nowin.htm>;
- <http://www.okobox.narod.ru/diskwww.html>;
- <http://www.webcenter.ru/~zwb/arachne.htm>.

## Linux

Вовсе не обязательно, что компьютер с этой ОС — устаревший. Но все же, на совсем новых компьютерах эта ОС встречается реже, чем на уже поработавших.

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 на самом деле достаточно много) этой системы — Fedora — можно приобрести менее чем за триста рублей, если заказать дистрибутивные диски в Linux-центре. 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 журнальный файл.

#### **ПРИМЕЧАНИЕ**

Пользователи Windows привыкли к понятию log-файл, которым по сути и является журнальный файл. Но Linux использует этот файл самостоятельно без участия пользователя. Его назначение — не показать пользователю результат операций, а дать возможность самой системе запомнить выполненные действия и, при необходимости, вернуться к предыдущему состоянию. В Linux этот файл принято называть — *“журнальный файл”*.

Только после проверки правильности внесенных изменений запись в журнальном 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. Это определило категорию пользователей, применяющих Linux, — в основном это грамотные пользователи, регулярно использующие Интернет. Но сети Microsoft Windows тоже стали использовать TCP/IP. Соответственно, применение ОС Linux возможно и в сетях Microsoft Windows.

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<sup>1</sup> (Extensible Markup Language, расширяемый язык разметки), расположенные на другом сервере. Все, доступные мне и моим знакомым компьютеры под Windows нормально видели эти страницы, а доступный мне компьютер с 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 для Linux не смогут быть решены Windows-системой. Система Linux не понимает и доменов Active Directory от Microsoft.

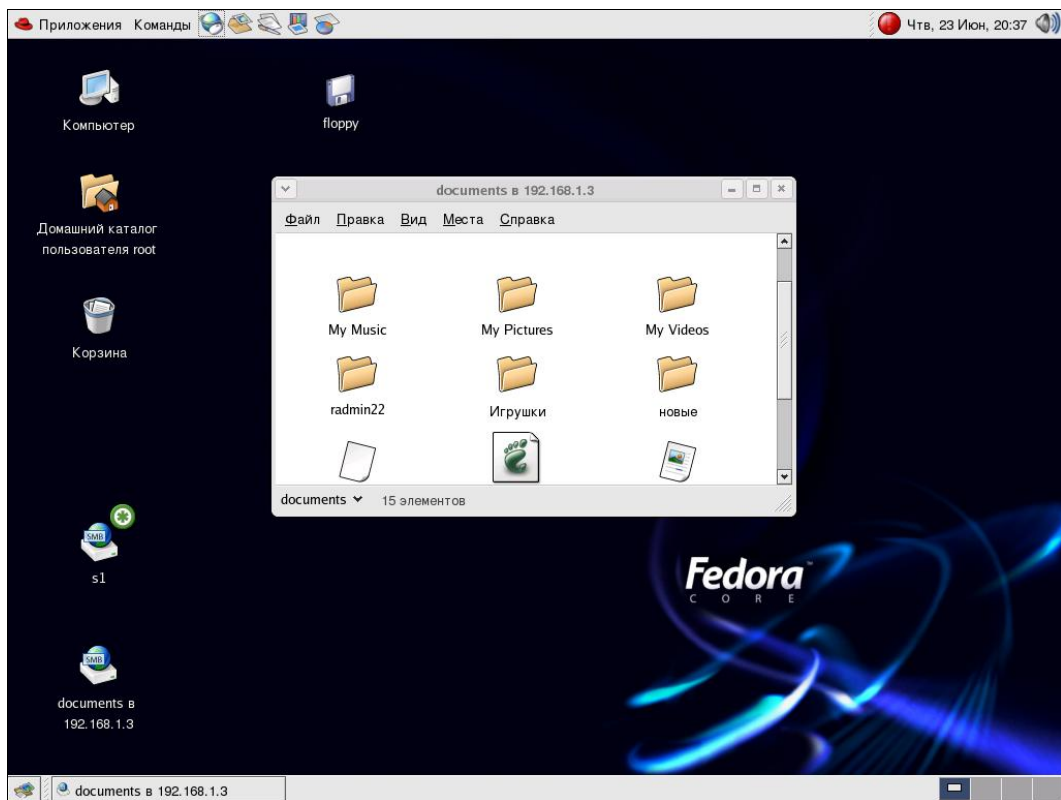
---

<sup>1</sup> Подробнее об этом языке можно прочитать по адресу в Интернете <http://www.codenet.ru/webmast/xml/>.

**ПРИМЕЧАНИЕ**

Справедливости ради, следует сказать, что не все версии Linux не понимают доменов Active Directory. Самая последняя версия Linux XP (с последними обновлениями, доступными с 01.10.2006) понимает Active Directory.

Это значит, что с такой рабочей станции невозможно войти в сеть Microsoft Windows под управлением Active Directory. Но в сети с рабочими группами работать можно вполне. На рис. 6.4 показан вид сетевой папки, которая расположена на компьютере с Windows и к которой подключен компьютер с Linux.



**Рис. 6.4.** Рабочий стол Linux с открытой сетевой папкой на нем

Развитые средства для работы в Интернете позволяют подключаться к каталогам компьютеров Windows, как к Web-папкам (рис. 6.5). И такая настройка доступа не вызывает затруднений.

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. Знатки 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.

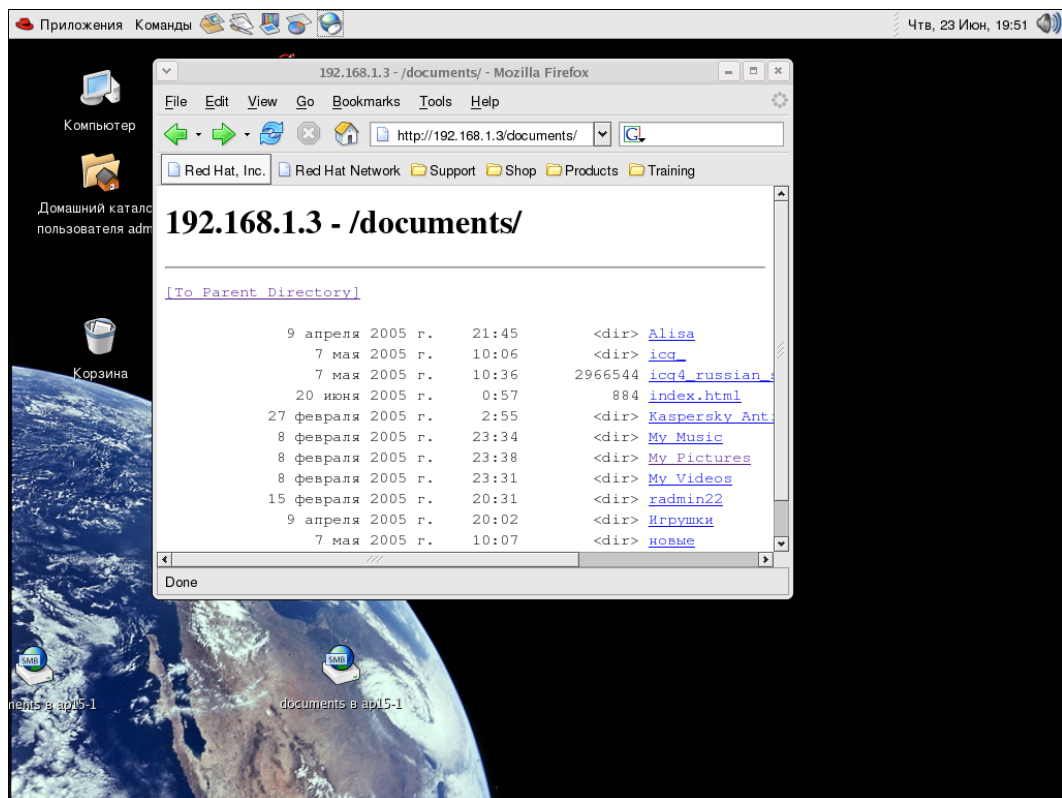


Рис. 6.5. Рабочий стол Linux с сетевой Web-папкой

Часто, ориентируясь на слухи, начинающие администраторы локальных сетей считают, что Linux намного совершеннее Windows, существенно стабильнее, 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.

В последнее время все больше пользователей Windows пытаются перейти на Linux XP, которую можно найти по ссылке <http://www.linux-online.ru>.

Это русифицированная версия Linux, полностью совместимая с Fedora. Она не совсем бесплатна, но за мизерную цену вы получаете поддержку в течение первого месяца, что позволяет разобраться с большинством проблем, связанных с установкой на вашем компьютере, если они возникнут.

Интерфейс этой системы максимально приближен к Windows XP, что позволяет быстро в нем освоиться пользователю Windows. Как можно видеть из рис. 6.6,

в системе можно использовать различные приложения, в том числе и клиента терминального доступа для Windows-сервера.

Это позволяет использовать компьютер с ОС Linux XP, как полноценную рабочую станцию в сети Windows.

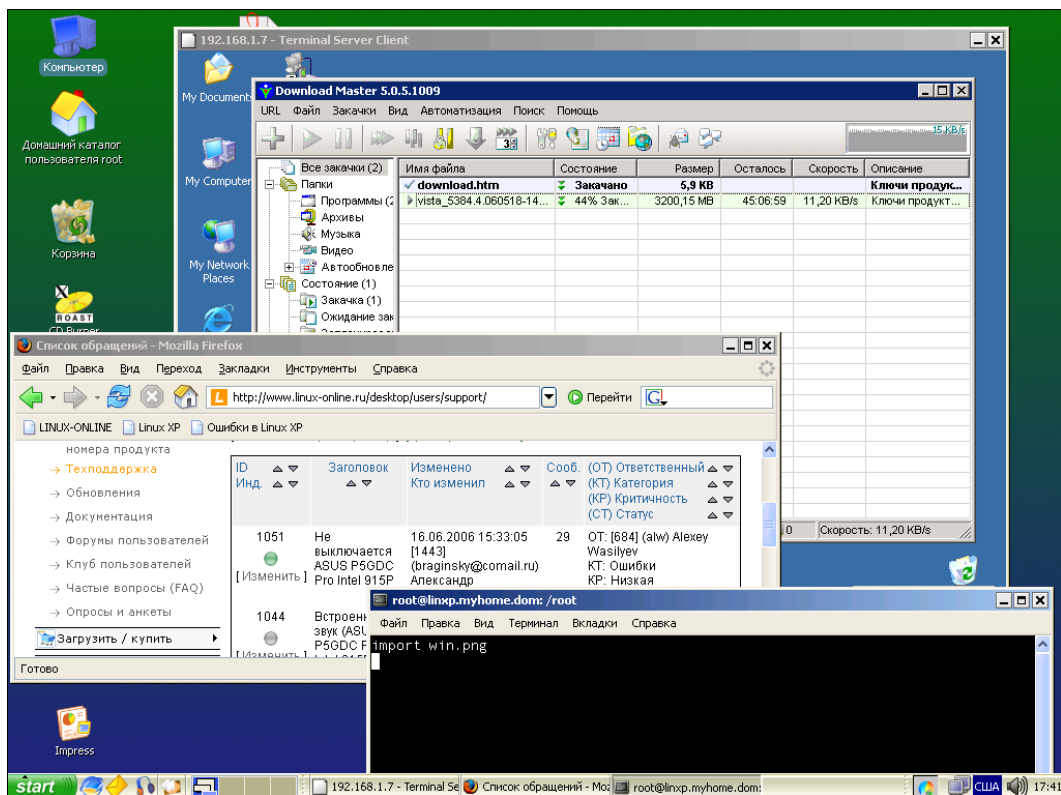


Рис. 6.6. Рабочий стол Linux XP с окнами приложений

## Некоторые замечания

Применение рабочих станций с не-Windows операционными системами может дополнить вашу сеть средствами достаточно безопасными и не дорогими.

Мало распространены вирусы, которые могут навредить DOS и Linux. Находясь в Интернете, вы можете быть уверены, что вирусы не просочатся через вашу рабочую станцию в сеть.

Возможно применение таких рабочих станций при создании рабочих мест с использованием более одного системного блока, что расширяет возможности такого рабочего места. Производительность и безопасность такой рабочей станции может быть повышена путем рационального использования ресурсов каждого системного блока. Как можно видеть на рис. 6.6, один из системных блоков занят загрузкой дистрибутива Windows Vista (окно 192.168.1.7 Terminal Server Client), а другой с

ОС Linux XP свободен для работы (основной экран). Экран любой системы доступен на мониторе благодаря применению терминального доступа или программ удаленного администрирования.

Программы удаленного администрирования доступны в Интернете как платные, Radmin, например, так и бесплатные по следующим ссылкам:

❑ <http://www.delphisources.ru/>;

❑ <http://berkutsoft.jino-net.ru/>.

Для DOS программу удаленного управления найти сложнее. Мне известно действующее на сегодняшний день предложение NetOp Remote for DOS, описание которой можно почитать на английском языке по адресу в Интернете [www.netop.com/media\(75,1033\)/NetOp\\_for\\_DOS\\_brochure.pdf](http://www.netop.com/media(75,1033)/NetOp_for_DOS_brochure.pdf).

Если в ваших архивах сохранились программы NetOp Remote for DOS или PCanywhere v5.0 for DOS, то их можно использовать.

О применении двух системных блоков, как одной рабочей станции, написано в статье по следующим ссылкам:

❑ <http://www.okobox.narod.ru/kompdist2.htm>;

❑ <http://www.okobox.narod.ru/kompdist1.htm>.

О других программах удаленного управления можно прочитать в статье <http://www.osp.ru/text/302/132197/>.







## ЧАСТЬ III

# Средства восстановления и повышения отказоустойчивости сети

Создавая сеть, есть смысл подумать заранее об отказоустойчивости и возможности восстановления компьютеров и серверов, их операционных систем. Задача обеспечения отказоустойчивости весьма обширна, и в больших сетях ее решение обычно связано с существенными финансовыми и материальными затратами. В малых сетях затраты меньше, но если пренебречь ими, можно попасть если не в катастрофическую, то весьма неприятную ситуацию. Даже переустановка системы и установка программ на рабочей станции после серьезного сбоя может занять пару дней вашего времени. Если предусмотреть хотя бы некоторые средства для повышения отказоустойчивости, можно надеяться, что вам не придется лихорадочно восстанавливать систему и пропавшие файлы именно в тот момент, когда они крайне необходимы.



## ГЛАВА 7



# Хранение данных, восстановление системы

Прежде чем что-нибудь восстановить, надо это разрушить. Нет, конечно, не надо, но случается, что система разрушается вопреки нашему желанию. Для того чтобы эта ситуация не застала врасплох, к ней надо готовиться заранее.

## 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 дисках CD-R удобно хранить дистрибутивы и данные, которые не будут изменены в обозримом будущем. Данные, которые могут меняться относительно часто, можно сохранять на дисках 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 данных. 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.

Согласно моему опыту, удобно процедуры архивирования и резервирования данных разбить на три группы.

1. Резервное копирование текущих данных.
2. Резервное копирование системы.
3. 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 излившихся 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 Xсору для копирования изменившихся данных.

## **Acronis True Image — резервное копирование всей системы**

Программа Acronis True Image 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.

<http://www.acronis.ru/enterprise/products/ATISWin/> — по этой ссылке можно найти всю информацию об этом продукте.

В качестве примера рассмотрим работу с одной из серверных версий, позволяющей делать резервные копии сервера (рис. 7.1).



Рис. 7.1. 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. 7.2).

Выбрав диск и/или раздел и нажав кнопку **Далее**, мы можем выбрать место сохранения архива (рис. 7.3). 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.

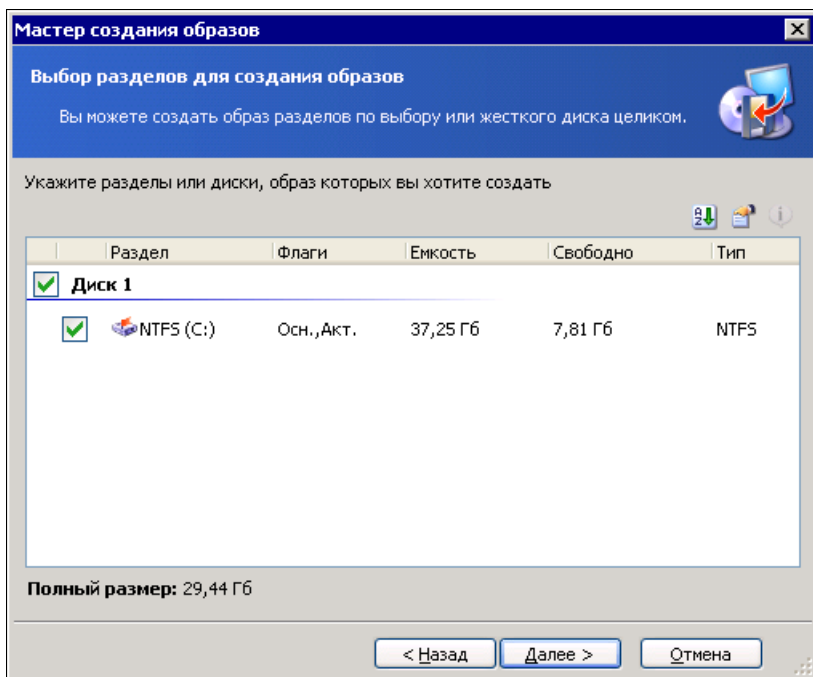


Рис. 7.2. Окно **Мастер создания образов** программы **Acronis True Image Server** (выбор разделов для создания образов)

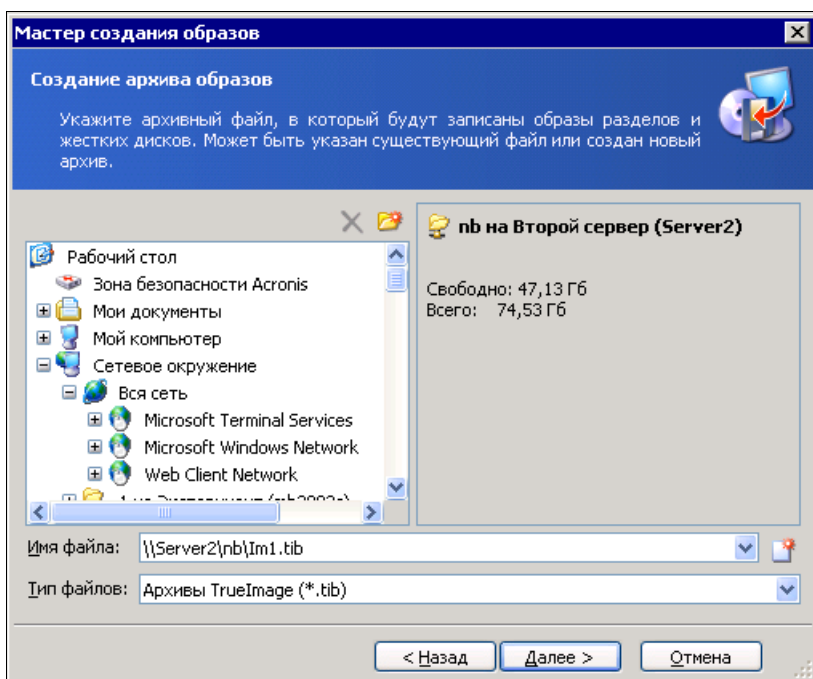


Рис. 7.3. Окно **Мастер создания образов** программы **Acronis True Image Server** (создание архива образов)

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. 7.4). 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 диски CD-R, размер файлов можно установить в соответствии с емкостью дисков.

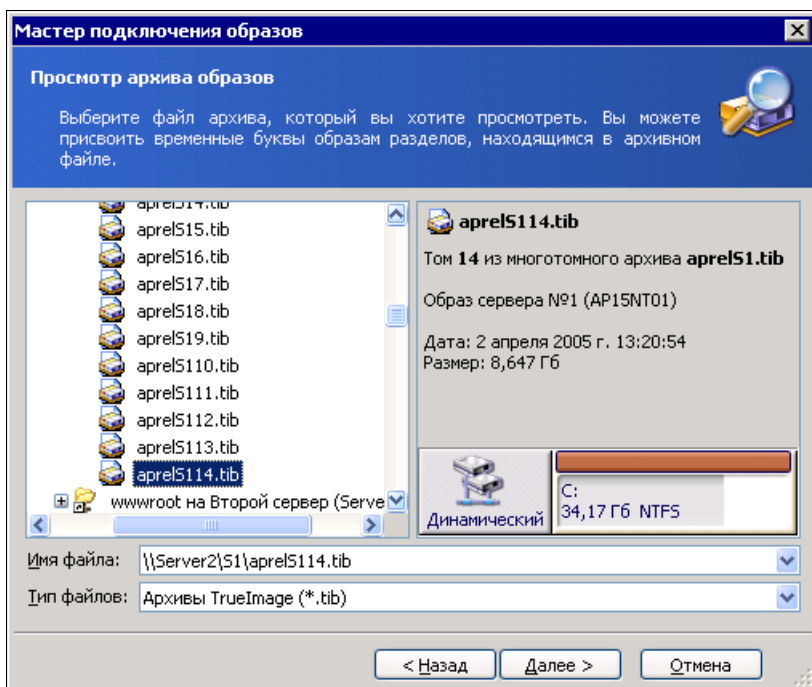


Рис. 7.4. Окно **Мастер подключения образов** программы **Acronis True Image Server** (просмотр архива образов)

Подключив образ, вы можете копировать файлы как с обычного сетевого диска (рис. 7.5).

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.

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.

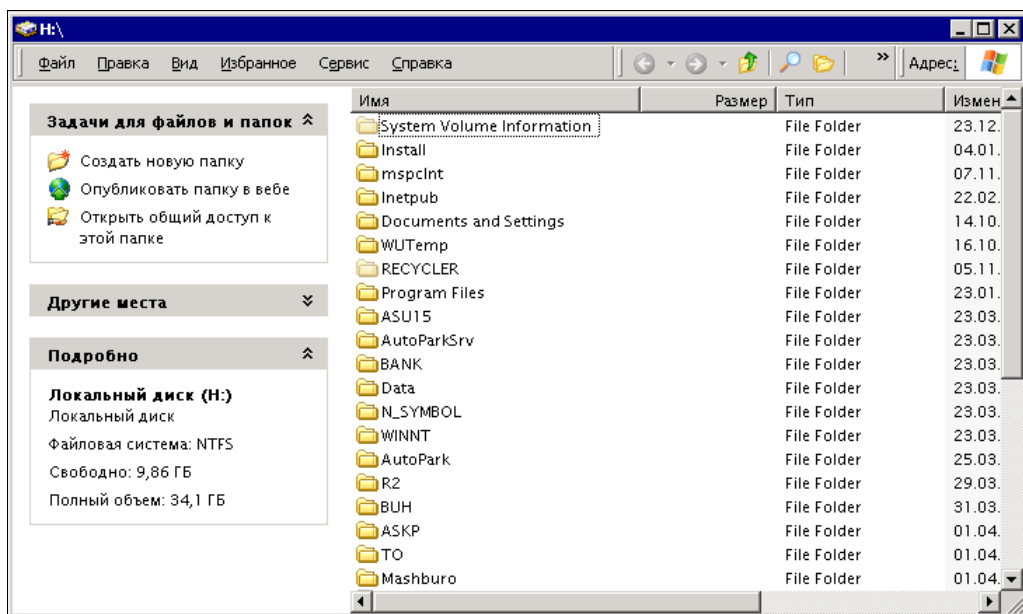


Рис. 7.5. Образ сервера, подключенный как сетевой диск

### 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.

В последних версиях программы появилась возможность работы с файлами и папками, делая резервные копии наиболее важных компонентов системы для их быстрого восстановления.

Подробнее описание работы с Acronis можно прочитать по адресу:

<http://www.thg.ru/software/20050127/index.html>.



В Интернете можно найти описание и других программ, предназначенных для восстановления системы. Но по личному опыту и отзывам в Интернете отечественная программа по многим параметрам превосходит зарубежные аналоги.

Описания работы с другими программами можно прочитать в Интернете:

**<http://www.thg.ru/software/20050518/index.html>**.

Создав образ диска системой, можно быть уверенным, что в случае серьезного сбоя вам удастся восстановить работоспособную систему со всеми программами и данными, актуальными на момент создания образа.

Дополнительно можно создавать копию важных данных с необходимой периодичностью.

## Средства Windows

Windows в своем составе обычно тоже содержит средства восстановления системы.

В составе этих средств обычно три программы:

- System Restore (Восстановление системы) — %SystemRoot%\System32\restore\rstrui.exe;
- Backup (Программа архивации) — %SystemRoot%\system32\ntbackup.exe;
- Remote Storage (Удаленное хранилище) содержится в средствах администратора системы Windows Server 2003 (устанавливается отдельно с диска Windows Server 2003).

Первая из этих программ позволяет создавать контрольные точки для восстановления системы. По этим контрольным точкам возможно восстановление состояния системы на момент создания контрольной точки.

Эта возможность может быть применена в случае проблем после установки программ или изменения параметров системы, которые привели к сбоям, но не катастрофическим. Система продолжает загружаться, но работает не так, как требуется.

Backup позволяет сделать резервную копию важных файлов. Это могут быть как системные, так и файлы данных. Наличие резервной копии может помочь восстановлению рабочего состояния системы после вынужденной переустановки или потери данных. В случае серьезных сбоев эти архивы могут использоваться для восстановления системы при загрузке в режиме восстановления (с оригинального дистрибутивного диска системы).

Чтобы создать набор аварийного восстановления системы с помощью программы архивации, выполните следующее:

1. Запустите приложение Backup (Программа архивации).
2. По умолчанию программа архивации запускается в режиме мастера, если этот режим не отключен.
3. Нажмите кнопку **Advanced** (Расширенный) в окне мастера архивации.
4. Выберите в меню **Сервис** команду **Мастер аварийного восстановления системы**.
5. Далее следуйте инструкциям, появляющимся на экране.

### ПРИМЕЧАНИЕ

Необходимо иметь наготове дискету емкостью 1,44 Мбайт для сохранения параметров системы и носитель для хранения файлов архива.

Remote Storage позволяет выбрать удаленное хранилище, в котором можно поместить архивы системы или данных. В случае нарушения работы системы в результате сбоя, но при сохранении связи с сетью можно использовать сохраненные в удаленном хранилище файлы для восстановления работы системы.

Все описанные средства можно применять комплексно. В зависимости от конкретной ситуации каждое из этих средств может обладать преимуществами или особенностями, которые становятся решающими при выборе того или иного средства восстановления системы или важных файлов. Программа архивации рассчитана на применение внешних запоминающих устройств на магнитной ленте, но это не мешает выбрать любой накопитель, доступный в момент архивации. Если выбран сетевой каталог или удаленное хранилище, то в отдельных случаях, когда сбой привел к недоступности сети, может потребоваться копирование файлов архива на носитель, который можно подключить к восстанавливаемому компьютеру.

## Используем консоль восстановления

Это средство администратора, всегда входящее в дистрибутив Windows XP, очень часто применяется пользователями и начинающими администраторами. Тем не менее, консоль восстановления может принести немалую пользу, если заранее подготовиться к ее применению в случае необходимости. Собственно в сети с этим инструментом делать нечего, но если компьютер (сервер) отказался загружаться, или потерян доступ к разделам винчестера, содержащим важные данные, то восстановить работоспособность компьютера вполне возможно. При этом, восстановив загрузку в режиме командной строки, вы уже можете использовать возможности сети.

Например, если при редактировании файла boot.ini, в котором описан порядок запуска операционных систем, установленных на компьютере, вы допустили серьезную ошибку, то компьютер Windows XP не загрузится. Консоль восстановления позволяет заменить испорченный файл сохраненной копией или даже файлом с другого компьютера.

## Консоль восстановления в загрузочном меню

Несмотря на то, что консоль восстановления может быть загружена с дистрибутивного компакт-диска Windows XP, лучше установить ее в качестве одной из операционных систем, которую можно выбрать из загрузочного меню.

Чтобы установить консоль восстановления в виде варианта загрузки, необходимо установить ее на локальный компьютер. Для этого достаточно во время работы Windows XP вставить установочный компакт-диск, нажать кнопку **Пуск**, выбрать команду **Выполнить** и ввести следующую строку:

```
D:\i386\winnt32.exe /cmdcons
```

где D: — привод компакт-дисков. После того как программа установки завершит работу, в корне загрузочного раздела появится каталог `\cmdcons` объемом чуть меньше 8 Мбайт.

Если заранее не позаботиться, то в критической ситуации вы сможете получить доступ только к папке `Windows`. Чтобы работать со всем диском, следует выполнить некоторые действия, пока система исправна: **Пуск | Выполнить**, и ввести строку:

```
secpol.msc /s
```

Далее в локальных политиках (параметры безопасности) необходимо включить политику **Recovery console: Allow floppy copy and access to all drivers and all folders** (Консоль восстановления: разрешить копирование дискет и доступ ко всем файлам и папкам). При желании можно включить и политику **Recovery console: Allow automatic administrative logon** (Консоль восстановления: разрешить автоматический вход администратора). Это избавит вас от ввода пароля администратора в каждом сеансе работы с консолью. Но будьте осторожны при выборе данного параметра. Его выбор позволит каждому, кто имеет физический доступ к компьютеру, загрузить консоль восстановления и получить доступ к командам консоли восстановления.

После входа в консоль восстановления следует выполнить одну из команд, полный перечень которых приведен далее в следующем разделе.

Команда, которой необходимо воспользоваться, — это `set`. С ее помощью настроим переменные среды консоли:

```
set allowallpaths = true
set allowremovablemedia = true
set allowwildcards = true
```

Эти три команды следует вводить в каждом сеансе работы с консолью, т. к. после выхода переменные среды, определяющие возможность записи на все диски и каталоги, включая съемные, устанавливаются в состояние по умолчанию, т. е. в "false".

Следует заметить, что команды консоли восстановления отличаются от аналогичных в командной строке `Windows`. Кроме того, во время работы Консоли восстановления нет файлов, которые используются `Windows`. Все это дает некоторые преимущества и свободы. Например, в `Windows` невозможно удалять созданные разделы на дисках, в том числе на съемных носителях. Через Консоль восстановления вы можете подготовить `Flash Drive` для использования в качестве загрузочного, сформировав необходимые разделы и логические диски.

## Основные команды Консоли восстановления

Функциональные возможности Консоли восстановления ограничены; она предоставляет только интерфейс командной строки и поддерживает лишь команды, представленные в табл. 7.1.

Таблица 7.1. Команды Консоли восстановления

Команда	Описание команды
attrib	Позволяет изменить некоторые атрибуты файлов: установить или сбросить атрибуты "только чтение", "скрытый" и "системный"
batch	Позволяет выполнить последовательность команд Консоли восстановления, сохраненную в текстовом файле. Требуется указания как имени, так и расширения файла. Позволяет также указать имя выходного файла
chdir (cd)	Действует аналогично команде DOS <code>cd</code> , назначая указанный каталог текущим, при отсутствии параметра выводит на экран обозначение текущего рабочего каталога
chkdsk	Действует аналогично команде DOS <code>chkdsk</code> . Позволяет указать два ключа: /p — разрешает проверку диска даже при установленном флаге "грязный"; /r — заставляет <code>chkdsk</code> исправлять любые найденные дефектные секторы
cls	Действует аналогично команде DOS <code>cls</code> — очищает экран
copy	Копирует файл. Если файл сжат, в процессе копирования он распаковывается. Команда <code>copy</code> не допускает использования шаблонов групповых операций. Ключи отсутствуют
delete (del)	Действует практически так же, как и команда DOS <code>delete</code> . Удаляет указанный файл или файлы
dir	Действует аналогично команде DOS <code>dir</code> . Выводит на экран имена файлов и подкаталогов указанного каталога. Не имеет ключей. Выводит размеры файлов, их даты и атрибуты
disable	Используется для блокирования службы или драйвера устройства. Блокированные служба или драйвер получают метку <code>SERVICE_DISABLED</code> , что предотвращает их запуск после перезапуска системы
diskpart	Контролирует разделы на дисковых устройствах. Позволяет добавлять или удалять разделы. При добавлении раздела параметры команды задают размер раздела в мегабайтах
enable	Используется для разблокирования службы или драйвера устройства. Разблокируемой службе (или драйверу) придается указанный пользователем тип службы: <code>SERVICE_AUTO_START</code> , <code>SERVICE_DISABLED</code> , <code>SERVICE_DEMAND_START</code> , <code>SERVICE_BOOT_START</code> или <code>SERVICE_SYSTEM_START</code>
exit	Завершает сеанс работы Консоли восстановления и перезагружает компьютер
expand	Действует аналогично команде DOS <code>expand</code> . Распаковывает файлы, извлекая их из исходного файла CAB. С командой используются два ключа: /d — выводит содержимое файла CAB; /y — подавляет возможные предупреждающие сообщения о затирании имеющихся файлов
fixboot	Исправляет или заменяет сектор загрузки указанного (необязательно) диска
fixmbr	Исправляет или заменяет главную загрузочную запись указанного (необязательно) диска
format	Действует аналогично команде DOS <code>format</code> . Форматирует диски, использующие системы FAT, FAT32 и NTFS. Единственный ключ /q определяет быстрое форматирование без проверки поверхности диска. Это допускается, если диск заведомо исправен

Таблица 7.1 (окончание)

Команда	Описание команды
help	Выводит список доступных команд Консоли восстановления
listsvc	Выводит список служб и драйверов, доступных в текущей конфигурации компьютера
Logon	Запускается автоматически при первом запуске Консоли восстановления. Используется для входа в систему Windows NT, Windows 2000 и Windows XP
Map	Используется для вывода на экран списка отображения всех дисков
mkdir (md)	Действует аналогично команде DOS <code>md</code> ( <code>mkdir</code> ). Позволяет создавать каталоги внутри системного каталога текущей конфигурации, сменных дисков, корневых каталогов разделов жесткого диска и каталога локальной установки
more	Действует аналогично команде DOS <code>type</code> . Выводит на экран содержимое файла. Параметров не имеет
rename (ren)	Позволяет пользователю переименовать файл. Не поддерживает шаблоны групповых операций
rmdir (rd)	Действует аналогично команде DOS <code>rd</code> ( <code>rmdir</code> ). Удаляет каталоги в системном каталоге текущей конфигурации, на сменных дисках, в корневых каталогах разделов жесткого диска, а также в каталогах локальной установки
set	Консоль восстановления поддерживает ограниченный набор переменных среды. Эти переменные влияют на работу только самой Консоли восстановления
systemroot	Объявляет текущим каталог <code>%systemroot%</code> текущей конфигурации. Функционально эквивалентна команде <code>cd %systemroot%</code> в обычном сеансе DOS
type	Действует аналогично команде DOS <code>type</code> . Выводит на экран содержимое файла. Параметров не имеет

Поскольку переключение раскладки клавиатуры после загрузки не предусмотрено, команды, содержащие кириллические имена файлов, можно указывать в заранее подготовленном текстовом файле. Для выполнения таких команд следует воспользоваться командой `batch`.

Формат этой команды такой:

```
batch c:\<Имя_файла_с_командами> c:\ <Имя_файла_вывода_результата>
```

Если файл вывода результата команд не указать, то вывод будет осуществляться на экран.

Конкретные случаи применения Консоли восстановления рассматривать не будем, поскольку стандартных аварийных ситуаций не бывает. Каждый раз приходится подходить к решению задач творчески. Но, пока не грянул гром, установите на своих компьютерах Консоль восстановления и "поиграйте" с ней. Хорошо, если не пригодится, но всякое может случиться... Во всяком случае, когда невозможно загрузить систему, у вас есть средство доступа к файлам системы, возможность заменить тот или иной файл, если вам известно, что он испорчен и не позволяет загрузиться системе.

Более подробно о Консоли восстановления можно прочитать по ссылкам, использованным при подготовке этой главы:

- <http://www.computerra.ru/softerra/35993/>;
- <http://winall.ru/xp/consol.shtml>;
- <http://www.windowsfaq.ru/content/category/3/14/37/>;
- <http://www.windowsfaq.ru/content/category/3/19/57/>.

## Сохраняем важные данные

В какой-то степени материал этой главы перекликается с материалами *глав 2 и 6*. Но данные приходится сохранять не только для восстановления работоспособности системы. Сохранение данных требуется и для возможности обращения к ним, когда такая необходимость появится. Например, сохраняя файлы перед их изменением, вы можете вернуться к более старой версии файла, если оказалось, что изменения привели к нежелательному результату. Сохранять версии файлов необходимо при разработке программ, больших текстовых произведений, графических работ. Если работа над файлами ведется коллективно, то сохранение версий должно проводиться в сети.

Существуют специализированные программные средства для выполнения резервного копирования файлов, но они часто требуют много ресурсов компьютера, работают не быстро. Кроме того, команды командной строки позволяют "лепить" процесс по своему усмотрению, что делает его наиболее подходящим именно вам.

Во всяком случае, именно существование команды `xcopy` не позволило мне упасть духом, когда половина этой книги была написана, а Windows на моем рабочем компьютере "приказала долго жить".

## Копирование данных в сетевой каталог

Один из наиболее простых способов сохранения файлов в сети — применение команды `xcopy`. Команда имеет множество параметров, которые позволяют сделать ее работу интеллектуальной. Работая с большим числом файлов, нет необходимости копировать уже скопированные и не изменившиеся, поскольку это отнимает время и ресурсы компьютера. В то же время новые и измененные файлы должны быть скопированы. Для копий следует создать доступный в сети каталог, а саму процедуру копирования можно запускать автоматически с помощью планировщика Windows.

### Команда `Хcopy`

Команда `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 выполняться анализ копируемых файлов, анализ уже существующего архива, а в зависимости от результатов анализа могут осуществляться те или иные действия.

xcopy, несмотря на свою кажущуюся простоту, команда интеллектуальная, что позволяет использовать ее 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 команду `xcopy` в целях создания резервного архива данных, посмотрите листинг 7.1, в котором приведены команды, необходимые для этой процедуры. Это настоящий пакетный файл, работающий в реальной сети. Вам потребуется только изменить пути к файлам, чтобы заставить его работать в вашей сети.

#### Листинг 7.1. 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 команды останавливается. Это возможно благодаря тому, что команда `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 `xcopy` находятся в параметрах, указанных через слэш ("/) после самой команды.

Приведем описания параметров, которые использованы в файле `CopyData.bat` (листинг 7.1).

- ❑ `/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 7.2).

#### Листинг 7.2. 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.

Подобным образом можно создать командный файл для копирования файлов, с которыми вам приходится работать ежедневно и копии которых должны быть доступны другим пользователям сети.

Нет ничего приятного в ситуации, когда несколько дней работы над важным для вас материалом пропадают впустую из-за проблем с Windows или ваших неосторожных действий. Если команду `xcopy` запускать с помощью планировщика Windows, то копирование может осуществляться по расписанию каждый день или чаще. Лучше, если копирование планируется на время простоя компьютера.

Аналогично копируются важные системные файлы или вся система. Составив разумное расписание резервного копирования, вы всегда будете иметь копии важных файлов, которые позволят оперативно провести восстановление при сбоях или переустановке системы.

## Копирование настроек

Скопировав файлы, вы можете быть уверены, что не пропадет важная информация. Но если случилась неприятность, и пришлось переустановить систему, то требуется достаточно много времени, чтобы восстановить настройки системы. Ведь вы настраивали ее не сразу, кое-что забыли записать, и при восстановлении придется вспоминать что и как вы настраивали. Но кроме файлов можно копировать и настройки системы! Настройки системы и приложений сохраняются в системном реестре и в файлах, поэтому необходимо найти все ключи реестра, содержащие необходимые настройки и файлы. Пример командного файла, который позволяет скопировать все необходимые настройки, приведен в листинге 7.3. При повторении этого файла следует учесть, что команды должны записываться одной строкой.

### Листинг 7.3. Файл CopySett.bat

```
@ECHO OFF
REM === Программы ===
REM Настройки Internet Explorer

REGEDIT /EA D:\BACKUP\Registry\hkcu\
InternetExplorer.reg "HKEY_CURRENT_USER\
Software\Microsoft\Internet Explorer"
```

REM Там, где есть пробелы, обязательно ставим кавычки

REM Основной шаблон Word

```
XCOPY "C:\Program Files\Text\Editors\MS Word7\
normal.dot" D:\BACKUP\
```

REM Список автозамены Word – файл с расширением ACL

```
XCOPY C:\WINNT\User000.acl D:\BACKUP\
```

REM Пользовательский словарь Word

```
XCOPY "C:\Program Files\Text\Editors\MS Word7\
custom.dic" D:\BACKUP\
```

...

REM === Системные файлы ===

REM Адресная книга

```
XCOPY "C:\Documents and Settings\Administrator\
Application Data\Microsoft\Address Book\
Administrator.wab" D:\BACKUP\
```

REM Избранное Internet Explorer

```
XCOPY "C:\Documents and Settings\Administrator\Favorites\*.*" ↵
D:\BACKUP\Favorites\ /E
```

...

REM === Рабочие файлы ===

```
XCOPY D:\LANGUAGES\ENGLISH\Vocabulary\*.xls D:\BACKUP\
```

...

```
XCOPY "D:\LANGUAGES\ENGLISH\English Grammar.rtf" D:\BACKUP\
```

Подразумевается, что после каждой команды XCOPY стоит комбинация ключей /C /D /H /R /Y, а ключ /E указан там, где нужно. Ключ /EA после команды REGEDIT предписывает сохранение REG-файлов без лишних вопросов и в формате ANSI, а не UNICODE (чтобы не иметь трудностей при открытии этих файлов редакторами, не поддерживающими UNICODE).

Реальный файл экспорта настроек может быть довольно большого размера, но написав его один раз, можно быть спокойным, что восстановление настроек займет немного времени.

## Настройки Outlook Express

Отдельно следует рассмотреть сохранение настроек почтовой программы.

Запустите редактор реестра Windows REGEDIT (**Пуск** | **Выполнить** | regedit | <Enter>). Найдите строку HKEY\_CURRENT\_USER\Identities\{набор букв и цифр}\Software\Microsoft\Outlook Express (набор цифр может иметь примерно такой вид: {7173EFE5-2BF8-4886-BD21-75FB4B7D3562}). Выделите ее и нажмите в меню редактора

реестра **Registry** | **Export registry file** (Файл | Экспорт). Выбираем, где сохранить (в качестве имени файла желательнее выбрать именно этот набор цифр — для этого нажмите клавишу <F2>, <Ctrl>+<C>), в каком формате (зависит от операционной системы), и нажимаем <Enter>. В указанном каталоге появится REG-файл.

Теперь можно спокойно переустанавливать Windows. По окончании заглядываем в реестр, копируем в буфер обмена новый "набор цифр и букв" и открываем экспортированный ранее REG-файл с помощью текстового редактора. В нем производим глобальную замену старого набора букв и цифр на новый, сохраняем и закрываем. Потом выполняем двойной щелчок по нему и нажатие кнопки **ОК**. Все, ваши фильтры (и все остальные настройки Outlook Express) на месте!

При переустановке серверной операционной системы сохраненные файлы и ключи реестра позволят оперативно восстановить все настройки, восстановление которых вручную может потребовать не одного дня.

О сохранении данных реестра, конфигурационных файлов и файлов данных можно почитать по следующим ссылкам:

- ❑ [http://www.security.nnov.ru/articles/xs/backup\\_implementation.asp](http://www.security.nnov.ru/articles/xs/backup_implementation.asp);
- ❑ <http://www.windowsfaq.ru/content/view/299/60/>;
- ❑ <http://offline.computerra.ru/1998/247/1317/>;
- ❑ <http://www.igorkalinin.com/articles/backup.ru.html>.

Возможно, что вместо *хсору* вы будете использовать программу *nnBackup*. Эта программа имеет целый ряд особенностей, описание которых может занять очень много места. Создана она специально для резервного копирования файлов и синхронизации каталогов. В Интернете по адресу [http://www.nncron.ru/index\\_ru.shtml](http://www.nncron.ru/index_ru.shtml) есть описание программы на русском языке. Там же можно загрузить саму программу. Программа бесплатна, но требует регистрации на сайте.

## Настройки Mozilla Thunderbird

Эта рекомендация относится к рабочим станциям под Linux. Mozilla Thunderbird — один из распространенных почтовых клиентов для Linux (есть и версии для Windows). В Linux нет реестра. Все настройки программ для текущего пользователя хранятся в его папке. Только настройки программ хранятся в скрытых папках, которые в Linux первым символом в имени имеют точку. Включив отображение скрытых файлов или просто открыв свой каталог в файловом менеджере Midnight Commander, который вызывается в окне терминала командой *mc*, вы увидите папку *.mozilla-thunderbird* или просто *.thunderbird* с точкой впереди имени. В этой папке и хранятся настройки программы и письма. Достаточно сохранить этот каталог перед переустановкой системы, чтобы потом быстро восстановить письма и настройки программы. Точно так же можно поступать практически со всеми программами в Linux.

## ГЛАВА 8



# Обеспечиваем бесперебойное питание

Если домашнему пользователю не часто приходится сталкиваться с проблемой бесперебойного питания, а перерывы в электроснабжении не приводят к серьезным проблемам и убыткам, то в сети вопрос надежности электроснабжения может стоять очень остро. Особенно важно обеспечить бесперебойное питание для сервера и рабочих мест, для которых недопустимы перерывы в работе независимо от обстоятельств. Представьте себе, что на рабочем месте авиадиспетчера произошел сбой питания, и диспетчер не смог довести авиалайнер до посадочной полосы... В домашних сетях, конечно, таких ответственных мест нет, но тоже не очень приятно получать жалобы от пользователей, потерявших доступ к Интернету из-за временного перерыва электроснабжения сервера или коммуникационного оборудования. Если для обычных домашних компьютеров и рабочих станций не сложно организовать бесперебойное питание, применив любой стандартный *источник бесперебойного питания* (ИБП), то для обеспечения комплекса оборудования, которое включает в себя два сервера или более, решение задачи не так просто, как может показаться на первый взгляд.

## Бесперебойное питание для двух серверов

Задача состоит в следующем:

1. Необходимо обеспечить питание серверов и коммутационного оборудования в условиях нарушения основного электроснабжения. При этом сервер должен работать максимально возможное время, а затем корректно отключиться.
2. До отключения сервера системный администратор должен получить уведомление о выключении сервера.
3. После восстановления работы электросети запуск всего оборудования должен быть достаточно простым, чтобы не обладающий специальными знаниями и навыками сотрудник мог включить всю систему.
4. Необходимо максимально упростить и стандартизировать программную составляющую системы обеспечения бесперебойного питания, чтобы изменения в со-

ставе аппаратных средств не повлияли на ее работоспособность, а цена ее должна быть минимальной.

Такая задача может возникнуть в сети любого назначения. Но если крупные предприятия имеют возможность приобретать достаточно дорогостоящие аппаратные и программные средства, то в мелких и средних организациях нередко есть определенные трудности при выделении средств на эти цели.

## Существующие решения

Поиски в Интернете пригодного для применения в небольшой компьютерной сети решения к успеху не привели. *PowerChute Pluss* — практически единственное приложение, позволяющее решить поставленную задачу. Цена комплекта программ *PowerChute Pluss* — несколько десятков долларов. Тем не менее, если не надеяться на то, что все будет решено авторами программы, приложить немного своей настойчивости и подумать над собственными возможностями, можно получить практически бесплатное решение, которое удовлетворит многих системных администраторов. Описываемое далее решение было применено автором в реальной сети и работает до настоящего времени.

Упрощенная схема организации бесперебойного питания серверов показана на рис. 8.1. Здесь приведены лишь основные связи, обеспечивающие собственно резервное питание. Не показаны на рисунке пути передачи служебных сообщений.

Несмотря на разнообразие типов ИБП, разработчикам ОС Windows удалось создать стандартный интерфейс для настройки взаимодействия ИБП и компьютеров. Этот интерфейс объединен с апплетом **Электропитание** в панели управления. 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.



Рис. 8.1. Организация бесперебойного питания серверов

Время после подачи первого предупреждающего сигнала для оповещения администратора о возможном отключении сервера должно оставлять возможность до окончательного отключения предпринять какие-либо действия, например запустить генератор.

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. 8.2).

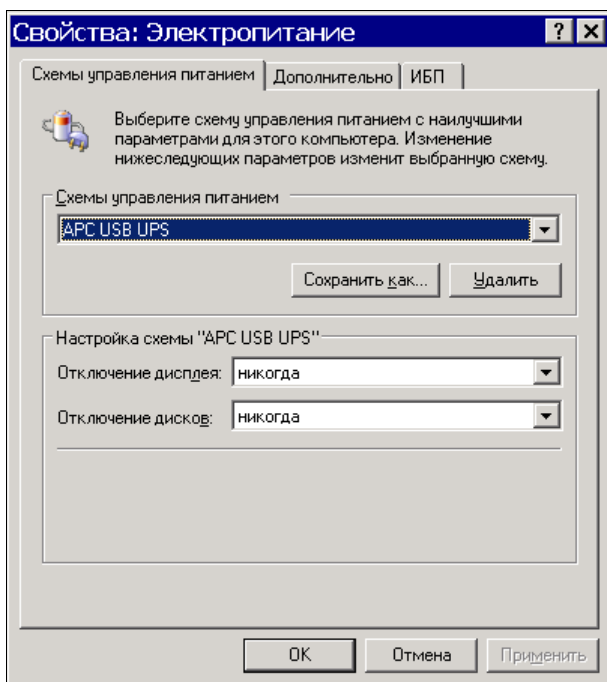


Рис. 8.2. Окно **Свойства: Электропитание**, вкладка **Схемы управления питанием**

Для корректной работы ИБП необходимо настроить параметры его взаимодействия с сервером. Для этого на вкладке **ИБП** (рис. 8.3) следует нажать кнопку **Настроить**. Откроется окно **Настройка ИБП** (рис. 8.4). В этом окне можно выбрать подходящий нам режим взаимодействия ИБП с сервером.

Рассмотрим режим, который применяется в моей сети. При этом в окне **Настройка ИБП** должен быть установлен флажок **Включить все уведомления**. В следующих двух полях устанавливаем интервалы времени между неполадкой и первым уведомлением, между уведомлениями, если сбой питания продолжается достаточно долго. Эти уведомления выводятся 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.

Далее настраиваем режим работы после достижения критической величины разряда аккумуляторов. В этот момент должен быть подан критический сигнал. Значе-

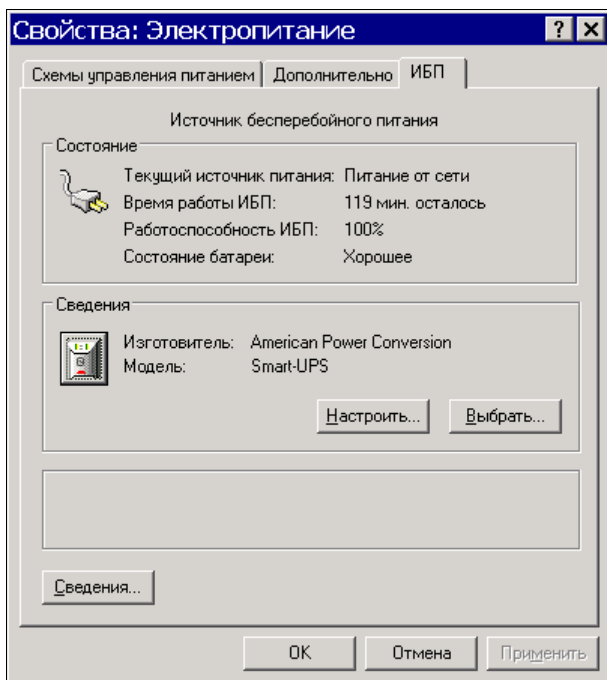


Рис. 8.3. Окно **Свойства: Электропитание**, вкладка **ИБП**

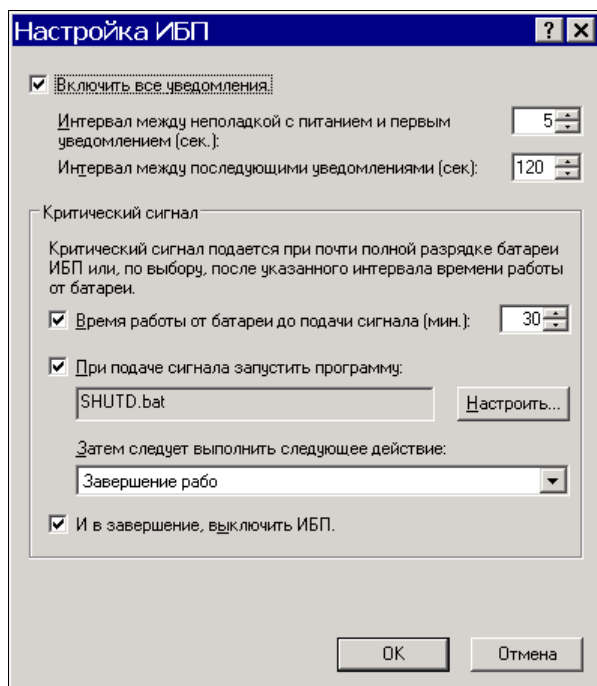


Рис. 8.4. Настройка ИБП



ние поля **Время работы от батареи до подачи сигнала (мин.)** устанавливаем в зависимости от возможностей нашего ИБП. Следует экспериментально 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. 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.

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 8.1.

#### Листинг 8.1. 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 8.2).

**Листинг 8.2. 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 файла 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 8.3).

**Листинг 8.3. 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.

Выполнив все указанные настройки, вы всегда будете проинформированы о критических ситуациях, связанных с электропитанием в вашей сети. Учитывая, что выключение второго сервера происходит по команде, переданной с компьютера, к которому непосредственно подключен интерфейсный кабель ИБП, вы можете передавать команды и на другие компьютеры сети. Возможна запись всех команд в журнальные файлы, выполнение каких-либо операций в сети перед выключением сервера, если это необходимо. В описанном примере используется ИБП APC Smart-UPS 2200, но возможно применение практически любых источников бесперебойного питания. Важно лишь, чтобы ИБП имел USB- или COM-порт для связи с компьютером. Само собой разумеется, что мощность источника должна быть достаточной для обеспечения потребностей всего подключенного к нему оборудования.

### **ЗАМЕЧАНИЕ**

Несмотря на простоту, универсальность и дешевизну, этот вариант организации бесперебойного питания имеет некоторые недостатки. Например, в отличие от PowerChute Pluss у нас нет средств для контроля параметров окружающей среды или мониторинга уровня напряжения в сети электропитания. Если вам необходимы эти возможности, придется купить PowerChute Pluss или приобрести ИБП с дополнительными картами, позволяющими организовать контроль различных параметров и передачу сообщений... или еще немного подумать самостоятельно.

Более подробно ознакомиться с возможностями различных моделей ИБП, прилагаемого к ним программного обеспечения, а также с отзывами о них можно по следующим ссылкам:

- ❑ <http://forum.ippon.ru/viewforum.php?f=2>;
- ❑ <http://www.bytemag.ru/?ID=604273>;
- ❑ <http://forums.overclockers.ru/viewforum.php?f=26>.





## ЧАСТЬ IV

# Сетевые серверы

В этой части будут рассмотрены советы по установке и настройке серверов различного назначения. Сервер серверу — рознь. Кому-то необходим серьезный центр управления сетью, другому нужен файловый сервер для хранения информации, а кто-то решил организовать студию видео- и аудиовещания. Все варианты применения сервера в сети, пожалуй, перечислить очень сложно. Создавая сеть, планируя сервер в сети, необходимо подходить к этому делу творчески. Никакие руководства не дадут вам полной информации о настройках именно вашего сервера в вашей сети. Вариантов так много, что процесс настройки сервера и сети можно сравнить с искусством, а настроенный сервер — с произведением искусства. Поэтому не пренебрегайте информацией, приведенной в предыдущих главах. И правильно организованное питание, и возможность восстановить неожиданно отказавшую машину помогут сохранить нервы и сберечь массу времени. Кроме того, произведение искусства повторить невозможно. Любая копия — это только копия. Даже в такой логически стройной системе, как операционная система сервера, возможно множество нюансов в настройках. Иногда на результат влияет даже последовательность проведения каких-либо операций, что не всегда можно объяснить с точки зрения логики. Поэтому каждый сервер, если это не просто стандартно настроенная машина, несет в себе отпечаток характера системного администратора. Холодное железо согрето душой человека и ведет себя иногда подобно этому человеку.



## ГЛАВА 9



# Выбираем операционную систему

На первый взгляд и выбирать-то здесь нечего. *Сервер* — значит серверная операционная система. Обычно это Windows Server 2008, Windows Server 2003 или Windows 2000 Server.

Но задачи сервера могут быть столь специфичны или средства столь ограничены, что сам по себе выбор ОС ("операционки") для сервера может стать творческим процессом. Предположим, что вам необходим FTP-сервер. Можно просто установить одну из современных Windows-систем, можно применить Linux, если есть опыт общения с этой системой, а можно использовать и почти забытую DOS. Последний вариант позволит использовать пылящуюся в кладовке старую машину, которая не в состоянии работать с современными ОС. Но нам требуется только FTP-сервер. Не нужен офис, не нужны игры, просто нужно хранить файлы, которые могут быть доступны по сети. А с этим может справиться и старая, уже никому не нужная машина. С другой стороны, если необходима высокая производительность сервера, если предполагается хранение больших объемов информации, если требуется серьезная защита информации и сложный учет прав пользователей, контроль за действиями пользователей, высокая надежность сервера, то без современной операционной системы и мощного компьютера не обойтись. Попробуем разобраться в наших потребностях и возможностях.

## Операционная система для сервера

Итак, нам нужна операционная система для сервера. Сервер, работающий в сети, должен предоставлять сервисы рабочим станциям. А задача администратора сети — выбрать решение, которое удовлетворит запросы пользователей сети. ОС Windows Server 2008, совсем недавно выпущенная корпорацией Microsoft, пока еще не обкатана пользователями, и мы не будем ее рассматривать. Преимущества этой системы перед ее предшественницами в основном должны быть заметны в крупных сетях. Применительно к малым сетям есть более десятка других операционных систем для серверов, которые рекомендуют специалисты. Но, рассматривая локальную сеть, как объект творчества системного администратора (даже если ваша сеть у вас

дома, вы ее системный администратор), мы не будем подходить к этому вопросу стандартно. По адресу

**[http://www.opennet.ru/base/sys/weekend\\_onet.txt.html](http://www.opennet.ru/base/sys/weekend_onet.txt.html)**

можно прочитать статью автора под псевдонимом WintiX "Установка FreeBSD на домашнем компьютере (freebsd install rus)". Возможно, она пригодится вам, если вы решите устанавливать на свой компьютер FreeBSD. Но в данный момент нас интересуют рекомендации автора по выбору операционной системы и описание особенностей различных ОС.

Из опыта автора статьи следует, что все доступные для ПК операционные системы можно поделить на три класса. К третьему классу относятся все разновидности DOS и Windows 95/98 — эти ОС загружаются только с первого раздела первого винчестера, т. е. с диска C:. Ко второму классу относятся ортодоксальные UNIX-системы (FreeBSD, NetBSD, QNX RTP). Они загружаются с любого раздела, но о расширенном разделе не хотят ничего знать. Системы первого класса наиболее дружелюбны и загружаются из любого раздела любого диска: Windows NT, Windows 2000, Windows XP, Windows Server 2003, BeOS, Linux.

Приняв для себя такую классификацию операционных систем, можно сделать вывод, что для домашней (квартирной) сети, а также для сети малого офиса, где наиболее вероятно применение нескольких операционных систем на одном компьютере, наибольшее предпочтение следует отдать Windows, начиная с Windows NT или Linux. Из Linux мной были опробованы Fedora Core 3, Fedora Core 5, а также Linux XP и Mandriva Linux 2008, которые наилучшим образом русифицированы. Эти системы вполне могут работать в качестве серверных в небольших сетях, но все же на настоящий момент Windows 2000 Server и Windows Server 2003 наиболее близки к идеальной серверной операционной системе, причем не только для малого офиса. Стабильность Windows Server 2003 настолько высока, что вполне может сравниться с Linux. Тем не менее есть ситуации, когда Linux окажется вне конкуренции. Если по каким-то причинам нет возможности применить хорошую антивирусную программу в виду ее несовместимости, например с какими-либо приложениями, а также при невозможности использовать дорогое лицензионное программное обеспечение под Windows, вы сможете найти много бесплатных или почти бесплатных приложений для Linux-сервера. Обычно комплект таких приложений входит в дистрибутив, который можно скачать с сайтов в Интернете. Вирусов для Linux почти не пишут, а стоимость всего комплекта необходимых серверных приложений окажется неизмеримо ниже, чем аналогичных программ под Windows. Правда, следует учесть, что в наше время появляется множество разработок с открытым кодом и часто бесплатных для Windows.

Единственный реальный недостаток Linux-систем — это отсутствие стандартов, подобных тем, что применяются в Windows-системах. А отсюда сложность обслуживания системы, ее администрирования, особенно для тех пользователей, которые работали только с Windows. О Linux написано много статей и книг. При желании можно освоить эту систему и достаточно квалифицированно с ней работать, но пока ОС Windows наиболее распространена, понятной для начинающих информации о ней существенно больше. Поэтому, если вам требуется в минимальные сроки установить сервер и развернуть сеть, Windows предпочтительней. Лучшим выбо-



ром будет Windows 2000 Server или Windows Server 2003. Первая операционная система несколько проще в освоении и дальнейшей настройке, а вторая содержит в своем составе некоторые дополнения, которые могут пригодиться в дальнейшем. Например, в составе Windows Server 2003 есть полноценный почтовый сервер, имеет более развитые средства защиты, что особенно важно при использовании сервера в качестве маршрутизатора и компьютера общего доступа в Интернет. Если же есть финансовые проблемы, есть время на освоение, есть желание разбираться в непривычной пока среде, то вполне можно попытаться установить и Linux. При этом следует подготовиться к решению проблем с драйверами. Разработчики новых компьютеров (материнских плат и других устройств) не всегда предлагают драйверы для Linux. В то же время встроенные в дистрибутив драйверы нередко прекрасно работают и с новым оборудованием.

Установка операционной системы Windows 2000 Server или Windows Server 2003 практически не отличается от установки любой другой ОС. Следует учитывать только, что Windows 2000 Server и Windows Server 2003 могут быть установлены в качестве контроллера домена. Если это не требуется, то в процессе установки надо выбрать соответствующий режим работы сервера.

В качестве сервера можно использовать компьютер любого производителя, включая и собранный самостоятельно, если вы уверены в его надежности. Вполне возможно, что вы не будете использовать специализированную серверную конфигурацию. Обычный компьютер может с успехом исполнять роль сервера, если он обладает достаточным размером оперативной памяти, свободным пространством на дисках и достаточной рабочей частотой процессора. Практически все современные процессоры могут работать на сервере. Каждый тип процессора обладает своими особенностями и может в наибольшей степени подходить для ваших целей. Учитывать надо как технические характеристики, так и экономические. Цены могут отличаться более чем в 6 раз. Нет смысла гнаться за самыми высокими характеристиками процессора, если сервер нужен только для идентификации пользователей в сети и хранения файлов. В то же время, если вы хотите применять сервер в качестве сервера приложений, дать возможность пользователям работать в терминальном режиме, когда все процессы идут именно на сервере, то вам не обойтись без современного двухъядерного процессора, а может быть, даже двух. Максимальный размер оперативной памяти современного компьютера зависит от его конфигурации. Специально разрабатываемые для работы в качестве сервера компьютеры могут работать с объемом оперативной памяти более 4 Гбайт. Для "обычных" компьютеров размер оперативной памяти может быть 512 Мбайт. Рабочая частота процессора у большинства современных компьютеров достигает 1 ГГц и более. Размеры винчестеров менее 80 Гбайт теперь тоже встречаются редко, в любой компьютер можно установить до четырех жестких дисков общим объемом более 100 Гбайт. Характеристики большинства современных компьютеров позволяют использовать их в качестве сервера с теми или иными возможностями. Компьютеры, специально предназначенные для работы в качестве сервера, отличаются повышенной надежностью своих систем, несколько специфическим дизайном, возможностью запереть компьютер, защитив от любопытных глаз и рук. Дорогие специализированные серверы имеют также серверные возможности, упрощающие администрирование и

повышающие надежность при бесперебойной работе. Так в разработках фирмы Hewlett-Packard предусмотрена "горячая" замена как дисков, так и оперативной памяти, предусмотрены встроенные средства удаленного администрирования, возможность запуска нескольких операционных систем на одном сервере, объединение серверов в кластеры. Такие особенности этих серверов позволяют строить системы с практически абсолютной надежностью, аварийная остановка которых имеет вероятность, близкую к нулю. Домашняя сеть или сеть небольшой организации, остановленная для планового обслуживания на 10—15 минут или аварийно остановившаяся один раз в год на 20 минут, не вызовет своей остановкой больших убытков. Скорее всего, эти убытки будут в сотни и тысячи раз меньше, чем цена эксплуатации сложной серверной системы. Другое дело, крупные корпорации, банки... Не стоит "стрелять из пушки по воробьям". Оцените свои потребности и соотнесите с возможностями. Один из серверов в нашей сети давно уже отстал от обычных рабочих станций по быстродействию, объему памяти и дисковому пространству, но исправно выполняет свои обязанности, никому не доставляя хлопот, внося свою лепту в работу сети, ничем не проявляя своей "отсталости". Важно, чтобы конфигурация сервера была совместима с операционной системой, которую мы хотим установить на него. Для Windows 2000 Server необходим компьютер с рабочей частотой не ниже 500 МГц, объемом оперативной памяти не менее 256 Мбайт, размером винчестера не менее 20 Гбайт. Требования для установки системы еще скромнее, но практика показывает, что при указанных параметрах большинство задач сети сервер решает прекрасно. Само собой разумеется, что должен быть дисковод компакт-дисков для обеспечения возможности установки системы с накопителя CD-ROM, хотя, возможна и установка системы по сети. Требования к видео и звуковой плате (адаптеру) практически никаких. Поскольку на сервере обычно не работают, то и монитор ему нужен условно, на всякий случай. В нашей сети на два сервера один плохонький монитор, и тот почти никогда не включается. Правда, при наличии свободных средств, монитор лучше приобрести нормальный. Иногда конфигурация компьютера не позволяет его эксплуатировать без монитора и клавиатуры. В этом случае без монитора не обойтись. Не обойтись без него и при первой установке системы. Далее мы рассмотрим процедуру установки русской версии Windows 2000 Server.

## Установка операционной системы на сервер

Эта операционная система специально разрабатывалась для сервера, для управления вычислительными сетями. Возможности, которыми обладает эта операционная система, позволяют без лишних хлопот эффективно администрировать достаточно крупные сети. Тем более, в небольшой сети, эта система будет надежно управлять сетью, соблюдая необходимый уровень защиты информации и надежности ее хранения.

Установка ОС Windows 2000 Server имеет некоторые особенности по сравнению с другими операционными системами, предназначенными для рабочих станций. Прежде всего, необходимо отметить, что после запуска сервера в рабочем режиме сложно, а иногда и невозможно, изменить или добавить компоненты операционной

системы. Несколько лучше дело обстоит с программным обеспечением. Во многих случаях Windows 2000 Server не требует перезагрузки после установки новых программ. Это позволяет расширять возможности сервера "в горячем" режиме. Но операционная система должна устанавливаться сразу в необходимой конфигурации. Важно тут же решить, какую роль будет выполнять этот сервер, будет единственным или вторым сервером в сети, если вторым, то будет ли он главным. Мы будем ориентироваться на ситуацию, когда наш сервер единственный в сети. Windows 2000 Server содержит очень важный компонент — "Active Directory", содержащий всю информацию о пользователях, компьютерах, других объектах сети, а также информацию о правах этих объектов и правах доступа к ним. Подробное описание Active Directory не входит в нашу задачу, его можно найти в справочниках по операционной системе Windows 2000 Server. Но очень важно, устанавливая операционную систему, сразу иметь четкое представление о том, будет ли этот сервер контроллером домена, или он будет играть роль подчиненного сервера. В случае если у вас единственный сервер, ему необходимо дать роль контроллера домена. Имя компьютера при этом должно состоять не более чем из 15 символов (это обеспечит совместимость со старыми операционными системами других компьютеров сети), не должно содержать пробелов, должно являться комбинацией латинских букв, цифр и символов дефиса.

В процессе установки вам потребуется некоторая информация.

- ❑ *Имя компьютера (сервера)*, например — myserver. Полное имя сервера будет состоять из имени компьютера и имени домена, например — myserver.firma.dom.
- ❑ *Имя домена*. Если ваш сервер не входит в другие домены и является единственным, то имя домена может быть любым, например "firma.dom". "firma" — это либо название фирмы, либо название рабочей группы. "dom" — это имя глобальной зоны сети, по аналогии с ru, com, org в Интернете. Если у вас есть зарегистрированное имя домена в Интернете, то лучше использовать именно это имя. Это позволит вам держать на вашем сервере свой сайт и обеспечивать доступ к нему из Интернета. Все компьютеры, входящие в ваш домен, должны иметь одинаковое имя рабочей группы, соответствующее имени домена (firma). Это упростит работу компьютеров в сети. Если необходимо подразделять пользователей на отделы, функциональные группы или еще каким-нибудь образом, то Windows 2000 Server позволяет осуществить это средствами Active Directory. Обслуживая сеть, вы сможете управлять этими группами более эффективно, чем рабочими группами.
- ❑ *Пароль учетной записи администратора*. Пароль может содержать не более 14 символов.
- ❑ *Количество пользовательских лицензий на подключение к серверу*. Если вы не успели приобрести достаточное количество лицензий, то можно просто указать необходимое их количество, и сервер разрешит подключаться всем вашим пользователям, позже можно приобрести недостающие лицензии. При наличии одного сервера в сети удобно использовать лицензии на сервер, определяющие количество одновременно подключенных пользователей. Если число подключений достигло количества лицензий, то сервер будет отклонять все последующие

подключения, пока их число не уменьшится. Лицензирование можно применять и для ограничения нагрузки на сервер.

- *Список компонентов ОС, которые вы хотите установить.* Большую часть из них можно добавлять после установки.
- *Режим работы сервера.* Будет это сервер приложений или файл-сервер. Для работы сервера приложений необходимо обеспечить терминальный доступ пользователей. Если на компьютерах клиентах сервера терминалов установлены операционные системы ниже, чем Windows 2000, то потребуются дополнительные лицензии на терминальный доступ. Кроме того, установка программ на сервер терминалов имеет много особенностей. Иногда требуются дополнительные компоненты, которые можно найти в Интернете, но они могут иметь значительный объем. Установка Office 2000, например, со стандартного инсталляционного диска невозможна без этих дополнительных компонентов. Если вам необходимо иметь терминальный доступ к серверу лишь в целях администрирования, то эта возможность предоставляется в любом варианте установки. Всегда есть два доступных и не требующих лицензий сеанса для администраторов.

Установка может быть проведена с локального привода CD-ROM или по сети. Для реализации второго варианта требуется, чтобы на компьютер была уже установлена другая операционная система. Это может быть как Windows любой версии, так и DOS. Особый интерес представляет предварительная подготовка винчестера на другом компьютере. Команда `winnt32`, с помощью которой можно начать установку на компьютерах с предустановленной операционной системой Windows NT или Windows 2000, имеет среди прочих ключи — `/tempdrive:буква_диска` и `/syspart:буква_диска`. Запустив программу установки с такими ключами, мы заставим ее скопировать загрузочные файлы на диск и пометить его, как активный. После этого диск можно установить в другой компьютер, и установка будет продолжена после его загрузки.

В случае сетевой установки может быть полезен ключ — `/makelokalsource`. При наличии этого ключа все установочные файлы будут скопированы на локальный жесткий диск, и процесс установки продолжится даже при прекращении сетевого доступа. Такая ситуация возможна, когда предыдущая операционная система полностью заменяется на новую. Если предыдущая операционная система должна быть сохранена, то после установки Windows 2000 Server будет возможна загрузка по выбору. Более полную информацию о ключах можно найти в справочной системе Windows 2000 Server. Для первой установки нам достаточно рассмотренного материала. Отметим только, что Windows 2000 Server использует файловую систему *NTFS5*, несовместимую с другими файловыми системами, но обеспечивающую наивысший уровень надежности хранения данных. Может быть использована и *FAT32*, которую поддерживает Windows 98, но эта файловая система не позволит в полной мере применять возможности сервера. Поэтому, когда нужно выбрать раздел для установки операционной системы, преобразуйте его в *NTFS5*. Эта операция потребует некоторого времени, но не потребует никаких дополнительных знаний и умений.

### ПРИ УСТАНОВЛЕННОЙ ОС WINDOWS 9X

Должен быть свободный раздел на винчестере достаточного размера или второй винчестер. Если винчестер один, и свободного раздела нет, то его можно создать с помощью распространенной утилиты Partition Magic. Эта утилита позволяет без потери данных уменьшить основной раздел винчестера и на освободившемся месте создать расширенный раздел и логический диск. Форматировать этот логический диск под NTFS не следует, это будет сделано в процессе установки.

## Итак, начнем установку

Рассмотрим самый простой вариант установки операционной системы с применением загрузки с CD-ROM. Для этого необходимо:

1. В BIOS SETUP установить возможность загрузки компьютера с компакт-диска (если не установлена другая операционная система) или просто запустить Setup.exe, если на компьютере уже установлена Windows 9x. Во втором случае будет выдано сообщение, показанное на рис. 9.1.

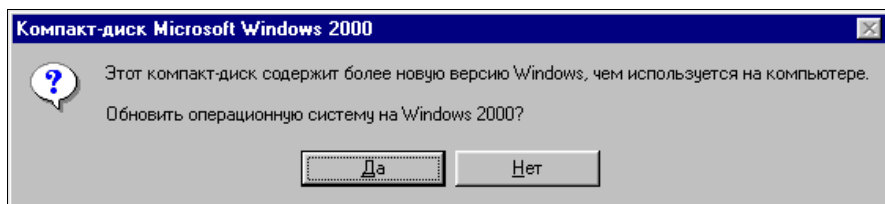


Рис. 9.1. Сообщение программы установки

Нам предстоит решить, будем мы обновлять систему или устанавливать заново. Лучше произвести новую установку. Это позволит избежать переноса ошибок, накопившихся в старой системе, да и на сервере скорее всего старая операционная система не понадобится. После ответа "НЕТ", на экране останется окно (рис. 9.2), позволяющее начать процесс установки.

2. Выбрав **Установка Windows 2000**, продолжим установку. Будет запущен мастер установки Windows 2000 (рис. 9.3). Нажимаем кнопку **Далее**.

Далее будет предложено прочитать лицензионное соглашение (рис. 9.4), затем ввести ключ, разрешающий дальнейшую установку (рис. 9.5).

На следующем шаге (рис. 9.6) можно выбрать некоторые специальные параметры установки.

3. Нажмите кнопку **Дополнительные параметры**, откроется одноименное окно (рис. 9.7).
4. Установите флажки **Копировать все файлы с CD-ROM на жесткий диск** и **Выбрать раздел диска для установки**. Нажмите кнопку **ОК**.
5. Последовательно появятся еще два окна: **Microsoft Windows 2000 Server Setup — Копирование установочных файлов** (рис. 9.8), в котором по завершении копирования нажмите кнопку **ОК**, и окно **Microsoft Windows 2000**

**Server Setup** — Перегрузка компьютера (рис. 9.9), где останется нажать кнопку **Готово**.

С этого момента начинается текстовая фаза установки.

- Программа установки предлагает указать диск и раздел, в котором будет выполнена установка Windows 2000 Server, и файловую систему, которую вы решили использовать. Если раздел не подготовлен, то вы можете его отформатировать средствами программы установки.



Рис. 9.2. Начало процесса установки

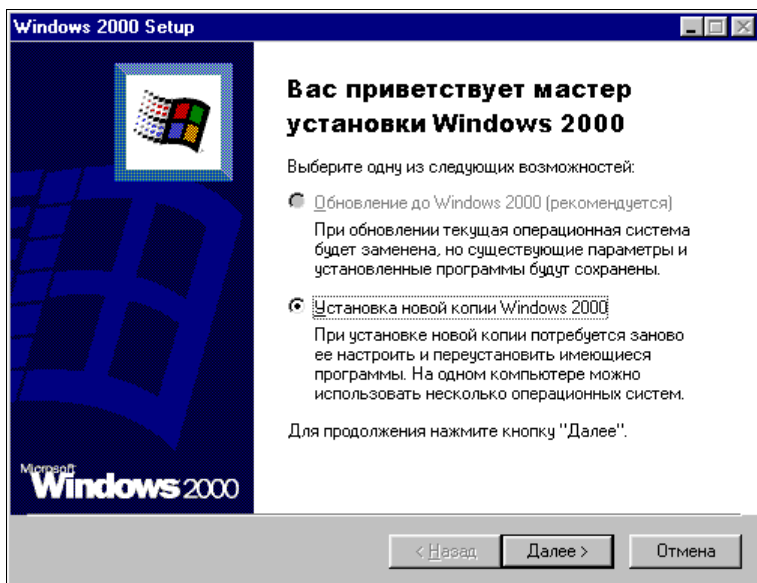


Рис. 9.3. Мастер установки Windows

- Программа установки копирует файлы на жесткий диск и перезагружает компьютер.

После перезагрузки снова начинается графическая фаза установки, во время которой вам будет предложено:

1. Указать компоненты, которые требуется установить.
2. Задать параметры сетевой конфигурации.
3. Установить пароль администратора системы и другую необходимую информацию.

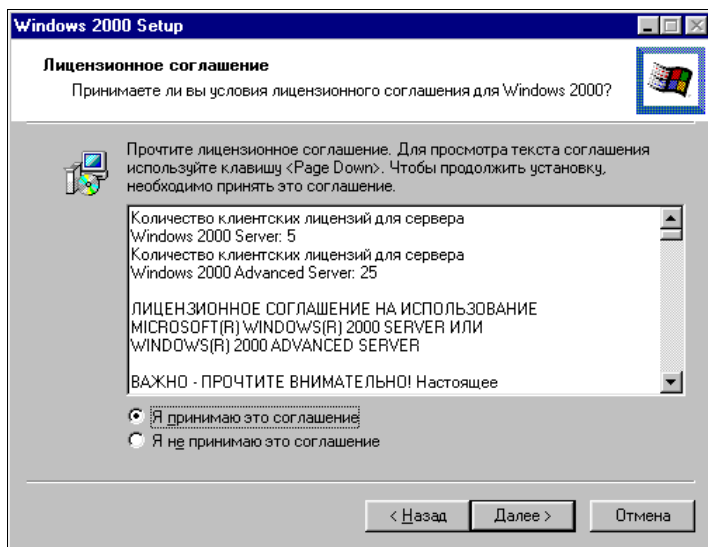


Рис. 9.4. Лицензионное соглашение

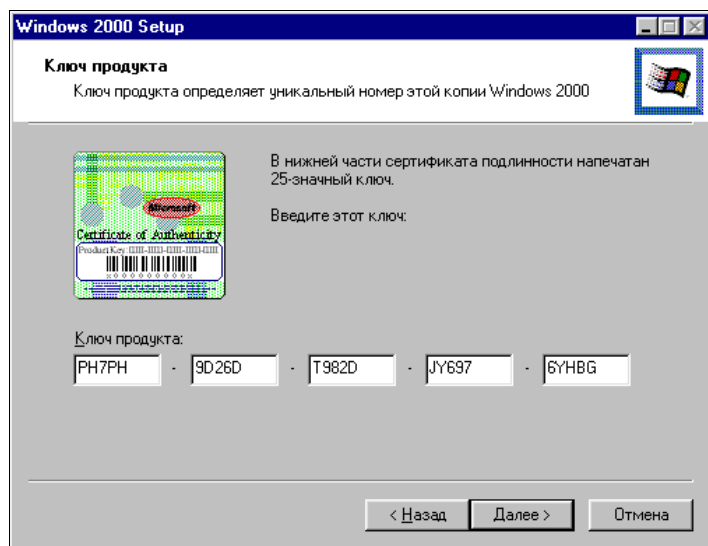


Рис. 9.5. Ввод ключа

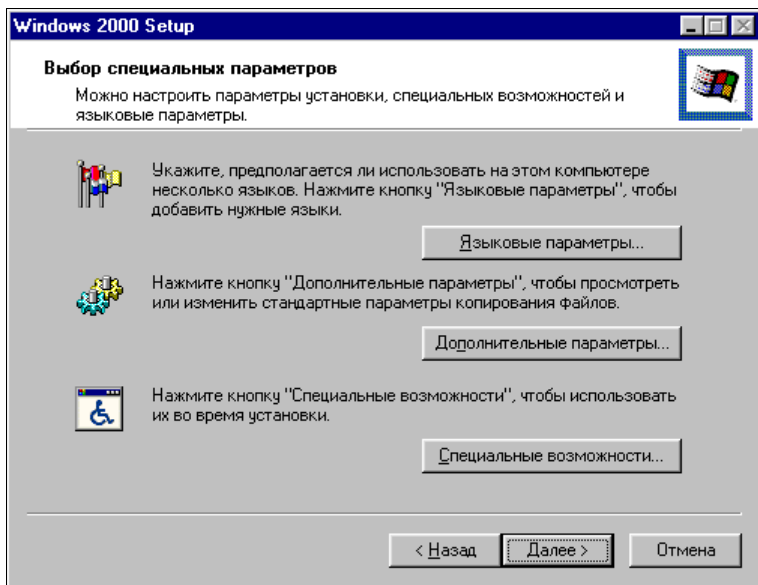


Рис. 9.6. Выбор специальных параметров

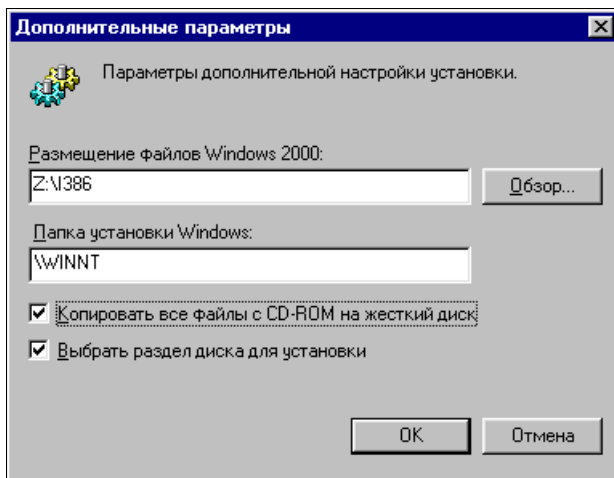


Рис. 9.7. Окно Дополнительные параметры

Эта фаза длится довольно долго, возможно более часа. После ее завершения и перезагрузки начинает загружаться Windows 2000 Server. После создания учетной записи администратора появится окно мастера настройки сервера (рис. 9.10). Вы можете закрыть это окно (по умолчанию оно будет запускаться каждый раз при загрузке системы) и проверить корректность работы компьютера после установки Windows 2000 Server. При необходимости, открыть окно настройки сервера можно через меню **Пуск**, последовательно пройдя по пунктам меню — **Программы** | **Администрирование** | **Настройка сервера**. При первой установке перед открытием



этого окна система задает еще один вопрос — является ли этот сервер единственным в домене. Если это так, то надо ответить утвердительно, поскольку позже изменить настройки, связанные с этим, сложнее.

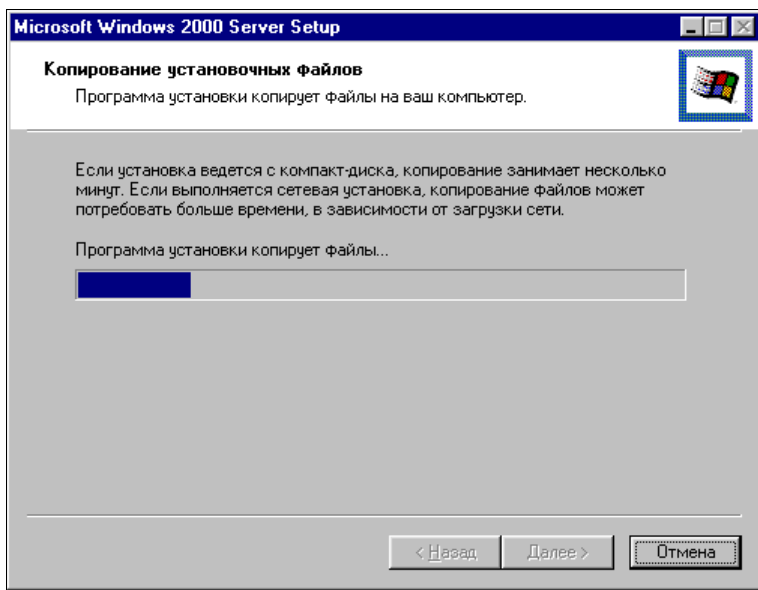


Рис. 9.8. Окно Microsoft Windows 2000 Server Setup — Копирование установочных файлов

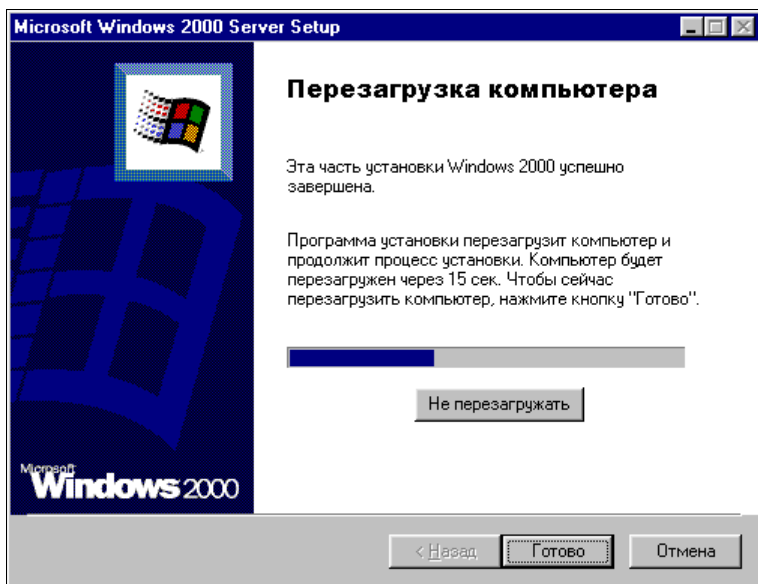


Рис. 9.9. Окно Microsoft Windows 2000 Server Setup — Перезагрузка компьютера

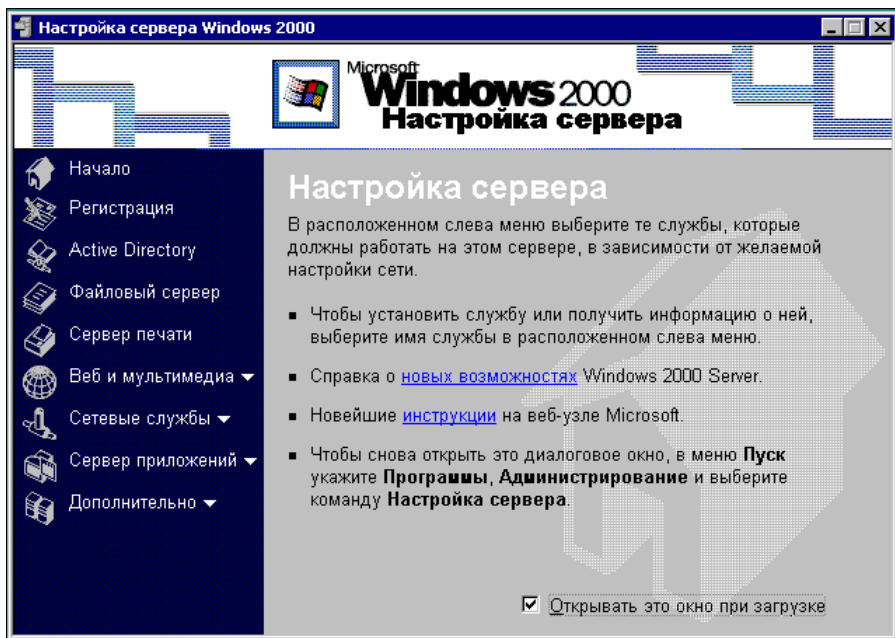


Рис. 9.10. Окно Настройка сервера Windows 2000

Для проверки корректности установки проделайте следующее:

1. Ознакомьтесь с сообщениями журнала событий. Для ознакомления с журналом событий необходимо открыть окно **Управление компьютером**. Это окно можно найти, последовательно пройдя по пунктам меню **Пуск | Программы | Администрирование | Управление компьютером**.
2. Проверьте сетевую конфигурацию компьютера, может ли он обмениваться данными с другими компьютерами сети. Это сделать совсем несложно. Достаточно использовать известную команду `ping` с указанием в качестве параметра IP — адреса любого доступного в сети компьютера.
3. Если на сервере должны храниться важные данные, проверьте работоспособность системы резервного копирования.

При ознакомлении с событиями системы (рис. 9.11) вы можете обнаружить сообщения об ошибке в системе, помеченные белым крестиком в красном круге.

Двойным щелчком по сообщению вы можете открыть его. Не все такие сообщения говорят о серьезных ошибках. В показанном на рисунке окне такие сообщения указывают на то, что сервер не может найти внешний источник времени для синхронизации своих часов. Ну, нет так нет. Если в сообщении говорится о некорректной или неправильной работе оборудования, невозможности инициализации драйверов, о других серьезных проблемах, то следует с ними разобраться. Возможно, придется заменить что-либо из оборудования или найти новые версии драйверов, совместимых с устанавливаемой операционной системой.

Если в процессе установки были заданы ошибочные параметры сетевой конфигурации, исправьте их.

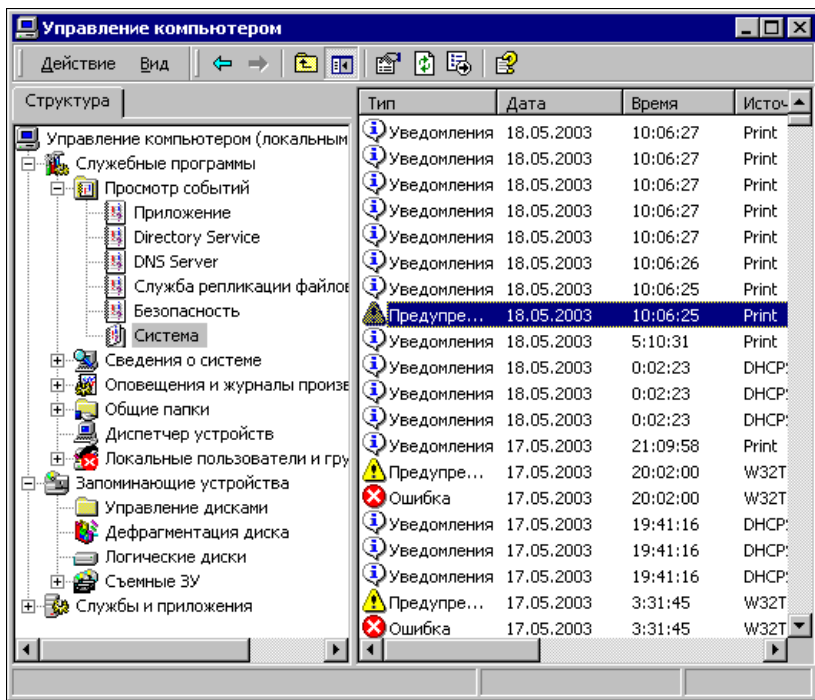


Рис. 9.11. Окно Управление компьютером

О системе резервного копирования очень подробно написано в справочной системе Windows 2000 Server.

Если вы убедились, что все работает нормально, то можно продолжать установку. В этом и состоит отличие серверной операционной системы от обычной, что установка, по всем признакам завершенная, на самом деле еще не завершена. Воспользуйтесь окном **Настройка сервера** (см. рис. 9.10) и просмотрите все пункты меню, расположенного слева. За каждым пунктом скрывается возможность добавить какие-либо свойства серверу или прочитать справочную информацию. Для нас важен пункт **Active Directory**. Если ваш сервер единственный в вашей сети, то в процессе установки этой службы вы должны сделать его контроллером домена. Это значит, что сервер не будет искать другие серверы, а будет себя "чувствовать хозяином положения". После установки Active Directory, пропадет возможность управления пользователями компьютера. В окне **Управление компьютером**, которое представлено на рисунке (см. рис. 9.11), в разделе служебных программ **Локальные пользователи и группы** помечены белым крестиком в красном круге. Теперь это не рабочая станция, а СЕРВЕР, а вы не администратор компьютера, а АДМИНИСТРАТОР ДОМЕНА. Другие серверы, которые в дальнейшем могут появиться в вашей сети, будут подчинены вашему серверу. Несколько позже мы рассмотрим настройку **Active Directory**, а пока сделаем небольшое отступление, касающееся обеспечения надежности работы сервера.

## Источник бесперебойного питания

Для надежной работы сервера необходим надежный источник питания. Если электросеть в вашем доме ненадежна, и случаются перебои с подачей электроэнергии, то, кроме сетевого фильтра, необходимо установить *источник бесперебойного питания (ИБП)*. Эти устройства сейчас распространены, выпускаются многими фирмами-производителями и имеют широкий диапазон возможностей и цен. Есть устройства, которые в случае перебоя в электроснабжении могут послать уведомление по электронной почте или выполнить другие операции. Но, вероятнее всего, у вас не предполагается удаленное администрирование с использованием Интернета, хотя и это возможно, а сообщение электронной почты не будет прочитано в ту же минуту. Поэтому вполне разумно использовать недорогой источник бесперебойного питания, который поддержит работу сервера в течение 7—10 минут. Сообщение, высланное пользователям локальной сети источником бесперебойного питания, позволит им завершить работу с файлами или приложениями для исключения потери данных. Большой популярностью пользуются источники фирмы APC, обозначаемые как Back-UPS CS *NNN*, где *NNN* — это номер серии приборов. Информацию о существующих на текущий момент устройствах этого типа можно получить в любом компьютерном магазине или по адресу [www.apc.com](http://www.apc.com) в Интернете. Если вы не успеваете подойти к серверу в отведенное время, то источник может самостоятельно корректно выключить сервер, правда, эта функция есть не у всех вариантов ИБП. В худшем случае питание просто будет выключено, но пользователи успеют завершить работу. Надежность файловой системы NTFS5 позволит быстро восстановить работоспособность сервера после включения питания. Установка простого ИБП не займет много времени. Back-UPS CS 500, например, определяется и устанавливается операционной системой самостоятельно. После установки потребуется небольшая работа по настройке реакции сервера на события, связанные с электропитанием. Если вы, забежав вперед, уже установили клиент службы терминалов на вашу рабочую станцию, и хотите настраивать сервер через терминальный доступ, придется в данном случае отказаться от такой возможности. Настройка ИБП возможна только локально. Включите монитор сервера и нажмите комбинацию клавиш <Ctrl>+<Alt>+<Delete>, если до выключения монитора вы решили завершить сеанс работы, и введите пароль администратора. Как и в обычной Windows 9x, щелкнув правой кнопкой на рабочем столе, откройте свойства рабочего стола (окно **Свойства: Экран**). На вкладке **Заставка** найдите кнопку **Питание** и нажмите ее. Откроется окно **Свойства: Электропитание** (рис. 9.12).

На вкладке **Сигнализация** (рис. 9.13) этого окна вы можете настроить варианты действий компьютера при снижении уровня зарядки батарей ИБП ниже некоторого порога. Для простых ИБП есть возможность настройки реакции компьютера на два порога. Это может быть сообщение и выключение, например. Есть возможность запуска какой-либо программы, которая обеспечит завершение каких-нибудь процессов и сохранение данных. Пока сервер не находится в рабочем режиме, поэкспериментируйте с ним. Выдернув шнур питания ИБП из розетки, засекайте время достижения первого и второго критического уровня зарядки батарей. Уменьшите это время на треть для учета старения батарей. Ориентируясь на полученные

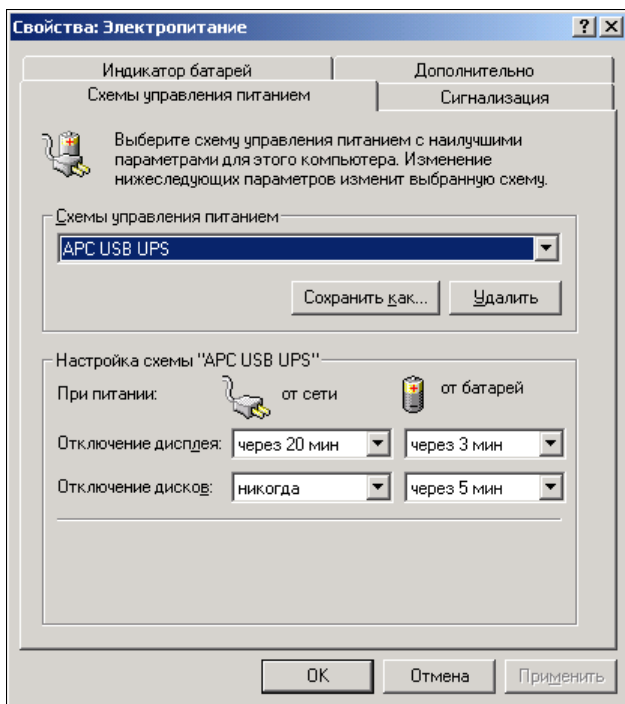


Рис. 9.12. Окно Свойства: Электропитание

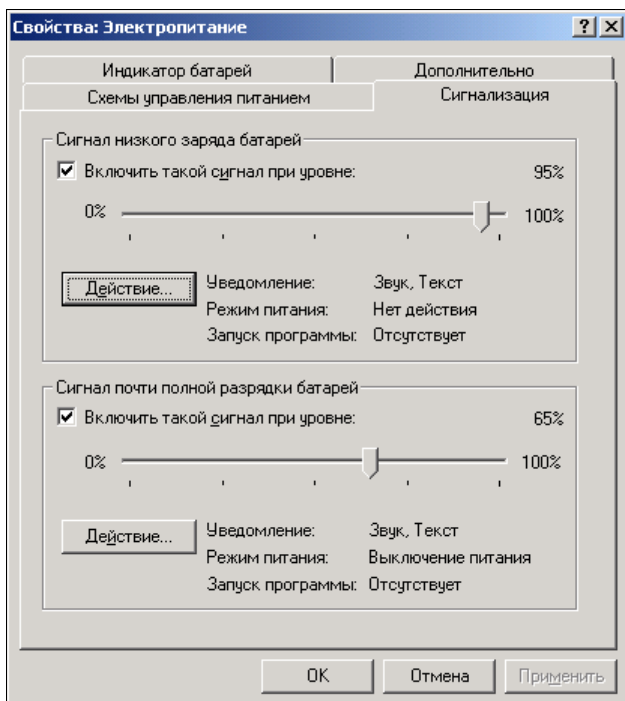


Рис. 9.13. Окно Свойства: Электропитание, вкладка Сигнализация

интервалы времени, вы сможете правильно спланировать реакцию сервера и ваши действия в случае аварийного отключения питания. При установке более сложных ИБП с расширенными возможностями обратитесь к прилагаемому к прибору руководству. После завершения установки и настройки источника бесперебойного питания можно продолжать настройку сервера.

## Планирование общих ресурсов и прав пользователей

Знание возможностей, которые предоставляет Windows 2000 Server для управления правами пользователей и общими ресурсами, поможет вам избежать многих проблем, связанных с безопасностью сети, а также лишних финансовых затрат на аппаратное обеспечение, приобретаемое ради этой безопасности. Мне известен случай, когда администратор сети, не зная возможностей системы, потребовал от администрации приобретения дорогостоящего маршрутизатора (для этой цели иногда используют и отдельный компьютер), ради разделения сети на две подсети, с целью ограничения доступа некоторых пользователей к отдельным ресурсам и разрешения другим пользователям печатать на принтерах из другой подсети. Прочитав этот раздел, вы поймете, что Windows 2000 Server позволяет решить такую задачу своими средствами. Надо лишь правильно спланировать права пользователей и общие ресурсы сети. Большое значение имеет правильное применение новых возможностей системы, таких как Active Directory.

### **ПРИМЕЧАНИЕ**

Установка Active Directory подробно будет рассмотрена в *главе 20*.

Вполне возможно, что ваша сеть уже имеет сервер, управляемый операционной системой Novell NetWare или работает без сервера (одноранговая сеть). В этом случае вы должны сохранить привычные имена пользователей сети. Особенно это актуально для NetWare. Вход в сеть для пользователей почти не будет отличаться от привычного для них. Потребуется, правда, некоторая перенастройка рабочих станций, которая может быть выполнена и без нарушения работы старого сервера, обеспечив параллельную работу серверов в течение некоторого времени до полного перехода на новый сервер. Оповестите пользователей о предстоящем переходе на новый сервер. Желательно, чтобы заранее был осуществлен переход на общую рабочую группу (Firma). Необходимо зарегистрировать пользователей домена. Для этого вам потребуется составить список всех пользователей сети с указанием сетевого имени. Пароли для входа в сеть собирать нет необходимости. Регистрируя пользователя, вы дадите ему возможность самостоятельно указать пароль при первом входе в сеть. Желательно разделить пользователей на группы по принадлежности к отделам или функциональным группам. Мы рассмотрим распределение пользователей по подразделениям и группам на примере организации сети предприятия. На основе этого примера можно легко сориентироваться при настройке любой сети.

После установки Active Directory в меню **Администрирование** появится еще один пункт **Active Directory — пользователи и компьютеры**. За этим пунктом скрывается окно с таким же именем (рис. 9.14).

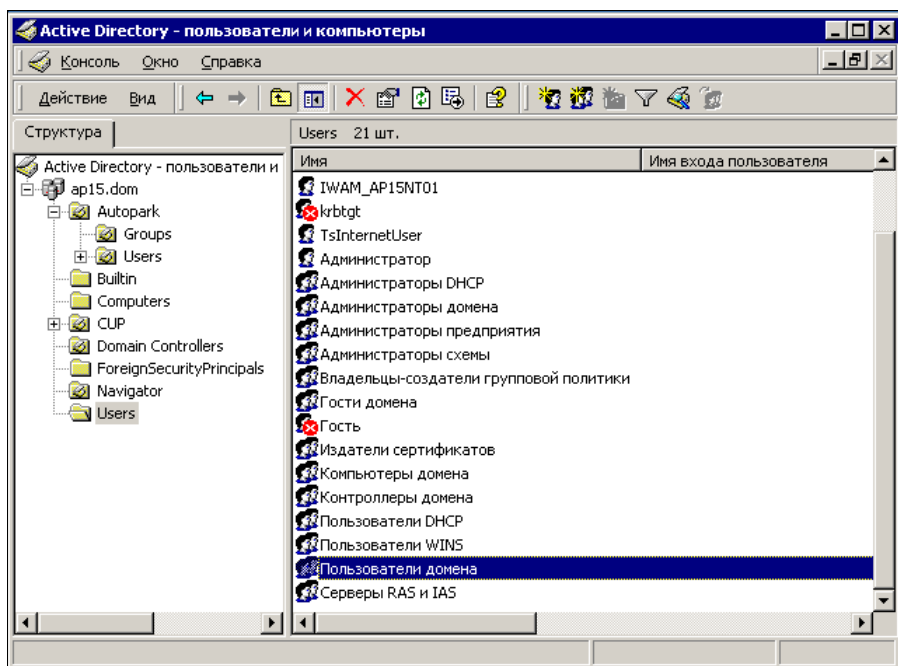


Рис. 9.14. Окно Active Directory — пользователи и компьютеры

Все окна, подобные этому и предназначенные для администрирования, называются *консолями*. Откройте консоль **Active Directory — пользователи и компьютеры**. В левой части консоли расположены папки, а в правой можно увидеть их содержание. По умолчанию операционная система уже содержит некоторые папки, как, например, папка **Users** (Пользователи). В этой папке находится список пользователей и групп пользователей, которые созданы по умолчанию. Пользователь **Администратор** был создан в процессе установки. Вы можете двойным щелчком открыть окно свойств этого пользователя и внести недостающие сведения. Выделив мышью значок, стоящий в заголовке списка папок в левой части консоли (группа компьютеров с именем вашего домена), и нажав кнопку **Действие** (рис. 9.15), вы откроете меню с перечнем всех возможных действий. В подменю **Создать** список всего, что можно создать. Сейчас, выбрав пункт **Подразделение**, необходимо создать подразделение. *Подразделение* — это просто папка, которая может содержать другие подразделения, группы пользователей, пользователей, компьютеры, принтеры и другие объекты. Active Directory позволяет унифицировать представление всех объектов сети и упростить работу с ними. На рис. 9.16 можно видеть содержание папки-подразделения. Не следует использовать для размещения пользователей сети папку **Users**, созданную по умолчанию. Она содержит большое число пользователей и групп, являющихся шаблонами для создания новых пользователей или

имеющих специфическое назначение. Пользователям и группам пользователей, которые содержатся в папке-подразделении, вы можете назначать права сразу для всего списка. Это бывает удобно, когда для работы с новым программным обеспечением требуется предоставить доступ к новым ресурсам сразу целому отделу. Группы пользователей, входящие в подразделение, могут содержать пользователей различных категорий, например руководителей и подчиненных, группы специалистов различного профиля. Не составляет труда включить, при необходимости, в такую группу пользователя из другого подразделения, если ему требуются права этой группы. На рис. 9.17 показан список пользователей, имеющих права группы ЦУП. Само подразделение ЦУП малочисленно, но многим пользователям сети необходим доступ к ресурсам, разрешенным для этой группы.

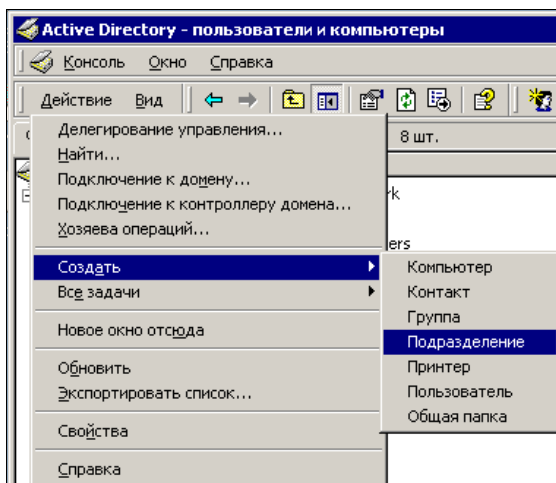


Рис. 9.15. Окно Active Directory — пользователи и компьютеры, меню Действие

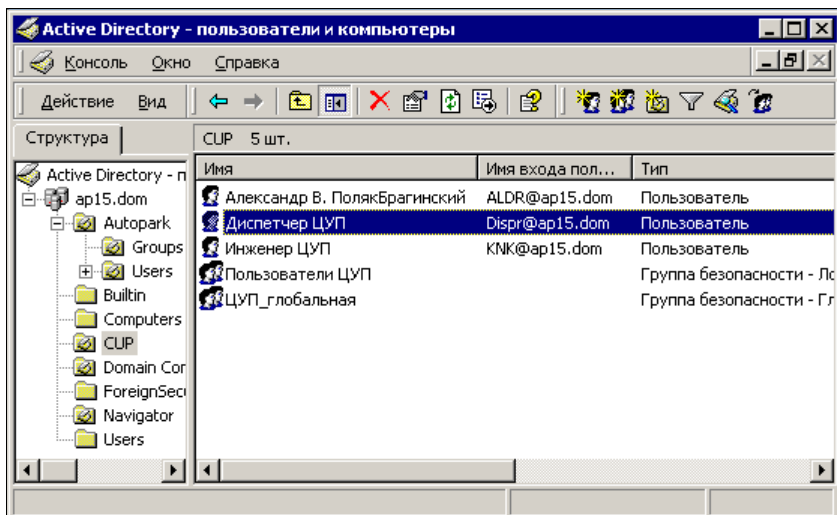


Рис. 9.16. Окно Active Directory — пользователи и компьютеры, содержание папки CUP



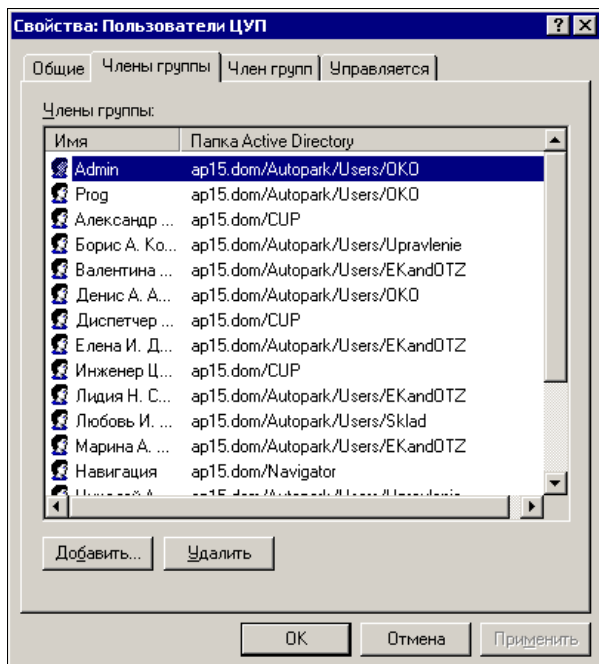


Рис. 9.17. Окно **Свойства: Пользователи ЦУП**

Пользуясь консолью **Управление компьютером**, вы можете добавлять права пользователей и групп на отдельные ресурсы сервера (рис. 9.18).

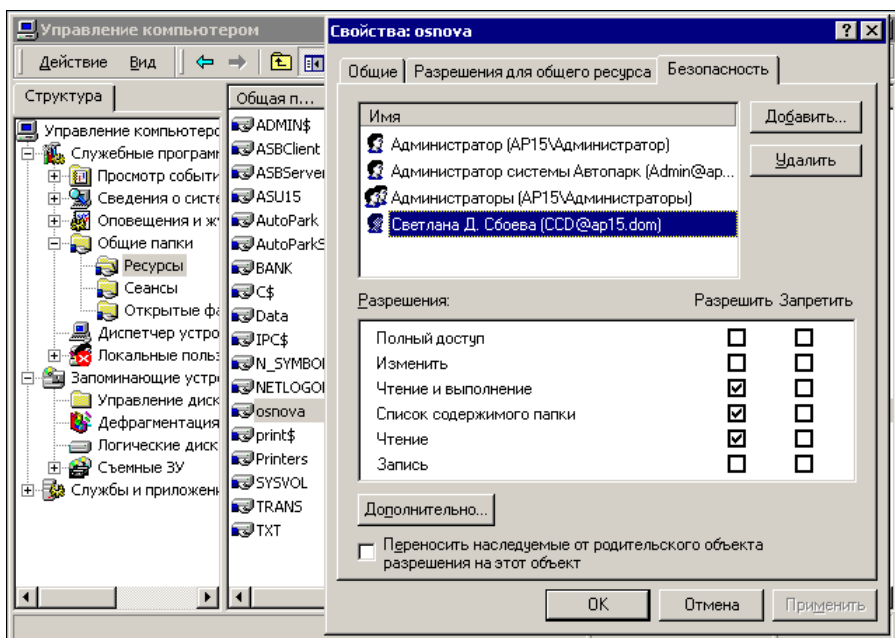


Рис. 9.18. Окно **Управление компьютером** (добавление прав пользователя на ресурс)

Следует отметить, что применение файловой системы NTFS5 не требует создания сетевого доступа к каждому общему ресурсу. В Active Directory применяется наследование прав от родительского объекта. Все объекты, расположенные внутри доступного родительского, будут так же доступны, но варианты разрешений можно устанавливать в соответствии с требованиями сети. Подробно о разрешениях на доступ к ресурсам можно прочитать в справочной системе. Но вы имеете возможность совершенно безопасно экспериментировать в этой области, создавая какие-либо ресурсы и определяя права на них различным пользователям, группам и подразделениям. Впоследствии, приобретя достаточный опыт, вы можете удалить эти ресурсы и настроить, если это необходимо, систему разрешений на действующие ресурсы.

## Пример создания нового пользователя и нового ресурса

Создадим нового пользователя, группу пользователей, в которую он входит, новое подразделение, новый ресурс, права на который этот пользователь должен иметь.

Предположим, что нам известна следующая информация о пользователе:

- имя пользователя: *Иванов Иван Иванович*;
- адрес пользователя: *Москва*;
- имя для входа в сеть: *YYY*;
- пользователь относится к категории опытных пользователей;
- группа: *Group1*;
- подразделение: *Новое*;
- имя ресурса: *NewResurs* (папка);
- права на данный ресурс: *Только чтение*;
- полные права на папку *NewResource* должен иметь *Администратор*.

Для создания пользователя с оговоренными свойствами выполните следующие шаги:

1. Откройте консоль **Active Directory** — **пользователи и компьютеры**.
2. В левой части консоли выделите мышью значок с именем вашего домена.
3. Нажмите кнопку **Действия**.
4. Выберите **Создать | Подразделение**.
5. В открывшемся окне **Новый объект** — **Подразделение** введите имя подразделения и нажмите кнопку **ОК**.
6. Выделите мышью только что созданную папку-подразделение и щелкните на ней правой кнопкой мыши.
7. В раскрывшемся меню выберите **Создать | Пользователь**.
8. В открывшемся окне **Новый объект** — **Пользователь** введите информацию о пользователе. Обратите внимание на порядок ввода имени. Вводится имя,

- инициалы (первая буква отчества) и фамилия. В поле **Полное имя** отображается вся внесенная информация. При необходимости замените инициалы на полное отчество, введите имя входа пользователя. При этом автоматически будет указано имя домена и имя для входа с компьютеров, на которых установлена операционная система Windows 9x. Нажмите кнопку **Далее**.
9. В открывшемся окне **Новый объект — Пользователь** (вид окна изменился) можно ввести пароль для входа в сеть или установить флажок **Потребовать смену пароля** при следующем входе в систему. Это даст возможность пользователю установить свой пароль при первом входе в сеть. Можно позже скорректировать режим использования пароля, например установить, что срок действия пароля неограничен. Нажмите кнопку **Далее**.
  10. В открывшемся окне проверьте правильность ввода данных и при необходимости вернитесь назад для их корректировки или нажмите кнопку **Готово**.
  11. Выделите мышью только что созданную папку-подразделение и щелкните на ней правой кнопкой мыши.
  12. В раскрывшемся меню выберите **Создать | Группа**.
  13. В открывшемся окне **Новый объект — Группа** введите имя группы. Отметьте тип группы **Группа безопасности** и область действия группы **Локальная** в домене и нажмите кнопку **ОК**. Изменить эти параметры можно только путем создания новой группы.
  14. Щелкните правой кнопкой мыши на значке новой группы и выберите в меню **Свойства**.
  15. Откройте вкладку **Члены группы** и нажмите кнопку **Добавить**.
  16. В открывшемся окне **Выбор: Пользователи, Контакты, Компьютеры или Группы** появится список пользователей домена. Новый пользователь в списке будет обозначен как *Иван Иванович Иванов* (YYY@firma.dom). Выделите его мышью и нажмите кнопку **Добавить**. Аналогично добавьте пользователя *Администратор*. Нажмите кнопку **ОК**, а в следующем окне кнопки **Применить** и **ОК**. В результате получим в окне консоли **Active Directory — пользователи и компьютеры** новое подразделение, пользователя и группу, в которую он входит (рис. 9.19).
  17. Создайте на диске папку *NewResource*.
  18. В окне свойств папки установите **Открыть общий доступ к папке** и назначьте ей сетевое имя, или примите имя, предложенное компьютером.
  19. Если требуется установить права для локального доступа, перейдите на вкладку **Безопасность** и добавьте нового пользователя и пользователя *Администратор*.
  20. Для пользователя *Администратор* установите все флажки, а для нового пользователя только флажок **Чтение**.
  21. Для настройки сетевого доступа откройте вкладку **Доступ** и нажмите кнопку **Разрешения**.

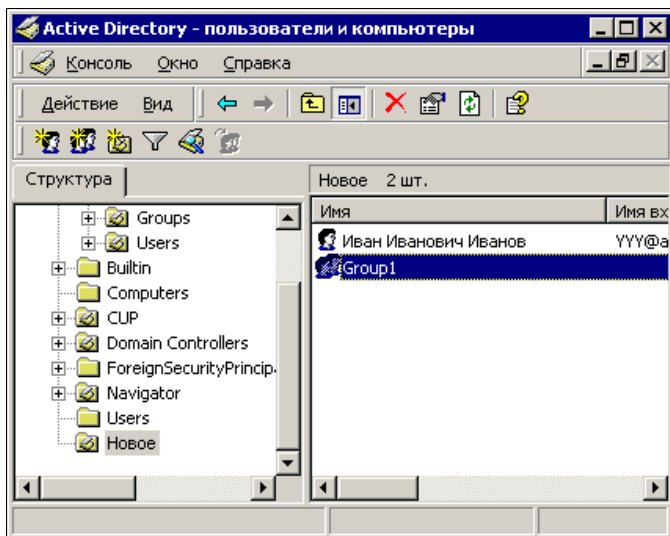


Рис. 9.19. Консоль Active Directory — пользователи и компьютеры: новое подразделение, пользователь и группа, в которую он входит

22. Добавьте сюда пользователей *Администратор* и нового пользователя, установив для администратора все флажки, а для нового пользователя только **Чтение**. Остальных пользователей удалите.
23. Нажмите кнопки **Применить** и **ОК**.

С этого момента только администратор имеет полный доступ к этому ресурсу, а Иван Иванович Иванов может лишь читать содержимое этого каталога. Это относится как к локальной работе, так и к работе по сети. Установка локальных прав возможна только при файловой системе FTFS, если вы не преобразовали диск и используете FAT32, то вкладка **Безопасность** будет отсутствовать, и вы не сможете управлять локальным доступом.

24. Закройте все открытые окна.

Подобным образом можно устанавливать права для групп или на другие объекты, например на принтеры, которые подключены к серверу или находятся в сети. Правда, если принтер физически подключен к другому компьютеру, а на сервере он установлен как сетевой, права на него могут быть установлены различные для доступа через сервер и для доступа через рабочую станцию, к которой он подключен. Но для пользователя сети это два разных принтера. При установке разрешений для группы правила будут распространяться на всех новых пользователей, добавленных в группу. Если предполагается обеспечить доступ пользователей группы к серверам других доменов, которые могут входить в вашу сеть, то область действия группы должна быть глобальной. Если вы уже создали локальную группу, но появилась необходимость дать пользователям группы глобальный доступ, необходимо создать еще одну группу с глобальной областью действия и добавить туда пользователей локальной группы. Для этого достаточно открыть свойства группы и добавить в нее членов.

Если вам показались описанные действия слишком сложными — не отчаивайтесь. Немного практики, и вы почувствуете, какую свободу в управлении правами пользователей на доступ к ресурсам предоставляет вам система. Есть возможность поступать от обратного. Всем можно разрешить доступ к ресурсу, а отдельным пользователям запретить, можно комбинировать эти методы. На вкладке **Безопасность** есть еще кнопка **Дополнительно**, нажав на которую вы получаете возможность более тонко регулировать доступ. Посмотрите на рис. 9.20.

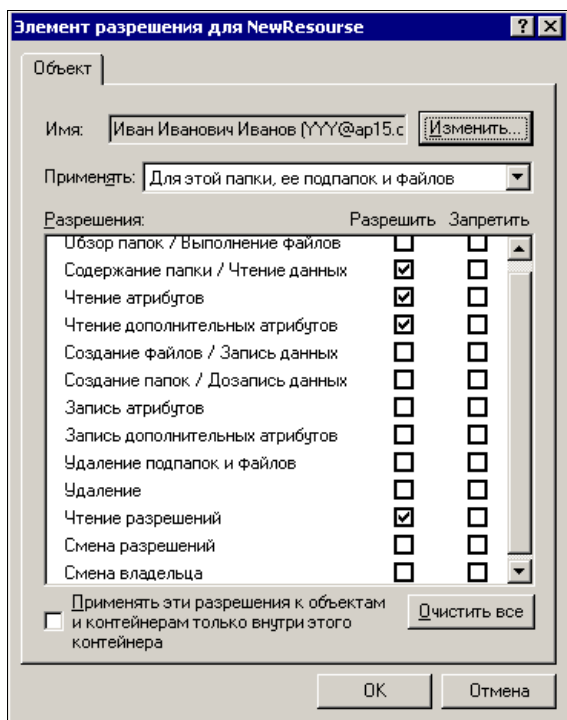


Рис. 9.20. Окно Элемент разрешения для NewResource

В списке вариантов разрешений тринадцать пунктов. Вы можете дать права на чтение и дозапись данных. При этом нельзя изменить или удалить данные. В этом же окне вы можете сменить пользователя, имеющего такие права. Возможности почти не ограничены.

## Другие возможности управления правами пользователей

Если вы имеете опыт работы с сетью NetWare, то знаете, что там можно устанавливать часы суток, разрешенные для входа пользователя в сеть. Windows 2000 Server предлагает более широкие возможности. Окно **Свойства: Иван Иванович Иванов** на вкладке **Учетная запись** имеет кнопку **Время входа**. Нажав на эту кнопку, вы откроете окно **Время входа для Иван Иванович Иванов** (рис. 9.21).

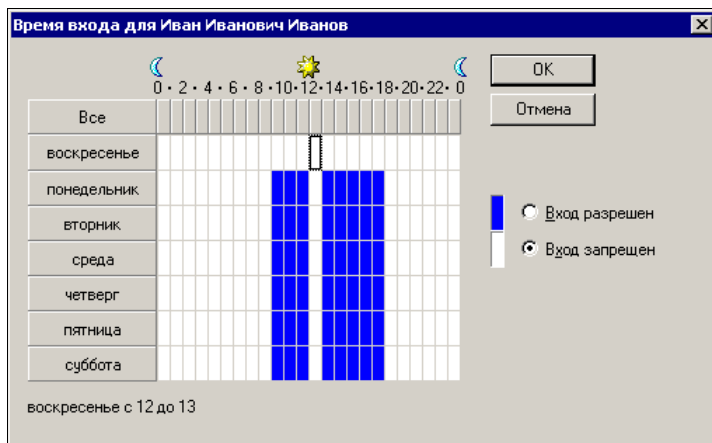


Рис. 9.21. Окно **Время входа для Иван Иванович Иванов**

Вы можете разрешить вход в сеть по конкретным дням и в определенные часы.

К сожалению, Windows 2000 Server не позволяет изменить время входа для группы пользователей. В следующей версии серверной операционной системы Windows Server 2003 этот изъян устранен.

Нажав кнопку **Вход на** в окне свойств пользователя, можно разрешить вход на отдельные компьютеры сети и запретить на остальные.

На вкладке **Сеансы** окна свойств можно ограничить время активного сеанса пользователя, ограничить время бездействия (пользователь забыл выключить компьютер и оставил открытыми файлы, что может помешать каким-либо процессам), на вкладке **Входящие звонки** можно разрешить или запретить пользователю доступ к виртуальной частной сети.

Словом, следует покопаться во вкладках и свойствах, и вы обнаружите для себя множество возможностей управления правами пользователей и ресурсами. Поиск возможностей и изучение свойств существенно облегчает оперативная справка по элементам окон.

## Windows Server 2003

В основном возможности этой системы те же, что и у Windows 2000 Server. Впрочем, есть и некоторые особенности и дополнительные возможности для администратора.

Установка может производиться как из среды предыдущей версии Windows, так и загрузившись с компакт-диска. Процедура установки практически не отличается от установки Windows 2000 Server. Но когда дело доходит до настройки сервера, мы обнаружим, что, в отличие от предыдущей версии, по умолчанию не устанавливаются сервисы сервера. Все, что вы хотите установить, необходимо выбрать явно. Кроме того, установив Active Directory, вы увидите, что ни одна из политик безопасности не определена по умолчанию. Необходимо самостоятельно определить правила доступа к домену для всех создаваемых групп и пользователей. С одной

стороны, для начинающего администратора — неудобство и сложность, но с точки зрения безопасности сети, — это разумное решение. Ни одно из правил доступа к ресурсам домена не будет использоваться без вашего ведома. Первое, с чем вы встретитесь в начале настройки, — это выбор роли сервера в окне **Manage Your Server** (Управление сервером) (рис. 9.22).

В этом окне следует нажать кнопку **Add or remove a role** (Добавить или удалить роли). При этом откроется окно со списком возможных ролей сервера (рис. 9.23).

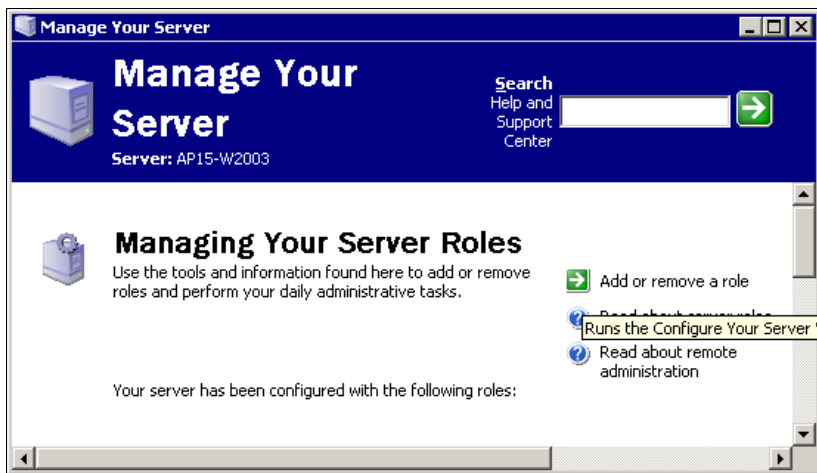


Рис. 9.22. Окно Manage Your Server

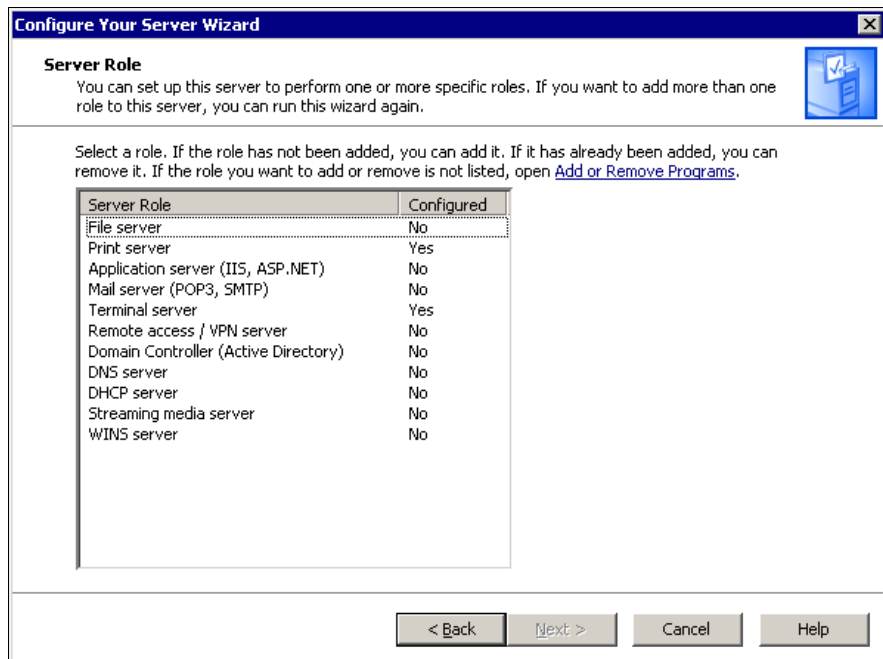


Рис. 9.23. Окно Configure Your Server Wizard — Server Role

В отличие от того, что вы видите на рисунке, при первой установке напротив каждого пункта списка будет стоять пометка **NO**. Для того чтобы добавить или удалить роли, необходимо открыть окно **Windows Components Wizard** (Установка компонентов Windows) (рис. 9.24), для этого в открытом окне достаточно нажать ссылку **Add or Remove Programs** (Добавить или удалить программы).

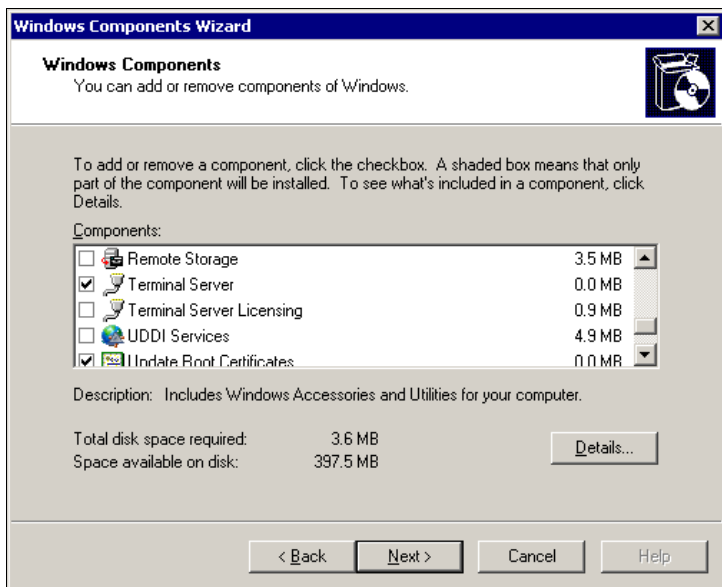


Рис. 9.24. Окно **Windows Components Wizard**

Это окно выглядит аналогично тем, что вы видели в других версиях Windows. Необходимо отметить выбранные компоненты и нажать кнопку **Next** (Далее). При этом система предложит подождать, пока будут скопированы файлы и установлены новые компоненты.

В остальном работа с новой операционной системой мало отличается от работы с Windows 2000 Server. Новые возможности, которые заложены в этой операционной системе, позволяют более комфортно управлять большими сетями, для чего она и разрабатывалась. Добавлены новые возможности для разработчиков программного обеспечения. Некоторые возможности новой системы могут и привлечь особое внимание, например встроенный почтовый сервер. Следует отметить и защиту сетевых соединений, как в Windows XP. Если ваш сервер будет постоянно подключен к Интернету, то злоумышленнику трудно будет проникнуть в вашу сеть извне — система безопасности находится под вашим контролем! Очень хорошо построена справочная система. Из каждого окна ссылки вы имеете возможность пройти по дополнительным ссылкам. Для небольшой сети Windows 2000 Server, установки "по умолчанию" в котором позволяют практически сразу приступить к работе с установленными службами и сервисами, предпочтительней, если только не планируется организация почтового сервера и управления сервером через Интернет без использования сервера терминалов.



## Варианты работы выделенного сервера

В зависимости от назначения сервера, его настройки и функциональные возможности могут отличаться. Для Windows 2000 Server в небольшой сети могут интересовать в основном два варианта работы — это файловый сервер, который обеспечивает хранение файлов пользователей и обеспечение политики доступа к этим файлам, или сервер приложений, который предоставляет пользователям возможность использовать установленные на сервере приложения, не имея их на локальной машине. После установки операционной системы с помощью окна **Настройка сервера Windows 2000** (рис. 9.25), выбрав необходимый пункт меню слева, вы получите доступ к меню настройки выбранного компонента. Настройка файлового сервера трудностей не вызовет. Сервер приложений может потребовать значительного внимания для своей настройки.



Рис. 9.25. Окно Настройка сервера Windows 2000

## Как работает сервер приложений?

Каждый пользователь рабочей станции, на которой установлена какая-либо версия Windows, имеет возможность подключиться к серверу и использовать все его

ресурсы для работы. К ресурсам относятся сами приложения, дисковое пространство для сохранения файлов, оперативная память сервера и его процессор. Независимо от возможностей самой рабочей станции, можно работать с приложениями, которые требуют значительной частоты процессора и существенного объема оперативной памяти. В ответ на команды пользователя, посылаемые нажатием клавиш, сервер передает рабочей станции изображения окон. Windows 2000 Server позволяет работать как с рабочим столом, так и с приложением, которое предварительно определено администратором и которое необходимо пользователю без доступа к рабочему столу. Поддерживаются 3 значения разрешений экрана — 800×600×256, 640×480×256 и 1024×768×256. Информация, передаваемая с сервера, может сжиматься для уменьшения сетевого трафика, рисунки могут кэшироваться для ускорения работы с ними. Закрыть приложение может только администратор. Сессия полностью сохраняется в памяти сервера. Войдя на сервер через несколько дней после завершения предыдущей работы, вы обнаружите, что все окна остались в том же положении, все приложения также запущены (если вы сами не завершили сеанс). В случае перегрузки сервер может запретить запуск приложений и ограничить подключение новых клиентов. Для работы с рабочими станциями с операционными системами ниже Windows 2000 требуется дополнительная лицензия на каждое рабочее место. Есть некоторые неудобства, связанные с тем, что обращаться к своим дискам пользователь может только как к сетевым. Для работы с офисными приложениями десяти пользователей сервер должен содержать процессор с частотой 500—600 МГц (или 2 по 300) и примерно 198 Мбайт оперативной памяти.

## Настройка сервера после установки

Сервер терминалов, который необходим для работы выделенного сервера в качестве сервера приложений, может иметь два режима работы. Это собственно сервер приложений и режим удаленного управления. Второй режим разрешает только два сеанса, которые обычно предназначены для администраторов. Но в небольшой сети может быть достаточно этих двух сеансов, если сервер используется в смешанном режиме — как файловый сервер и как сервер приложений для ограниченного числа пользователей. В этом варианте значительно упрощается установка приложений на сервер. Так, в небольшой офисной сети вы можете предоставить руководителю возможность работать в терминальном режиме, а сами будете иметь доступ с помощью второго сеанса.

Выбрав в окне **Настройка сервера Windows 2000** пункт **Настройка служб терминалов**, вы откроете одноименное окно (рис. 9.26).

При использовании режима управления появится сообщение о применении этого режима.

Нажмите кнопку **ОК**. Обычно дальнейшая настройка не требуется.

Для того чтобы клиент мог подключаться к серверу терминалов, необходимо установить клиентское программное обеспечение. Для этого сделайте следующее:

1. Вставьте чистую отформатированную дискету в дисковод.
2. Нажмите кнопку **Пуск**.

### 3. Выберите в меню **Программы | Администрирование | Создатель клиента служб терминалов**.

Будет создана дискета, с которой вы сможете устанавливать клиентскую часть сервера терминалов на рабочие станции.

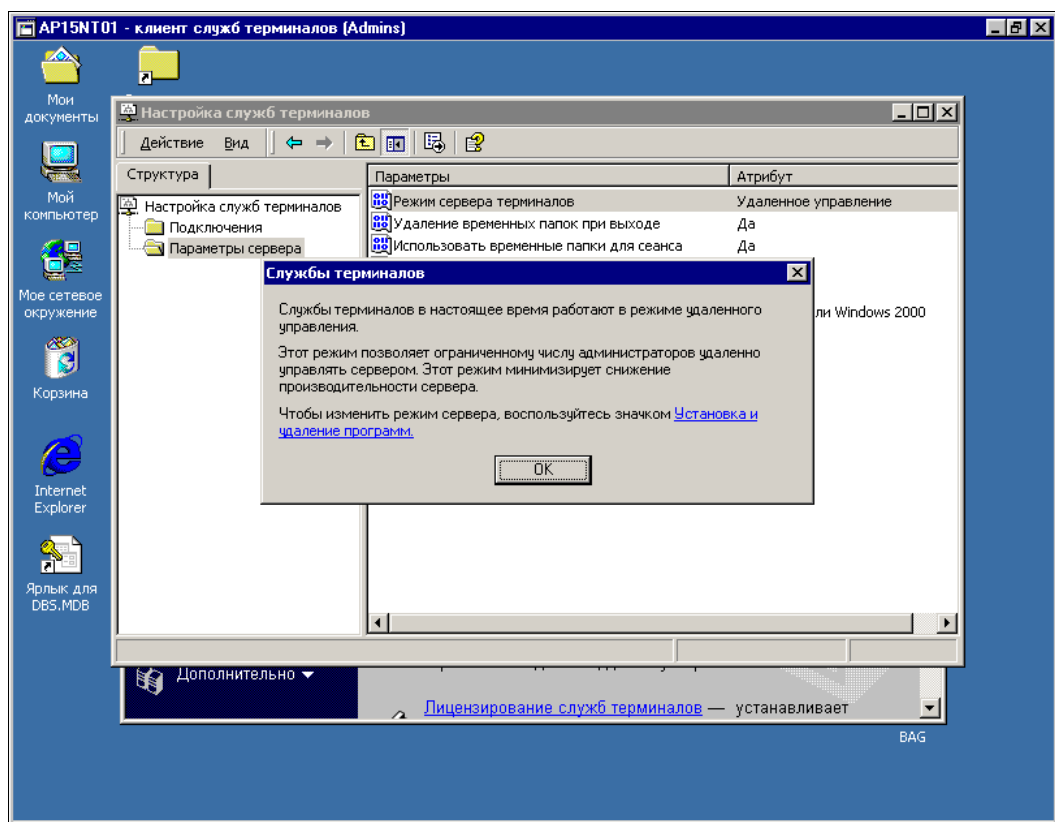


Рис. 9.26 Окно **Настройка служб терминалов**

После установки клиентского программного обеспечения на локальной машине в меню **Пуск | Программы** появится пункт **Клиент служб терминалов**, содержащий подпункты **Диспетчер клиентских подключений** (рис. 9.27) и **Клиент служб терминалов** (рис. 9.28).

В окне **Диспетчер клиентских подключений** вы сможете увидеть, создавать и выбирать уже созданные клиентские подключения. Окно **Клиент служб терминалов** служит для настройки клиента: выбора разрешения экрана, возможности сжатия данных и кэширования рисунков, а также для выбора сервера.

Создав подключение и выбрав его в окне **Диспетчер клиентских подключений**, двойным щелчком вы можете открыть сеанс терминального доступа. При этом откроется окно вашего сеанса и стандартное окно входа в Windows (рис. 9.29).

Вы можете работать в этом окне, как будто на самом сервере. Права доступа к файлам определяются локальными разрешениями на сервере. Закрыв окно, вы

сохраните сеанс открытым со всеми открытыми файлами и запущенными программами. Для того чтобы сеанс закрыть, необходимо нажать кнопку **Пуск** в окне сеанса и выбрать **Завершение сеанса**. Если выбрать **Завершение работы**, то сервер будет выключен! Во время работы в терминальном режиме можно применять "горячие" клавиши. Перечень возможных вариантов приведен далее в табл. 9.1.

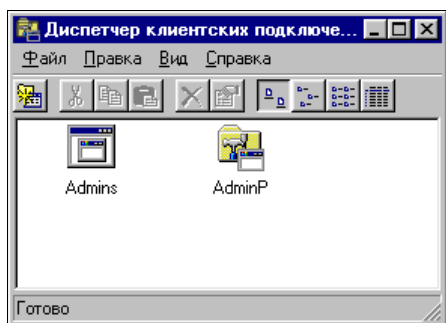


Рис. 9.27. Окно Диспетчер клиентских подключений

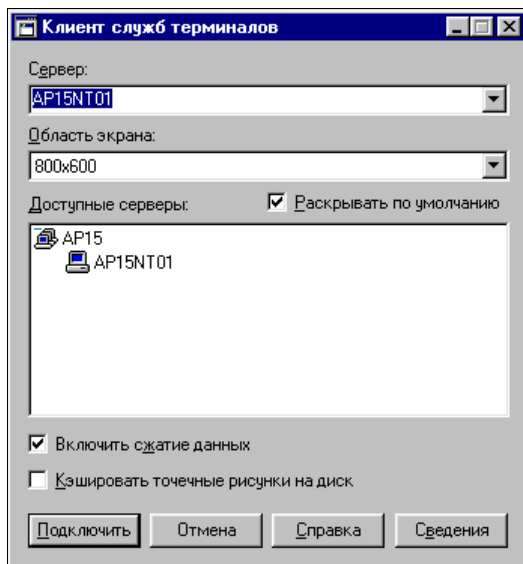


Рис. 9.28. Окно Клиент служб терминалов

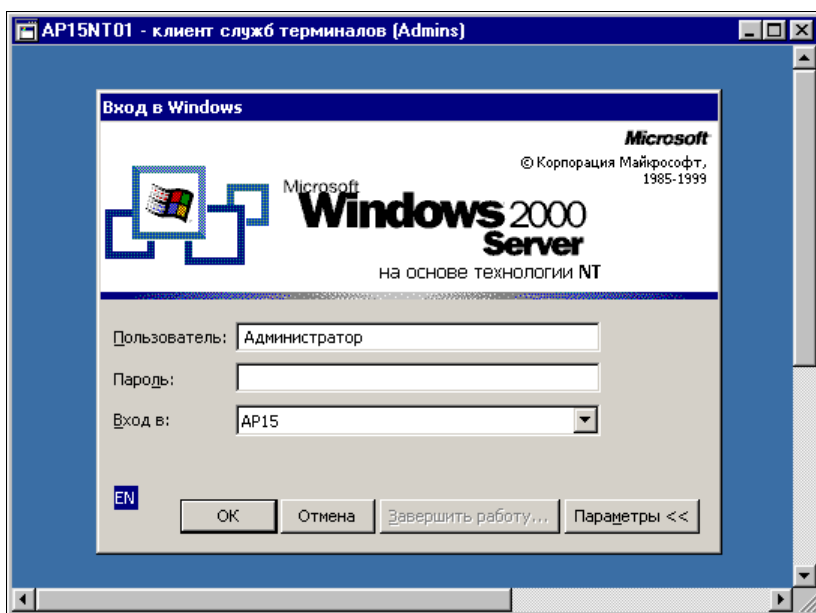


Рис. 9.29. Окна AP15NT01 — клиент служб терминалов и Вход в Windows

Таблица 9.1. "Горячие" клавиши, используемые в Windows и в окне клиента

Описание действия	В Windows	В окне клиента
Вызывается переключатель между приложениями и переход вправо по списку приложений	<Alt>+<Tab>	<Alt>+<PageUp>
Вызывается переключатель между приложениями и переход влево по списку приложений	<Alt>+<Shift>+<Tab>	<Alt>+<PageDown>
Осуществляется переключение между работающими приложениями	<Alt>+<Esc>	<Alt>+<Ins>
Запуск главного меню системы	<Ctrl>+<Esc>	<Alt>+<Home>
Открытие системного меню активного приложения	<Alt>+<Spacebar>	<Alt>+<Del>
Запуск панели Security в системе Windows NT	<Ctrl>+<Alt>+<Del>	<Ctrl>+<Alt>+<End>
Записать в буфер обмена содержимое окна клиентской программы	<PrintScreen>	<Ctrl>+<Alt>+<+> (<+> на цифровой клавиатуре)
Записать в буфер обмена содержимое активного окна в окне клиентской программы	<Alt>+<PrintScreen>	<Ctrl>+<Alt>+<-> (<-> на цифровой клавиатуре)
Переключение между оконным и полноэкранным режимами клиентского окна	<Ctrl>+<Enter>	<Ctrl>+<Alt>+<Break>

При необходимости, можно более тонко настроить сервер терминалов для ограничения доступа пользователей к ресурсам сервера.

## Настройка служб терминалов

В Windows 2000 Server есть возможность управления службами терминалов через два семейства параметров — **Подключения** и **Параметры сервера**. Для доступа к средствам настройки выберите в меню **Программы | Администрирование | Настройка служб терминалов**. Откроется окно **Настройка служб терминалов** (рис. 9.30).

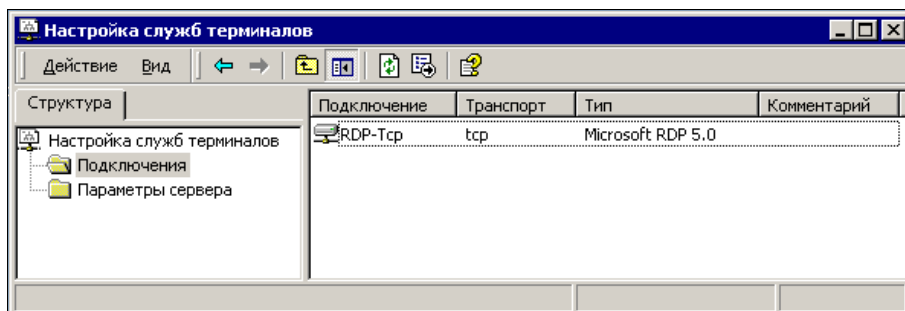


Рис. 9.30. Окно Настройка служб терминалов (Подключения)

## Подключения

Выберите из списка подключение, которое вы хотите настроить. Количество подключений определяется количеством сетевых адаптеров. Щелкните правой кнопкой по значку подключения и выберите в контекстном меню **Свойства**.

Откроется диалоговое окно свойств с восемью вкладками.

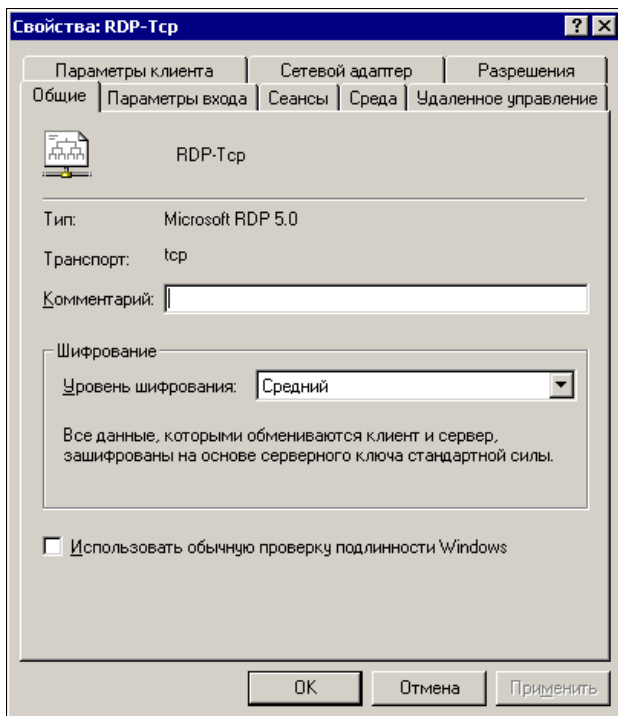


Рис. 9.31. Окно **Свойства: RDP-Тср**, вкладка **Общие**

На вкладке **Общие** (рис. 9.31) можно настроить уровень шифрования данных. **Низкий** — шифруется информация, вводимая пользователем при регистрации на сервере (имя пользователя и пароль), и данные, передаваемые от клиента к серверу. **Средний** — шифруются данные, передаваемые в обоих направлениях с помощью ключа стандартной длины (56 бит). **Высокий** — данные шифруются ключом длиной 128 бит (данный режим доступен только для тех версий, которые продаются на территории Северной Америки).

На вкладке **Параметры входа** (рис. 9.32) можно либо указать необходимость ввода регистрационных данных в клиентской программе — **Использовать регистрационные сведения клиента**, либо для всех сеансов задействовать регистрационные данные одного и того же пользователя — **Всегда использовать следующие сведения**. Можно также задать необходимость ввода пароля при установлении сеанса, даже если клиентская программа настроена на автоматический ввод имени и пароля — **Требовать пароль только для входа**.

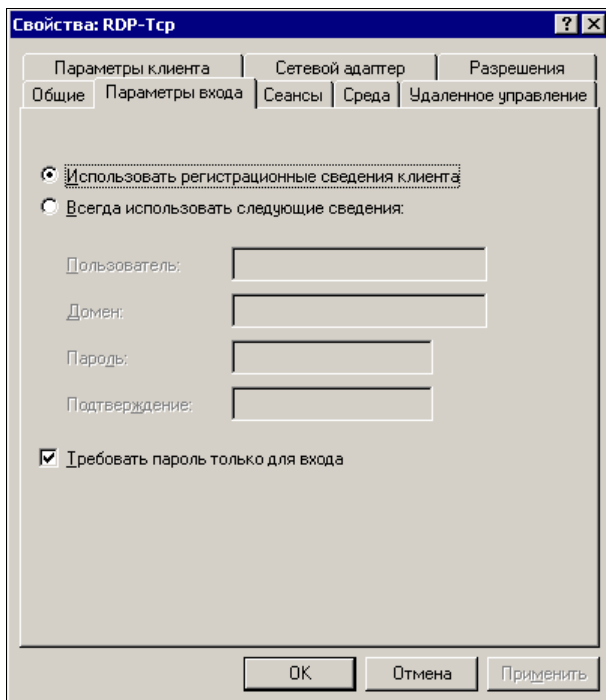


Рис. 9.32. Окно **Свойства: RDP-Тср**, вкладка **Параметры входа**

На вкладке **Сеансы** (рис. 9.33) можно заменить соответствующие настройки, сделанные в свойствах пользователей и относящиеся к длительности активного сеанса, длительности бездействующего сеанса и длительности отключенного сеанса.

На вкладке **Среда** (рис. 9.34) можно назначить пользователю приложение, загружаемое при запуске сеанса работы с терминальным сервером, а также запретить использование фонового рисунка на рабочем столе.

Вкладка **Удаленное управление** (рис. 9.35). Здесь можно разрешить или запретить удаленное управление сессией пользователя из сессии администратора (управлять пользовательской сессией таким образом можно только из клиентской сессии, в которой работает администратор, но не с консоли сервера).

Вкладка **Параметры клиента** (рис. 9.36). Здесь можно настроить подключение принтеров клиентского ПК в сессии терминального сервера, а также сопоставление в клиентской сессии LPT-портов клиентского компьютера и буферов обмена клиентского ПК и терминальной сессии.

Вкладка **Сетевой адаптер** (рис. 9.37) позволяет настроить на использование терминальных служб определенные сетевые адаптеры сервера (если их несколько).

Вкладка **Разрешения** (рис. 9.38) позволяет настроить управление доступом к соединениям RDP-Тср.

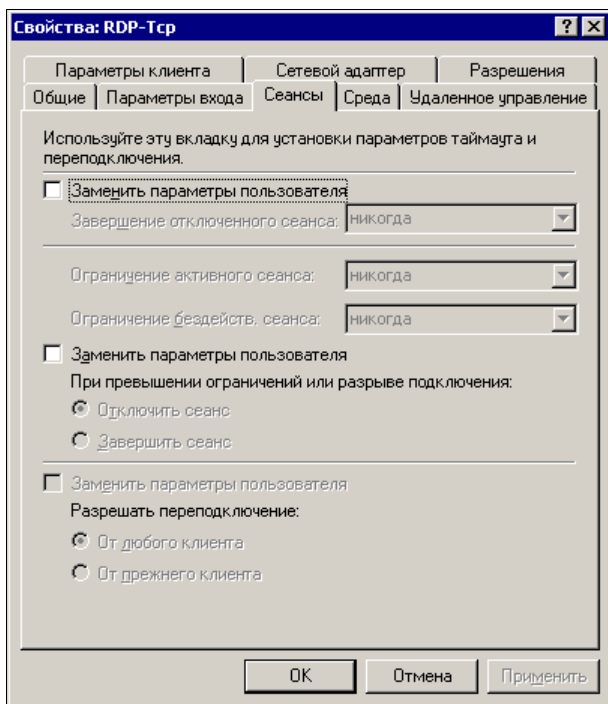


Рис. 9.33. Окно **Свойства: RDP-Тср**, вкладка **Сеансы**

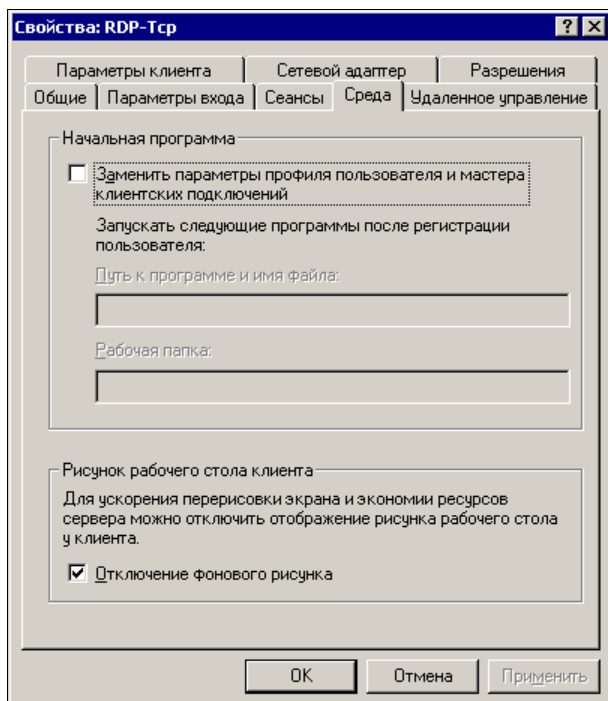


Рис. 9.34. Окно **Свойства: RDP-Тср**, вкладка **Среда**



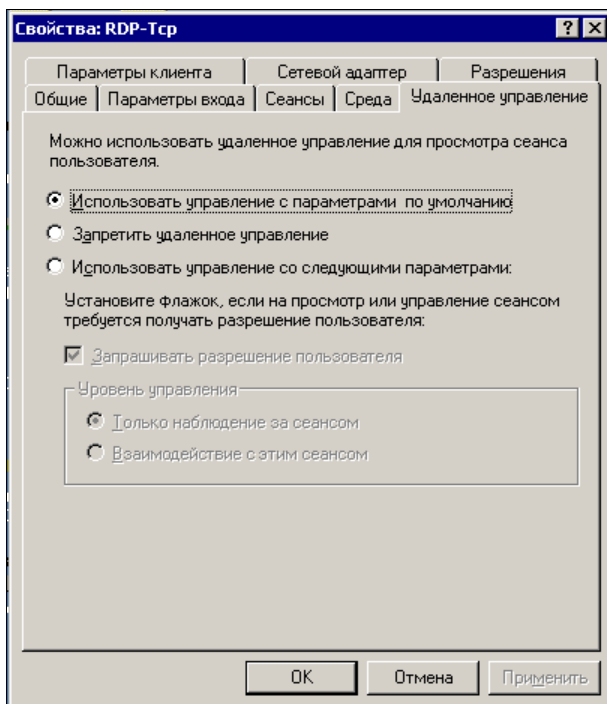


Рис. 9.35. Окно Свойства: RDP-Тср, вкладка Удаленное управление

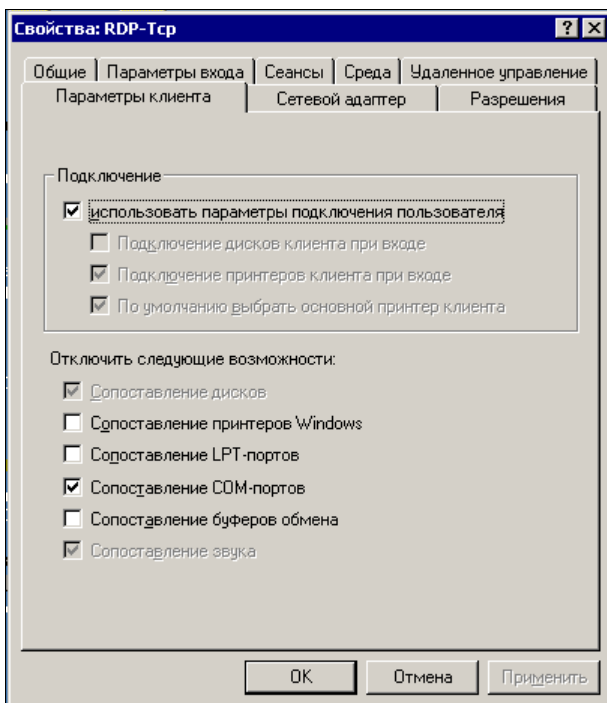


Рис. 9.36. Окно Свойства: RDP-Тср, вкладка Параметры клиента

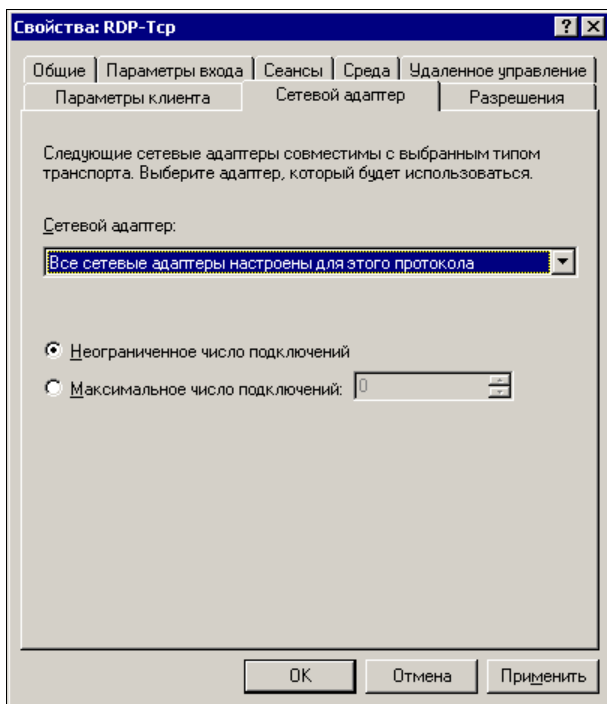


Рис. 9.37. Окно Свойства: RDP-Тср, вкладка Сетевой адаптер

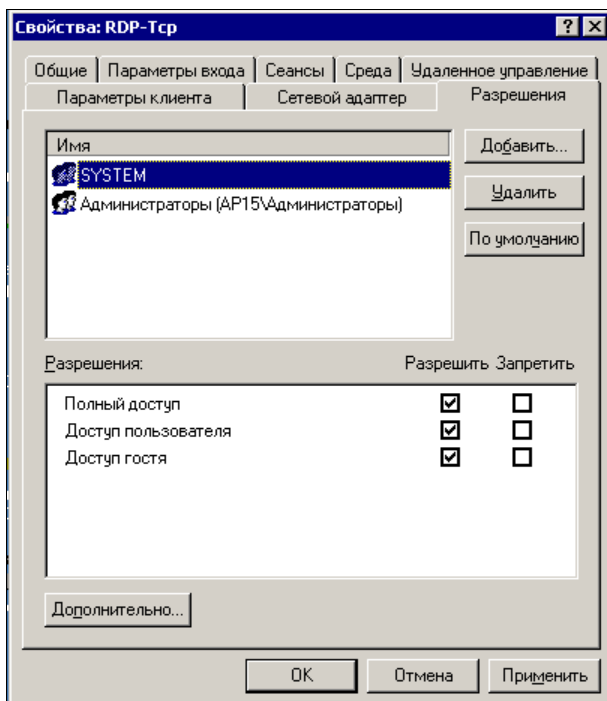


Рис. 9.38. Окно Свойства: RDP-Тср, вкладка Разрешения

## Параметры сервера

На рис. 9.39 показано, какие параметры сервера может настроить администратор.

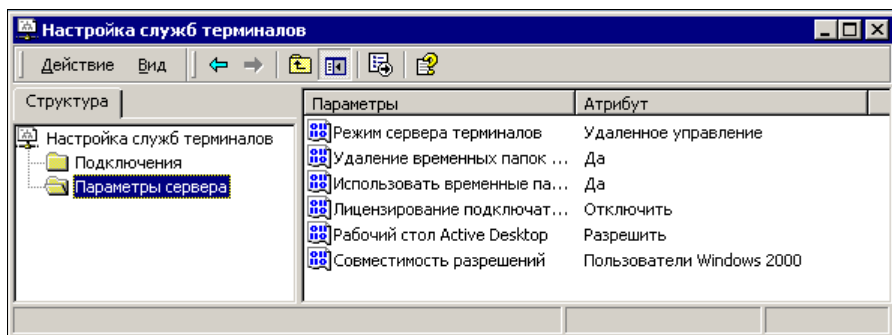


Рис. 9.39 Окно Настройка служб терминалов (Параметры сервера)

- Режим сервера терминалов** — режим сервера приложений или удаленного управления.
- Удаление временных папок при выходе** — на время работы клиентского сеанса на сервере создается временная рабочая папка, которую можно удалять или не удалять по окончании работы сеанса.
- Использовать временные папки для сеанса** — создавать или нет отдельные временные папки для каждого сеанса.
- Рабочий стол Active Desktop** — отключать или нет.
- Совместимость разрешений** — разрешения Windows NT 4.0 или Windows 2000 (в данном режиме некоторые приложения, разработанные без учета специфики Windows 2000, могут не работать).

## Свойства пользователей

Некоторые свойства пользователей позволяют настраивать работу пользователей с сервером терминалов.

Вкладка **Удаленное управление** позволяет предоставить системному администратору право на перехват управления сеансом пользователя и определить, каким образом он будет это делать — с разрешения пользователя или без его разрешения. Кроме того, можно задать уровень управления — только наблюдение за сеансом или взаимодействие с ним.

Вкладка **Профиль служб терминалов** позволяет определить место расположения профиля пользователя и домашнего каталога в сеансе работы с терминальным сервером, а также разрешение на использование терминальной службы.

Вкладка **Среда** позволяет включить запуск конкретного приложения в сеансе работы и подключение локальных устройств пользовательского ПК, при этом работать с локальными дисками можно только как с сетевыми из терминального сеанса.

Вкладка **Сеансы** — настройка тайм-аутов работы клиентской сессии.

Чтобы перехватить управление сессией какого-либо пользователя, администратор должен выбрать в диспетчере терминальных служб нужную сессию, щелкнуть правой кнопкой мыши и выбрать в меню пункт **Удаленное управление**. Если администратор должен запрашивать разрешение пользователя, то у пользователя появится панель с соответствующим запросом. Если он разрешит передать управление администратору, то последний получает его. Уровень управления чужой сессией опять же зависит от свойств конкретного пользователя — либо только наблюдение за сеансом, либо взаимодействие с ним, т. е. администратор работает в сеансе пользователя, как в своем собственном. Данная возможность позволяет администратору решить многие проблемы пользователей, находясь на своем рабочем месте. Администратор может вернуться в свою сессию, нажав комбинацию клавиш <Ctrl>+<\*> (клавиша <\*> нажимается на дополнительной цифровой клавиатуре).

Для успешной работы с выделенным сервером, независимо от режима, в котором он работает, необходимо настроить рабочие станции. Об этом далее в *главе 10*.

## Операционная система для рабочей станции

Теперь поговорим о рабочей станции. Здесь выбор операционной системы может быть существенно шире. Несмотря на бурное развитие Windows и возможность применения Windows Server 2003 в качестве ОС для рабочей станции, вполне возможно применение и Windows 98. Последние реализации этой системы достаточно стабильны при работе с офисными приложениями и в локальной сети. В сети предприятия, где мне выпало работать, до настоящего времени есть машины под управлением этой операционной системы. Зачем менять ее, если для этого потребуется менять и сам компьютер? Если система обеспечивает потребности пользователей, работает без сбоев, то и пусть себе работает. Другое дело — выбор системы для нового компьютера. Здесь есть над чем подумать.

Наиболее распространенная в наше время ОС для рабочих станций — Windows XP. Об установке и настройке этой системы можно прочитать по адресу <http://www.hardwareportal.ru/Handmade/Windows.work/index.html>.

Но в большинстве случаев пользователю не требуется выполнять таких сложных процедур, которые описаны в этой статье. Достаточно просто вставить в дисковод диск с дистрибутивом и ответить на несколько вопросов, которые будут выведены на экран в процессе установки. Простота установки и универсальность Windows XP сделали ее самой популярной в настоящее время. Поддержка практически всех современных технологий работы с мультимедийными программами и файлами, наличие очень удобного комплекта офисных программ от Microsoft сделала эту систему почти незаменимой для обычных пользователей ПК.

В последнее время получила распространение и Windows 7 с офисным пакетом MS Office 2007. Установка системы и офисного пакета не сложнее, чем в более ранних версиях, но требования к ресурсам компьютера выше.

Но существуют офисные пакеты не только от гиганта софтверной индустрии. Есть, например, OpenOffice, который выпускается в версиях как для Windows, так и

для Linux. Да кроссплатформенные и мультимедийные приложения тоже существуют. А это значит, что для небольшого офиса или для домашнего применения вполне может быть использована какая-нибудь другая ОС. Одна из перспективных для российских пользователей разработок — Linux XP (<http://www.linux-online.ru/desktop>). Интересно, что Linux XP разрабатывалась специально для пользователей, привыкших к Windows. Разработчики системы попытались максимально облегчить переход пользователей Windows на эту систему. В то же время в условиях небольшого офиса, где пользователи должны выполнять определенную работу и не отвлекаться на развлечения, администратор может защитить ее от деструктивных действий пользователя.

Надо сказать, что различные версии Linux в большинстве случаев содержат в своем дистрибутиве все необходимое для работы как на рабочей станции, так и на сервере. Из всех вариантов Windows, пожалуй, таким свойством обладает только Windows Server 2003, которую можно настроить и для рабочей станции, приложив некоторые усилия. Правда, цена этой ОС очень сильно отличается от бесплатных версий Fedora или совсем недорогой Linux XP. Причем в дистрибутив Linux включен обычно и OpenOffice, который в последних версиях совместим с Microsoft Office в такой степени, что для большинства пользователей будет одинаково удобно работать в любом из этих офисных пакетов.

Посетите страницу <http://ru.openoffice.org/about-product.html>. На ней вы сможете узнать подробности об OpenOffice (скачать ее можно со страницы <http://www.i-rs.ru/download>), а на странице <http://www.videolan.org/> есть информация о кроссплатформенном мультимедийном плеере VCL, который, возможно, заменит вам MP10 (Media Player 10 версии) от компании Microsoft. На странице <http://chelcom.ru/modules/smartsection/item.php?itemid=95> есть довольно подробные инструкции по настройке этого медиаплеера на русском языке (сам медиаплеер поддерживает русский язык). Windows-версии этих программ позволят опробовать их в среде Windows XP.

## Еще немного информации об ОС

Выбирая систему для сервера, мы не акцентировали внимания на его назначении. Windows Server 2003 и Linux Fedora Core позволяют сконфигурировать сервер практически любого назначения. Но для расширения кругозора, а также для ознакомления с некоторыми операционными системами, которые в нашем обзоре оказались за кадром, пройдите по ссылке [http://www.ccc.ru/magazine/depot/97\\_05/read.html?0804.htm](http://www.ccc.ru/magazine/depot/97_05/read.html?0804.htm), где помещена статья "Выбираем платформу для сервера Интернет".

Статья не очень новая. Но присутствующего в ней материала вполне достаточно для понимания особенностей нескольких операционных систем, которые при всех своих достоинствах не очень подходят для малых офисов и домашних сетей.

Кроме того, упомянутая в начале главы DOS тоже может быть применена для организации Web-сервера. Все зависит от потребностей и возможностей, а также желания администратора экспериментировать.

Пожалуй, теперь можно составить перечень операционных систем, которые можно применять в практике начинающих системных администраторов, не имеющих наставников по UNIX:

- DOS;
- Windows 98;
- Windows 2000, Windows 2000 Server;
- Windows XP (Professional и Home Edition);
- Windows Server 2003;
- Windows Server 2008
- Windows Vista;
- Windows 7;
- Linux Fedora Core (3, 4, 5);
- Linux XP (Pro);
- Mandriva Linux 2008.

Существуют и используются и другие ОС, в том числе достаточно распространенные, но не перечисленные здесь. Конечно, если вы хотите испытать малораспространенную в России ОС, никто вам этого не запретит. Но если вы хотите иметь работающую сеть, то лучше ориентироваться на уже испытанные многими пользователями системы. Если же вас заинтересует мир Linux, то вы без труда найдете в Интернете множество ссылок, которые помогут вам узнать об этих системах, а при желании скачать их дистрибутивы. Приобрести дистрибутив Linux можно через сайт <http://www.linuxcenter.ru/>, где можно найти и множество полезных публикаций о Linux.

Более конкретно о реализации серверов различного назначения мы еще будем говорить. А пока в следующей *главе 10* попробуем разобраться в мире файловых систем, познакомимся с рекомендациями по их выбору, которые можно встретить на просторах Интернета. Возможно, что для кого-то из начинающих администраторов и пользователей ПК этот материал будет полезен и поможет правильно выбрать файловую систему как для сервера, так и для рабочей станции.

# ГЛАВА 10



## Выбираем файловую систему

Операционная система не может быть установлена просто на новый винчестер, если его предварительно не подготовить. Вначале на диске необходимо создать файловую систему, разбить на разделы и логические диски, отформатировать логические диски.

Различные операционные системы могут требовать для своей установки и различные файловые системы. Кроме того, одна и та же операционная система может поддерживать установку на диски с различными файловыми системами. И еще, вполне вероятно, что вам потребуется установить не одну операционную систему на ваш компьютер. В этом случае могут понадобиться несколько файловых систем одновременно. А если устанавливается Linux, то несколько файловых систем могут потребоваться для установки одной операционной системе. Давайте рассмотрим наиболее распространенные файловые системы применительно к возможности их использования для установки распространенных ОС.

□ NTFS и NTFS5 — в настоящее время самая распространенная файловая система на персональных компьютерах. NTFS5 — модификация этой файловой системы, обладающая несколько более широкими возможностями:

- индексация файлов по параметрам;
  - оптимизация дискового пространства;
  - усовершенствованный механизм обеспечения безопасности;
  - возможность монтирования томов;
  - возможность подсоединения каталогов;
  - квотирование дискового пространства
- и др.

Более подробно о NTFS5 можно прочитать по ссылке <http://www.sdteam.com/?tid=1169>.

Большинство компьютеров с установленными ОС Windows XP, Windows 2000 или Windows Server 2003 имеют на своих дисках эту файловую систему.

- FAT32 — более простая по сравнению с NTFS файловая система. Появилась вместе с операционной системой Windows 95 и широко применяется для Windows 98. Не обладает такими возможностями, как NTFS, менее надежна, но ее относительная простота позволяла восстанавливать пропавшую на дисках информацию даже вручную (применялись редакторы дисков). Более ранние версии FAT — FAT16, FAT12 отличаются в основном тем, что применять их можно для дисков весьма ограниченного объема. Старые операционные системы (различные версии DOS) не всегда могут быть установлены на FAT32, и тем более на NTFS. Но Windows XP, например, вполне уживается с FAT32, хотя и с потерей уровня безопасности и надежности системы. С загрузочной дискеты, подготовленной стандартными средствами Windows 98, можно увидеть разделы дисков, отформатированных в FAT32 и во всех более старых версиях FAT.

## Сравнительная характеристика NTFS и FAT32

На странице <http://www.abc-it.lv/index.php/id/1125> можно увидеть сравнительную характеристику файловых систем NTFS и FAT32. Приведем эту характеристику здесь.

### NTFS

#### *Достоинства:*

- быстрая скорость доступа к файлам малого размера;
- размер дискового пространства на сегодняшний день практически не ограничен;
- фрагментация файлов не влияет на саму файловую систему;
- высокая надежность сохранения данных и собственно самой файловой структуры;
- высокая производительность при работе с файлами большого размера.

#### *Недостатки:*

- более высокие требования к объему оперативной памяти по сравнению с FAT32;
- работа с каталогами средних размеров затруднена из-за их фрагментации;
- более низкая скорость работы по сравнению с FAT32.

### FAT32

#### *Достоинства:*

- высокая скорость работы;
- низкое требование к объему оперативной памяти;
- эффективная работа с файлами средних и малых размеров;
- более низкий износ дисков, вследствие меньшего количества передвижений головок чтения/записи.



### *Недостатки:*

- низкая защита от сбоев системы;
- неэффективная работа с файлами больших размеров;
- ограничение по максимальному объему раздела и файла;
- снижение быстродействия при фрагментации;
- снижение быстродействия при работе с каталогами, содержащими большое количество файлов.

Обе файловые системы подходят для применения на рабочих станциях, но FAT32 не позволит управлять разрешениями на доступ к каталогам и файлам так гибко, как это возможно в NTFS. В то же время в аварийной ситуации, когда система не может быть загружена, доступ к файлам в FAT32 может быть обеспечен очень простыми средствами, тогда как для доступа к NTFS-дискам придется применять более сложные методы и программы.

## **Некоторые выводы**

Учитывая надежность NTFS и NTFS5, только эти системы можно применять на сервере и ответственных сетевых рабочих станциях. Но для обеспечения возможности быстрого доступа к файлам при аварийных ситуациях эти файлы можно хранить на разделах, отформатированных в FAT32.

Если у вас устаревший компьютер, на который все же можно установить Windows XP, например, лучше форматировать системный раздел в FAT32, что обеспечит большее быстродействие этой машины. Следует только иметь в виду, что FAT32 не поддерживает логические диски более 20 Гбайт.

## **Теперь немного о файловых системах для Linux**

Linux поддерживает очень много файловых систем, в том числе FAT(32), HPFS, UFS и многие другие, но в качестве рабочих файловых систем рекомендуется использовать только ext2, ext3, ext4, ReiserFS, XFS, а также специализированные файловые системы: devfs, tmpfs, proc, devpts, romfs. Практически все новые версии Linux могут обращаться и к NTFS. Есть еще сетевая файловая система NFS, которая позволяет Linux-машинам обращаться к сетевым ресурсам, как к локальным.

Несмотря на большое количество поддерживаемых файловых систем, большая часть дистрибутивов базируется на единой для всей системы файловой системе ext2, ext3 или ext4.

При этом ext3 отличается тем, что имеет возможность отслеживания транзакций, информация о которых записывается в журнал системы. Это делает ext3 очень надежной, что объясняет ее широкое применение на серверах. Особенности ОС Linux позволяют монтировать диски с различными файловыми системами, делая работу с ними одинаково комфортной. Так Linux Mint, установленная вместе с Windows XP

или Windows 7 на одной машине, позволяет читать файлы на разделах NTFS (запись некорректна), а на разделах FAT32 возможна и корректная запись файлов. Из Windows обращение к ext2, ext3 или ext4 невозможно.

Отсюда напрашивается еще один вывод: *установка Linux, например в качестве второй системы на рабочей станции, делает всю систему несколько надежнее.* Проблема с загрузкой Windows не приведет к потере ваших файлов, а посещение Интернета из Linux позволит вам чувствовать себя в большей безопасности, поскольку вирусов под Linux очень мало, а защищенность системы при выполнении основных рекомендаций по работе с ней весьма высока.

При установке Linux следует учитывать, что диск для этой системы необходимо разбить, как минимум, на три раздела. Для работы системы требуется загрузочный, swar- и системный разделы. Причем для swar-раздела обычно не требуется файловая система. В этот раздел при необходимости будет записываться содержание оперативной памяти. Загрузочный раздел (boot) имеет файловую систему VFAT или ext2, основной системный раздел (root) ext3 или ext4.

Суммарный необходимый размер разделов для большинства распространенных версий Linux не превышает 10 Гбайт, а разбиение диска может выполняться автоматически при установке системы. Следует, конечно, учитывать, что для установки дополнительных программ и сохранения ваших собственных файлов потребуется дополнительное место на диске.

Я думаю, что у вас уже сложилось представление, какую файловую систему и в каких случаях следует применять.

Но важно помнить, что самая надежная файловая система может испортиться по независящим от нее причинам. Жесткие диски не вечны. Для контроля исправности файловой системы, для резервного копирования разделов диска, для оптимизации размеров разделов на диске и многих других операций с файловыми системами существуют специальные утилиты. Так, в дистрибутиве Linux всегда можно найти GParted, предназначенную для управления разделами на диске. Использовать такие утилиты прямо из работающей системы не всегда удобно. Для того чтобы выполнить действия с разделом, его надо отмонтировать, чтобы система не использовала занятое им дисковое пространство. Поэтому были разработаны загрузочные диски с комплектом необходимых утилит.

## Parted Magic

Со страницы <http://partedmagic.com/download.html> можно загрузить образ диска, содержащего Linux и несколько полезных для работы с разделами утилит. Если у вас есть компьютер без CD-привода, установив программу UnetBootin (в дистрибутиве Linux Mint она есть), вы можете без труда создать загрузочную флэшку. Вид программы приведен на рис. 10.1.

В программе необходимо выбрать образ диска, который вы хотите поместить на флэшку, и сам USB-накопитель. Другие опции оставим по умолчанию.

Поскольку для системы требуется около 200 Мбайт, то остальное пространство можно использовать для хранения нужных файлов и сохранения файлов из "упавшей" системы. Для создания такого хранилища на флэшке ее необходимо обрабо-

тать с помощью утилиты GParted, уменьшив размер загрузочного раздела и создав раздел для хранения файлов. Окно программы приведено на рис. 10.2.

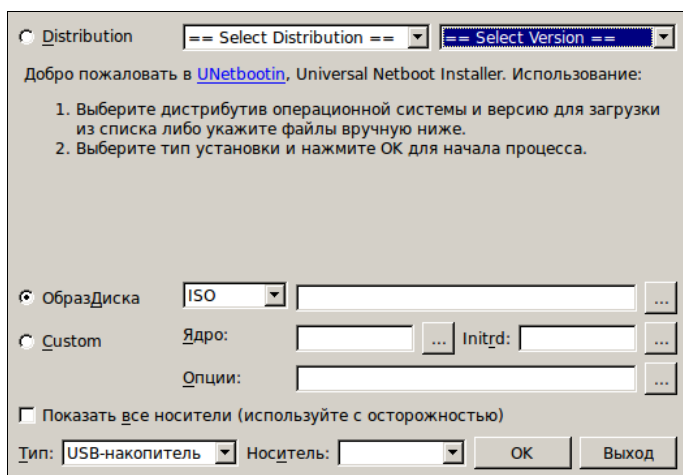


Рис. 10.1. Окно программы UnetBootin

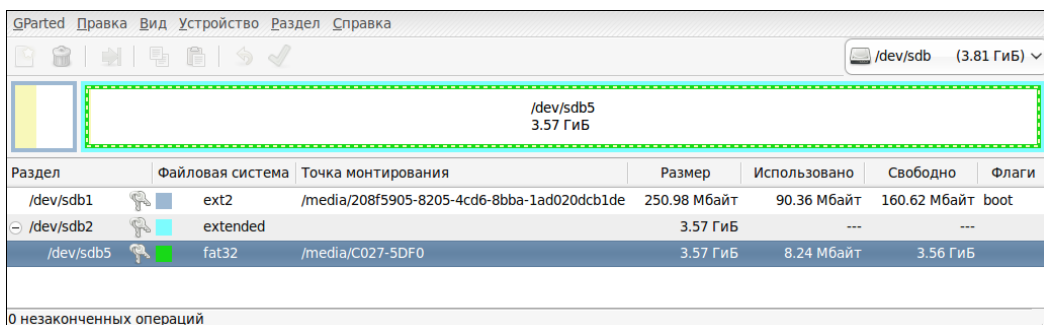


Рис. 10.2. Окно программы GParted

В выпадающем списке в правом верхнем углу окна выберите ваш накопитель, используя меню **Раздел**, размонтируйте все разделы накопителя и измените их размеры.

После загрузки с такой флэшки (рис. 10.3) дополнительный раздел будет доступен как отдельный диск. Из Windows дополнительный раздел может не читаться, но нам это и не требуется. Если придется работать с Windows-разделами, загружена будет Linux.

Прямо на экране вы можете увидеть некоторые полезные сведения о системе. Утилита GParted запускается с помощью ярлычка **Partition Editor**.

Кнопка в виде изображения компакт-диска в левом нижнем углу — меню системы. Из него вы можете получить доступ к нескольким утилитам, в том числе Clonezilla. Это программа работает в текстовом режиме, но при запуске начинает работать мастер, который помогает клонировать разделы и сохранять на других дисках.



Рис. 10.3. Экран Parted Magic

Parted Magic — это по сути полноценная операционная система с набором программ первой необходимости. Кроме специальных утилит, она содержит интернет-браузер, программу для просмотра графических файлов (viewer), текстовый редактор, медиаплеер и многое другое. Обслуживая компьютер, можно послушать музыку и посетить страницы в Интернете. Для получения доступа к дополнительному разделу на флэшке воспользуйтесь утилитой Mount Devices (ярлык на рабочем столе).

# ГЛАВА 11



## Устанавливаем виртуальный компьютер

Зачем столько внимания какой-то виртуальной системе? — спросите вы. На самом деле, что, кроме возможности проводить эксперименты с различными ОС, может дать виртуальная машина серверу?

А дать она может много, и даже очень много. Попробуем перечислить преимущества, которые можно получить, используя виртуальную машину для сервера.

- ❑ Возможность моментального восстановления сервера в рабочее состояние после вирусной атаки, атаки хакеров или другой причины, приведшей к серьезным проблемам на сервере. Эта возможность достигается всего лишь копированием рабочего файла диска виртуальной машины и заменой испорченного на исправную копию, при необходимости.
- ❑ Возможность размещения на одном физическом сервере более одного виртуального сервера. Это могут быть Web-сервер и пара серверов, принадлежащих разным подсетям. Серверы, несмотря на размещение на одной машине, совершенно независимы друг от друга. Единственное ограничение — число виртуальных серверов. Это ограничение обусловлено ресурсами хост-машины. Реальный компьютер должен обладать ресурсами, достаточными для обеспечения одновременной работы виртуальных машин.
- ❑ Возможность быстрой замены сервера на другую версию. Это может быть полезно при обучении пользователей, когда в течение одного занятия необходимо рассмотреть работу и настройки двух-трех вариантов сервера. При этом учащиеся могут совершенно безбоязненно самостоятельно проводить настройки сервера. Даже самые грубые ошибки не приведут к серьезным проблемам, ведь заменить сервер очень просто!
- ❑ Упрощение настроек базового физического сервера (хост-машины), что в свою очередь ускоряет и упрощает восстановление работоспособности сервера при серьезной аварии. Повышение надежности базового сервера. Вызывающие нестабильность в работе системы установки и переустановки программ выполняются только на виртуальных машинах.
- ❑ Возможность дистанционного восстановления работоспособности серверов. Достаточно иметь удаленный доступ к базовой машине. К счастью, в наше вре-

мя вариантов такого доступа может быть несколько, а один из весьма надежных — терминальный доступ возможен средствами Windows.

- Возможность размещения на одной физической машине одновременно работающих серверов под принципиально различными операционными системами, — Windows и Linux могут работать на одном компьютере одновременно.
- Возможность совершенно без риска для работы сервера испытывать различные программы, пригодность которых для ваших условий точно не установлена. Если в результате опыта выяснилась непригодность программы, то замена файла сервера позволяет полностью уничтожить следы установки программы, сохранив систему в максимально чистом виде.

Пожалуй, достаточно. Надо и вам дать возможность найти свои доводы в пользу виртуального сервера. Если кому-то покажется, что уже все сказано, то это может значить только то, что вы еще не вошли во вкус. Еще не опробовали работу с виртуальным сервером в полной мере. Если вы системный администратор или собираетесь им стать, то сможете найти еще с десятков плюсов у виртуального сервера. В каждой конкретной ситуации эти плюсы могут быть разными, но они есть всегда.

Понимание полезности виртуального сервера есть. Остается понять, как же установить этот сервер? Для этого существуют специальные программы. Среди них наиболее известны программы от Microsoft и VMware.

## Что можно установить?

Для кого-то покажется удивительным, но Microsoft предлагает нам виртуальный сервер Microsoft Virtual Server совершенно бесплатно! Требуется только регистрация перед загрузкой файлов. Получить этот сервер можно по адресу: <http://www.microsoft.com/windowsserver/system/virtualserver/software/default.mspx>.

Предварительно можно почитать описание этого сервера на странице:

[http://zeus.sai.msu.ru:7000/operating\\_systems/virtserver/](http://zeus.sai.msu.ru:7000/operating_systems/virtserver/).

Также бесплатно можно скачать и VMware Server, который аналогично продукту от Microsoft предназначен для создания виртуального сервера и управления им локально или удаленно через Web-интерфейс.

VMware также предлагает VMware Player, с помощью которого можно "проигрывать" виртуальные машины, созданные с помощью программ различных производителей (VMware GSX Server, VMware ESX Server, Microsoft Virtual PC и образы Symantec LiveState Recovery). Таким образом, создав виртуальную машину в доступной вам программе, вы можете перенести ее на любой другой компьютер, где установлен VMware Player. Если виртуальная машина была создана не средствами VMware, например MS Virtual PC, то плеер автоматически импортирует файлы, преобразуя в свой формат. Подобно Adobe Acrobat Reader, который предназначен для чтения популярных PDF-файлов, VMware Player может "читать" созданные кем-либо виртуальные машины. Вы можете сами создавать виртуальные системы с помощью VMware Workstation или бесплатных виртуальных серверов от Microsoft или VMware, распространяя их среди других пользователей ПК. Новому пользова-

телю виртуальной системы даже не придется искать драйверы. После запуска в плеере драйверы устанавливаются автоматически. У автора не возникло проблем при переносе виртуальной машины, созданной на самостоятельно собранном персональном компьютере, на ноутбук HPCompaq.

Познакомиться с другими продуктами VMware можно на странице <http://www.vmware.com>. Фирма предлагает не только программы для создания и запуска виртуальных систем, но и сами системы. После установки VMware Player можно скачать множество примеров виртуальных машин, одна из которых содержит в себе ОС Linux Ubuntu и браузер Firefox. Предназначена эта виртуальная машина для безопасного просмотра интернет-страниц. Как и любая другая виртуальная машина, Browser Appliance замкнута в себе. Никакие вирусы и опасные программы не смогут проникнуть в базовую или другую виртуальную систему. Эту виртуальную машину можно найти на странице <http://www.vmware.com/vmtn/appliances/directory/browserapp.html>.

## Установка Microsoft Virtual Server 2005 R2

Выбор этого сервера может быть обусловлен относительной простотой его настройки. Опыт других пользователей говорит о том, что на этот сервер можно установить не только Windows XP и серверные версии Windows, но и Linux. Интерфейс сервера не очень удобен для работы в виртуальной системе, хотя и позволяет это делать, но зато системой можно управлять дистанционно через Web-интерфейс с любого компьютера сети или даже... через Интернет! Компания Microsoft предлагает также инструментальный набор *Virtual Server Migration Toolkit* (VSMT) в качестве бесплатного дополнения для Virtual Server. Набор можно загрузить по адресу <http://www.microsoft.com/widowsserversystem/virtualserver/evaluation/vsmt.mspx>. С помощью VSMT можно преобразовать физические машины в VM, а виртуальные машины VMware в VM — в совместимые с Virtual Server (Компания VMware предлагает аналогичный продукт VMware P2V Assistant, но его нужно приобретать отдельно.) Большинство пользователей Windows смогут без значительных проблем установить и освоить этот продукт.

Перед установкой виртуального сервера следует проверить, установлен ли у вас в системе компонент Internet Information Services Manager из состава Internet Information Services (IIS) (рис. 11.1). Если компонент не установлен, то установите его. В системе Windows 2003 Server этот компонент находится в составе сервера приложений. На клиентском компьютере, где будет установлен Virtual Machine Remote Control (клиент удаленного контроля), никаких дополнительных компонентов не требуется.

Установка сервера не отличается от установки большинства обычных программ под Windows. Достаточно запустить на выполнение скачанный файл Setup.exe, и для первой установки ничего не изменять в параметрах установки по умолчанию. На физическом сервере, где будет установлен виртуальный сервер, следует выполнить полную установку. Дополнительно можно установить компонент Virtual Machine Remote Control (клиент удаленного контроля) на рабочую станцию, сняв отметки с остальных компонентов сервера во время установки.

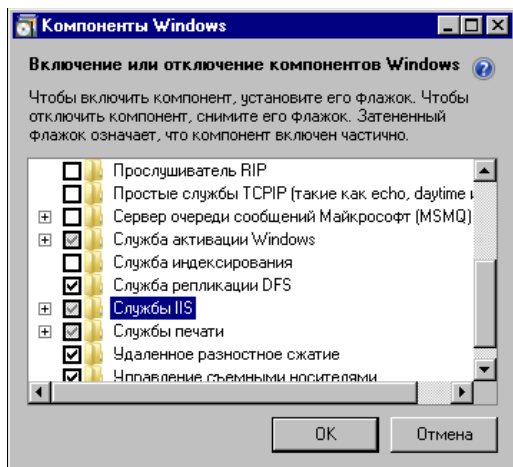


Рис. 11.1. Окно Компоненты Windows

После установки виртуального сервера в окне браузера откроется страница с информацией о результатах установки (рис. 11.2).

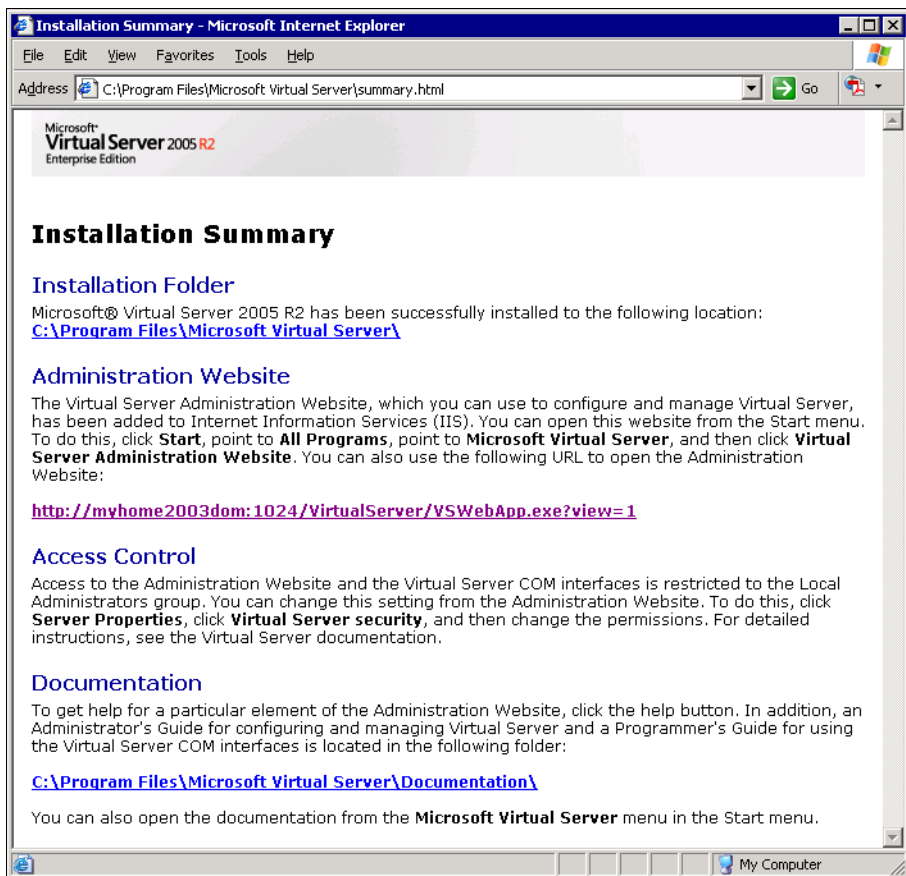


Рис. 11.2. Окно браузера Installation Summary (Результат установки)



В этом окне указаны пути, куда установлены компоненты программы, а также ссылка на Web-интерфейс администратора. Щелкнув по ссылке, вы можете вызвать этот интерфейс. Выбрав в меню страницы пункт **Virtual Machines | Create** (Виртуальные машины | Новая), вы попадете в интерфейс создания новой виртуальной машины (рис. 11.3).

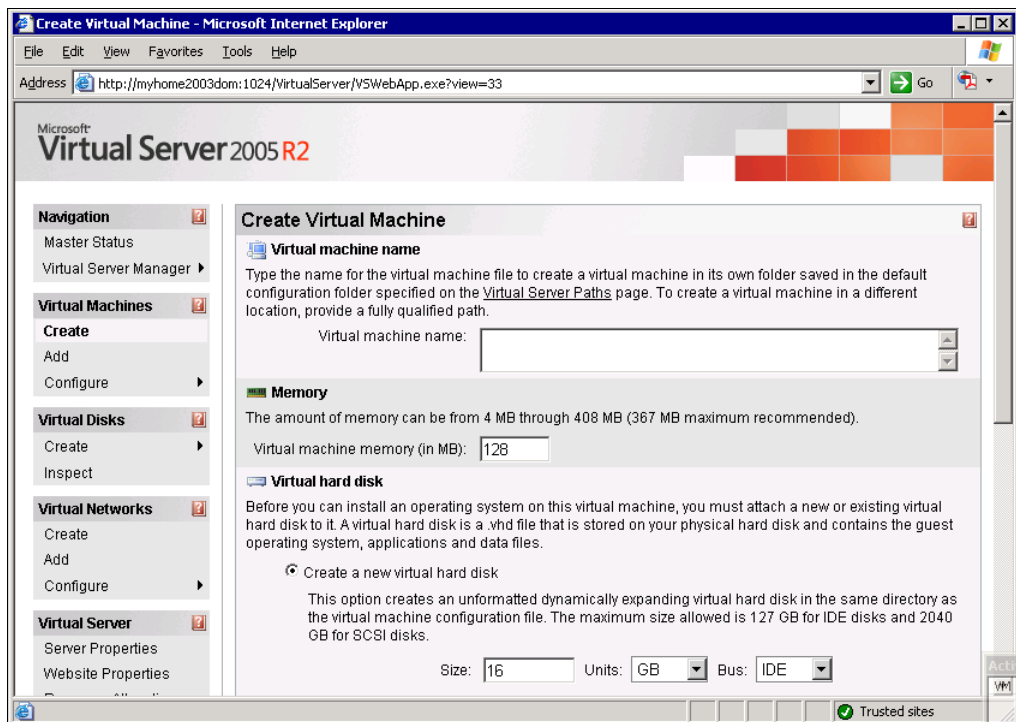


Рис. 11.3. Окно браузера **Create Virtual Machine** (Создание виртуальной машины)

Задав имя виртуальной машины, указав размер оперативной памяти для нее, размер и тип виртуального жесткого диска, а также указав, что должен использоваться физический сетевой адаптер, установленный на вашем компьютере, можно нажимать кнопку **ОК**. В процессе создания виртуальной машины программа предложит отключить автозапуск CD-ROM. Автозапуск будет мешать подключению дисководов к виртуальной машине.

После создания виртуальной машины перейдите в меню **Master Status** (страница состояния сервера) (рис. 11.4).

Из этого окна, воспользовавшись выпадающим меню у имени виртуальной машины, вы можете включить ваш виртуальный компьютер, а если в дисковод компакт-дисков вставлен дистрибутив Windows XP или Windows Server 2003, то можно сразу начать установку системы на виртуальный сервер.

Для того чтобы получить удобное окно управления виртуальной системой, можно щелкнуть по маленькому изображению этого окна в интерфейсе Virtual Machine Status или, воспользовавшись меню **Пуск**, запустить Virtual Machine Remote Control (рис. 11.5).

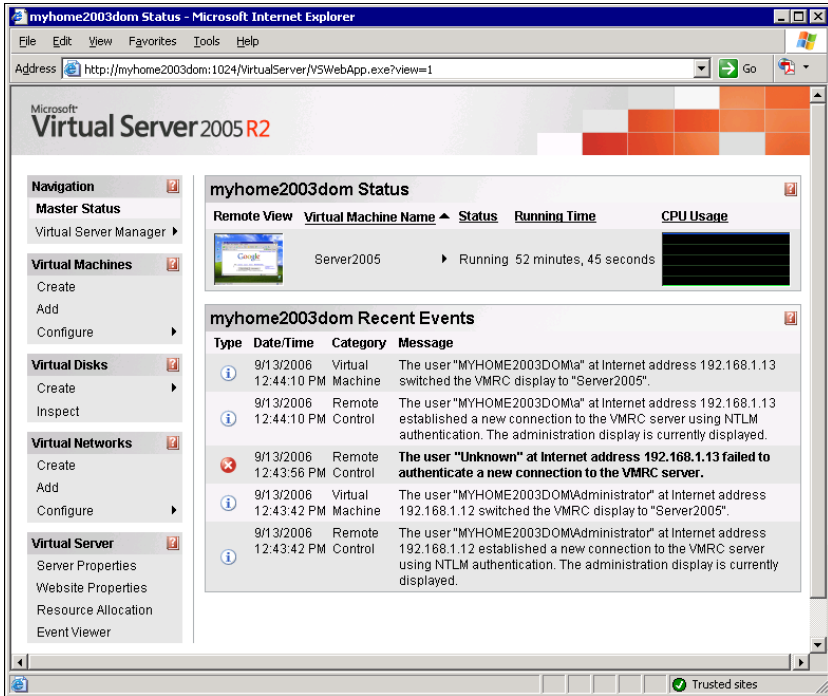


Рис. 11.4. Окно браузера Virtual Machine Status (Статус виртуальной машины)

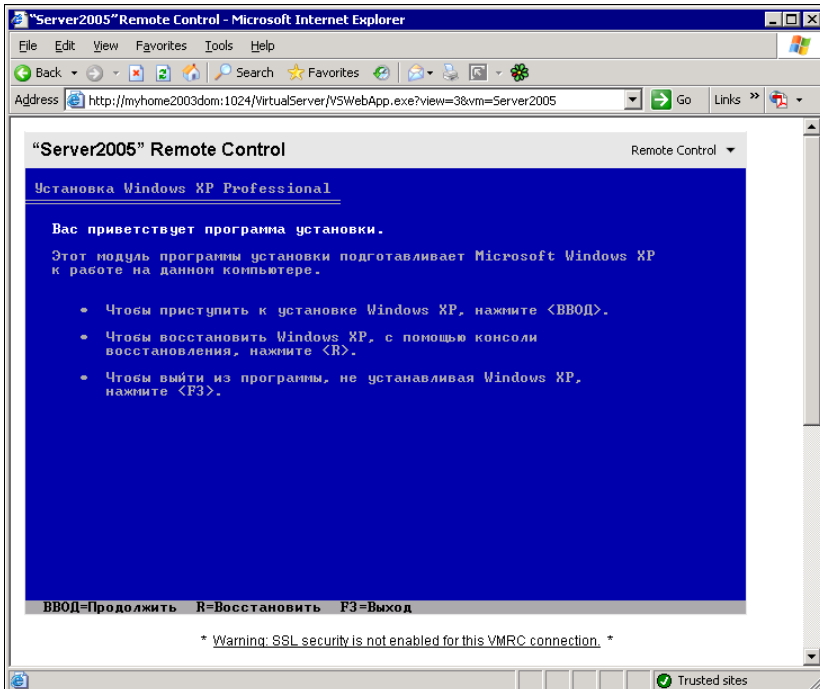


Рис. 11.5. Окно браузера Virtual Machine Remote Control (Клиент удаленного управления), установка системы

Пользуясь этим окном, вы сможете провести установку системы, а в дальнейшем просто работать в системе, производя необходимые настройки сервера (рис. 11.6).

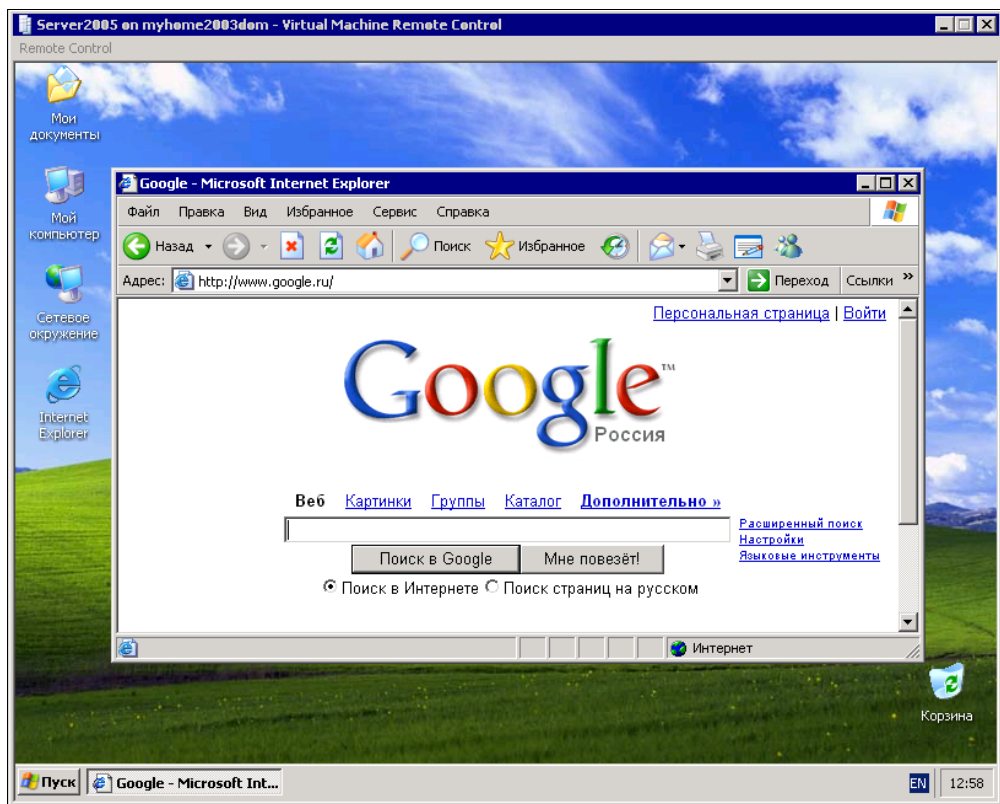


Рис. 11.6. Окно браузера Virtual Machine Remote Control (Клиент удаленного управления), система установлена

Учитывая виртуальность сервера, вы можете создавать любое мыслимое число виртуальных машин, сохранять удачные, уничтожать не понравившиеся вам и запускать несколько виртуальных машин одновременно. При этом браузер Virtual Machine Remote Control позволит переключаться между созданными машинами.

Создав более одного виртуального сервера, вы сможете подключаться с клиентского компьютера к любому из них. Установив на виртуальный сервер серверную версию операционной системы, вы можете осваивать варианты настройки сервера, применив впоследствии полученный опыт.

Некоторые подробности о виртуальном сервере можно найти на страницах [http://soft.mail.ru/article\\_page.php?id=91](http://soft.mail.ru/article_page.php?id=91) и <http://www.osp.ru/text/302/177505/>.

Вполне возможно, что вам не требуется интерфейс управления виртуальным сервером. Можно просто установить виртуальную машину и использовать ее, как обычный физический сервер. В этом случае для удаленного управления виртуальной машиной можно использовать средства удаленного доступа к физическому

серверу. Для управления самой виртуальной машиной можно организовать удаленный доступ прямо к ней. В этом случае можно заранее создать необходимые виртуальные машины, перенести их на физические машины, где они должны работать, а запускать их можно с помощью VMware Player.

## Используем VMware Player

Установка этой программы настолько проста, что описывать ее нет смысла. Единственное, на что можно обратить внимание, — если у вас уже установлена программа VMware Workstation версии ниже чем 5.0, то программа установки потребует ее удалить. Плеер входит в состав VMware Workstation 5.x, а бесплатные обновления для продуктов VMware возможны только в пределах основного номера версии программы. Но сам плеер бесплатный, а устанавливать его лучше на компьютер, где не установлена программа VMware Workstation.

После установки плеера и переноса на компьютер, где он установлен, файлов виртуальной машины можно запустить плеер. Программа выдаст запрос указать конфигурационный файл виртуальной машины, которую необходимо запустить (рис. 11.7).

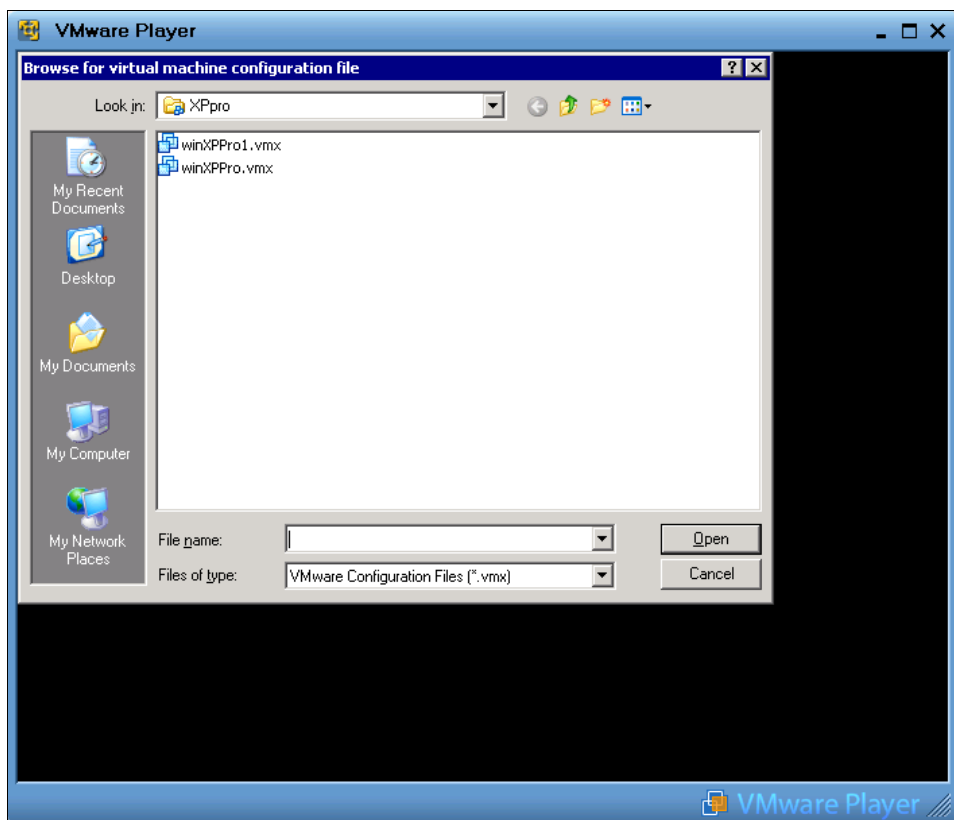


Рис. 11.7. Окно VMware Player (поиск файла конфигурации)

Если ваша виртуальная машина создана средствами Microsoft, то укажите соответствующий тип файла в раскрывающемся списке **Files of type** и выберите необходимый файл. Плеер преобразует виртуальную машину в формат VMware и запустит ее (рис. 11.8).

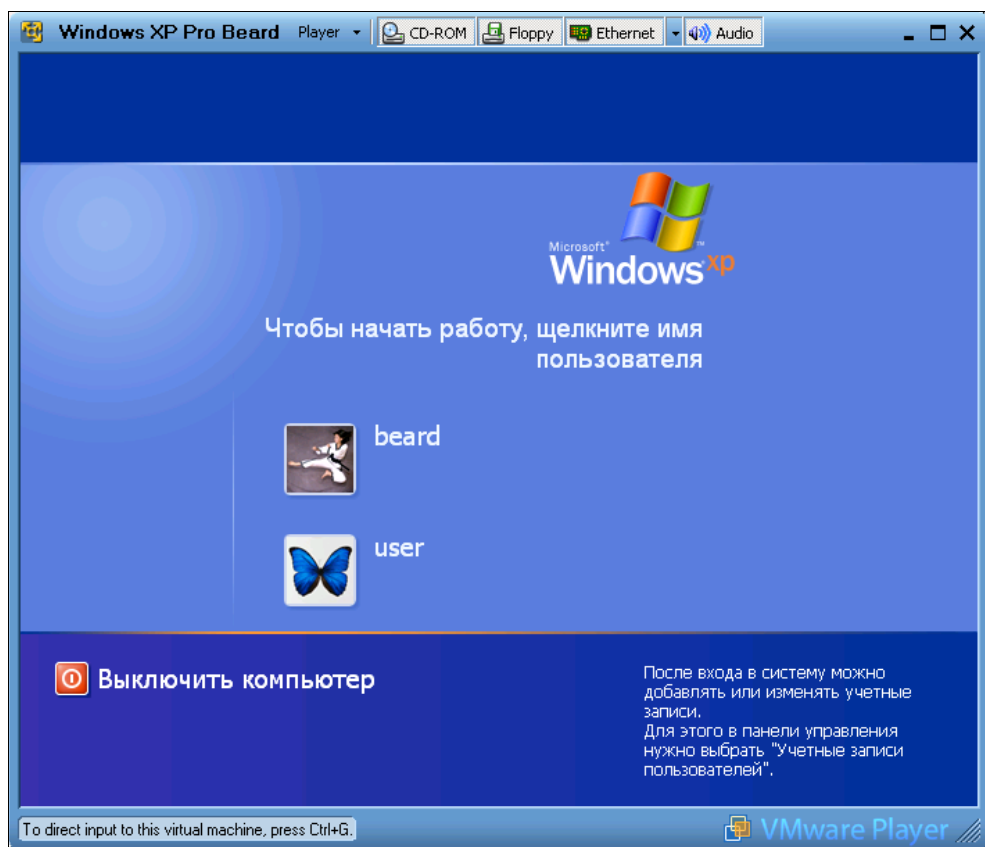


Рис. 11.8. Окно VMware Player (запуск виртуальной машины)

Управление плеером ограничено возможностью отключения и подключения дисководов, сетевой карты и аудиосистемы. Все свойства виртуального компьютера определяются во время его создания. Тем не менее, вам ничто не мешает устанавливать и переустанавливать операционную систему виртуального компьютера, выполнять в ней любые настройки. Соответственно, установив серверную операционную систему, вы можете настроить полноценный сервер.

Можно установить на один физический компьютер более одного виртуального сервера. Особенно интересен вариант, когда каждый из виртуальных серверов выполняет свою определенную задачу. В этом случае вы можете, совершенно ничем не рискуя, заменить, например, почтовый сервер, оставив без изменения файловый и Web-сервер. Если не понравилась работа нового сервера, то просто запустите старый файл сервера!

## VMware Server

Этот виртуальный сервер может быть установлен не только на машину с Windows, но и на компьютер с ОС Linux, как и VMware Player.

Загрузить VMware Server и VMware Player в версиях для Linux можно в Интернете по адресу:

<http://www.vmware.com/download/server/>.

Перед загрузкой потребуется регистрация. Только зарегистрировавшись, вы сможете получить серийные номера продуктов в необходимом вам количестве.

В Mandriva Linux установка VMware Player возможна с дистрибутивного диска или из репозитория стандартными средствами системы.

## Замечания по установке VMware Server и VMware Player под Linux

Установка программ под Linux, несмотря на существующие достаточно совершенные средства, не всегда так проста, как под Windows. Проблемы могут быть в разрешении зависимостей или в компиляции модулей устанавливаемой программы под имеющееся ядро Linux. Но первая проблема решается очень просто самой системой, если дистрибутив программы взят из соответствующего ей репозитория. Вторая проблема тоже часто имеет простое решение.

При инсталляции VMware Server и VMware Player на первом этапе вопросов не возникает, и программа устанавливается без проблем, но затем, при попытке запуска установленной программы, система просит выполнить конфигурацию программы для работы с имеющимся ядром. В процессе конфигурации система запрашивает об указании расположения так называемых заголовочных файлов ядра системы. Этот запрос у начинающих пользователей может вызвать недоумение. Приведенный в запросе стандартный путь для поиска этих файлов обычно не существует. Но проблема решается очень просто. Рассмотрим решение для Mandriva Linux — для других Linux действуйте по аналогии.

Откройте утилиту установки и удаления программ (рис. 11.9). В левой части окна **Управление программами** в разделе меню **Разработка** откройте пункт **Ядро**. В правой части окна вы увидите установленные в системе пакеты. Необходимо, чтобы в числе установленных был пакет **kernel-desktop-devel-<версия\_текущего\_ядра\_>mdv**. Если он не отмечен в числе установленных, отметьте его и нажмите кнопку **Применить**. Убедитесь также, что установлены пакеты Libgcc1, gcc, gcc-spp.

После добавления недостающих компонентов установка и конфигурация VMware Server и VMware Player пройдет без проблем.

Далее в листинге 11.1 приведен вывод на экран в окне терминала процесса конфигурации VMware Player с пояснениями, выделенными курсивом.

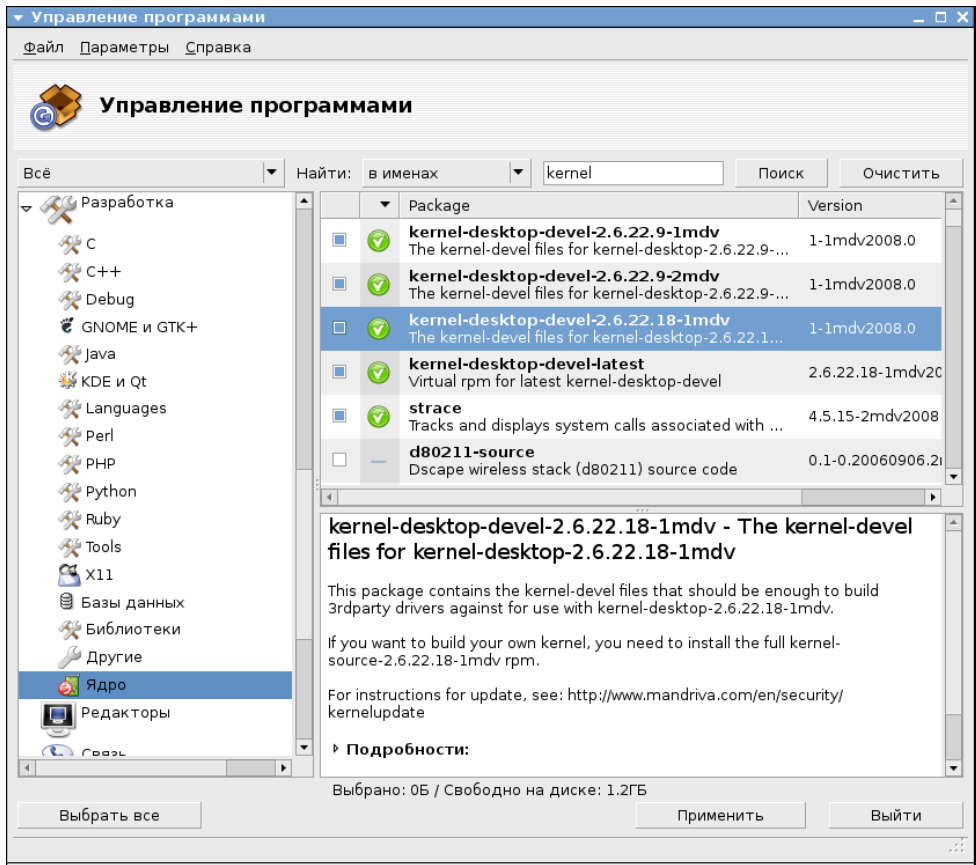


Рис. 11.9. Окно Управление программами (ядро)

### Листинг 11.1. Процесс конфигурации VMware Player

```
[beard@BeardM ~]$ su Прежде всего получаем права администратора (пользователя root), введя команду SU и пароль этого пользователя
```

Пароль:

```
[root@BeardM beard]# vmplayer Вводим команду запуска VMware player
```

vmware is installed, but it has not been (correctly) configured for this system. To (re-)configure it, invoke the following command:

```
/usr/bin/vmware-config.pl. Система сообщает о необходимости конфигурирования программы
```

```
[root@BeardM beard]# vmware-config.pl Вводим предложенную системой команду
```

Making sure services for VMware Player are stopped.

Stopping VMware services:

Virtual machine monitor

[ OK ]

Configuring fallback GTK+ 2.4 libraries.

In which directory do you want to install the theme icons?

[/usr/share/icons] **Нажимаем Enter**

What directory contains your desktop menu entry files? These files have a .desktop file extension. [/usr/share/applications] **Нажимаем Enter**

In which directory do you want to install the application's icon?

[/usr/share/pixmaps] **Нажимаем Enter**

/usr/share/applications/vmware-player.desktop: error: value "vmware-player.png" for key "Icon" in group "Desktop Entry" is an icon name with an extension, but there should be no extension as described in the Icon Theme Specification if the value is not an absolute path

Error on file "/root/tmp/vmware-config0/vmware-player.desktop": Failed to validate the created desktop file

Unable to install the .desktop menu entry file. You must add it to your menus by hand. **Не обращаем внимания на описание ошибки, позднее сделаем значок запуска программы самостоятельно**

Trying to find a suitable vmmon module for your running kernel.

None of the pre-built vmmon modules for VMware Player is suitable for your running kernel. Do you want this program to try to build the vmmon module for your system (you need to have a C compiler installed on your system)? [yes] y  
**Вводим YES или Y и нажимаем Enter**

Using compiler "/usr/bin/gcc". Use environment variable CC to override.

What is the location of the directory of C header files that match your running kernel?

[/lib/modules/2.6.22.18-desktop-1mdv/build/include] **Нажимаем Enter**

Extracting the sources of the vmmon module.

Building the vmmon module.

Using 2.6.x kernel build system.

make: Entering directory `/root/tmp/vmware-config0/vmmon-only'

make -C /lib/modules/2.6.22.18-desktop-1mdv/build/include/.. SUBDIRS=\$PWD SRCROOT=\$PWD/. modules

make[1]: Entering directory `/usr/src/linux-2.6.22.18-desktop-1mdv'

CC [M] /root/tmp/vmware-config0/vmmon-only/linux/driver.o

CC [M] /root/tmp/vmware-config0/vmmon-only/linux/hostif.o

CC [M] /root/tmp/vmware-config0/vmmon-only/common/comport.o

CC [M] /root/tmp/vmware-config0/vmmon-only/common/cpuid.o

CC [M] /root/tmp/vmware-config0/vmmon-only/common/hash.o

CC [M] /root/tmp/vmware-config0/vmmon-only/common/memtrack.o

CC [M] /root/tmp/vmware-config0/vmmon-only/common/phytrack.o

CC [M] /root/tmp/vmware-config0/vmmon-only/common/task.o



```
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciContext.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciDatagram.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciDriver.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciDs.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciGroup.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciHashtable.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciProcess.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciResource.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmciSharedMem.o
CC [M] /root/tmp/vmware-config0/vmmon-only/common/vmx86.o
CC [M] /root/tmp/vmware-config0/vmmon-only/vmcore/moduleloop.o
LD [M] /root/tmp/vmware-config0/vmmon-only/vmmon.o
```

Building modules, stage 2.

MODPOST 1 modules

```
CC /root/tmp/vmware-config0/vmmon-only/vmmon.mod.o
```

```
LD [M] /root/tmp/vmware-config0/vmmon-only/vmmon.ko
```

```
make[1]: Leaving directory `/usr/src/linux-2.6.22.18-desktop-1mdv'
```

```
cp -f vmmon.ko ../../vmmon.o
```

```
make: Leaving directory `/root/tmp/vmware-config0/vmmon-only'
```

The module loads perfectly in the running kernel.

Extracting the sources of the vmblock module.

Building the vmblock module.

Using 2.6.x kernel build system.

```
make: Entering directory `/root/tmp/vmware-config0/vmblock-only'
```

```
make -C /lib/modules/2.6.22.18-desktop-1mdv/build/include/.. SUBDIRS=$PWD
SRCROOT=$PWD/. modules
```

```
make[1]: Entering directory `/usr/src/linux-2.6.22.18-desktop-1mdv'
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/block.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/control.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/dbllnk1st.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/dentry.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/file.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/filesystem.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/inode.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/module.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/stubs.o
```

```
CC [M] /root/tmp/vmware-config0/vmblock-only/linux/super.o
```

```
LD [M] /root/tmp/vmware-config0/vmblock-only/vmblock.o
```

Building modules, stage 2.

MODPOST 1 modules

```
CC /root/tmp/vmware-config0/vmblock-only/vmblock.mod.o
```

```
LD [M] /root/tmp/vmware-config0/vmblock-only/vmblock.ko
```

```
make[1]: Leaving directory `/usr/src/linux-2.6.22.18-desktop-1mdv'
```

```
cp -f vmblock.ko ../../vmblock.o
```

```
make: Leaving directory `/root/tmp/vmware-config0/vmblock-only'
The module loads perfectly in the running kernel.
```

```
Do you want networking for your virtual machines? (yes/no/help) [yes] no
Вводим NO и нажимаем Enter
```

```
Starting VMware services:
```

```
Virtual machine monitor           [ OK ]
Blocking file system:             [ OK ]
```

```
The configuration of VMware Player 2.0.0 build-45731 for Linux for this running
kernel completed successfully.
```

```
You can now run VMware Player by invoking the following command:
"/usr/bin/vmplayer".
```

```
Enjoy,
```

```
--the VMware team
```

```
[root@BeardM beard]#
```

Итак, конфигурация завершена.



Рис. 11.10. Окно VMware Player

Теперь щелкнув правой кнопкой на рабочем столе, выбираем **Создать кнопку запуска**. В открывшемся окне вводим необходимые параметры, среди которых самый важный — это **Команда**. Вписываем — `vmplayer`. Теперь можно указать значок кнопки запуска, выбрав `vmware-player.png` в папке, которая была указана при конфигурации — `/usr/share/pixmaps/`.

Щелкнув по созданному значку, открываем окно **VMware Player** (рис. 11.10).

Кнопка **Download a Virtual Appliance** приведет нас на сайт, откуда можно загрузить уже готовые виртуальные компьютеры, а кнопкой **Open an existing Virtual Machine** можно открыть существующую виртуальную машину, полученную из Интернета или созданную самостоятельно. VMware Server под Linux устанавливается аналогично.

## Соблюдаем лицензии

Может возникнуть вопрос — не потребуется ли для виртуальных машин покупать отдельные лицензии на операционные системы? Ведь в правилах лицензирования ОС сказано:

*"Персональные операционные системы лицензируются по следующему принципу — одна лицензия на один компьютер. Не имеет значения, сколько физических лиц использует компьютер".*

Но на странице <http://www.toms-hardware.ru/business/200512091/index.html> есть указание на то, что в новых правилах лицензирования допускается использовать Windows XP Professional на одной физической и на одной виртуальной машине.

Лицензия на Windows Server 2003 R2 Enterprise допускает одновременное использование системы не более чем на одном физическом сервере и не более чем на четырех виртуальных серверах. Это значит, что на одном физическом сервере с Windows Server 2003 R2 можно установить еще четыре виртуальных сервера с той же ОС. При этом незапущенные копии системы могут храниться в любом количестве. Ограничения есть только на одновременно работающие копии системы.

По адресу:

[http://download.microsoft.com/download/4/7/4/47415510-647d-4847-a554-b5bb33bd44af/Licensing\\_with\\_Microsoft\\_Virtual\\_Server\\_R2.doc](http://download.microsoft.com/download/4/7/4/47415510-647d-4847-a554-b5bb33bd44af/Licensing_with_Microsoft_Virtual_Server_R2.doc)

можно получить документ, подтверждающий ваши права на использование операционной системы на виртуальной машине.

Но в отдельных случаях вам может не хватить разрешенного числа работающих копий. В этом случае вы можете использовать другие операционные системы на виртуальных машинах. Обычно это операционные системы семейства Linux. Но как установить и настроить систему, если у вас нет опыта работы в этих системах?

И здесь есть выход. VMware предлагает на своем сайте несколько десятков готовых виртуальных машин различного назначения!

## Virtual Appliances

Загляните на страницу <http://www.vmware.com/vmtn/appliances/>. На ней можно найти ссылки на готовые виртуальные машины. Virtual Appliances (Виртуальные приборы) — это уже установленные и сконфигурированные под определенные задачи системы.

Browser Appliance (Виртуальный браузер) уже упоминался в начале главы. Автор скачал и запустил этот инструмент с помощью VMware Player. Результаты просто ошеломляющие (рис. 11.11)! Без особого труда удалось подстроить систему под часовой пояс и использование русской раскладки клавиатуры. Были установлены дополнительные программы — текстовый редактор и Macromedia Flash Pleer. Теперь, запуская эту виртуальную машину, можно совершенно безопасно посещать самые рискованные участки Всемирной паутины, при этом не опасаясь проблем на базовой машине. Подключенная флэшка опознала моментально. Любые недостающие компоненты при настройке сети или установке программ моментально скачиваются из Интернета и устанавливаются.

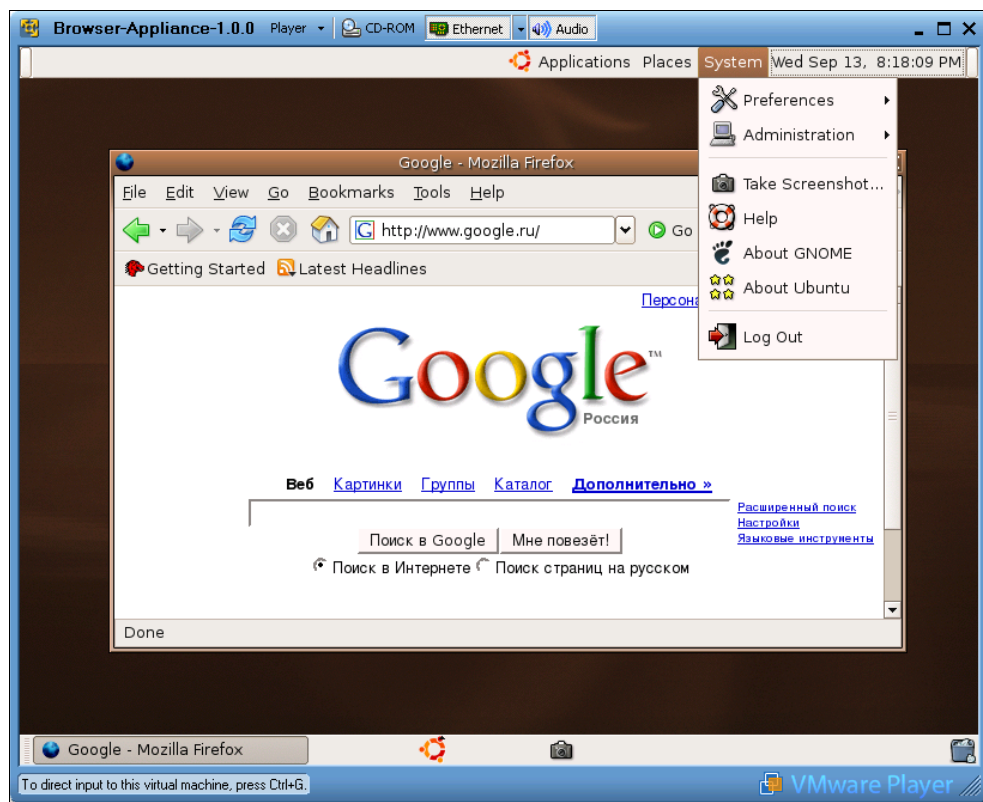


Рис. 11.11. Окно VMware Player с запущенным Browser Appliance и открытым системным меню

Есть Virtual Appliances с почтовым сервером и фильтрами спама, MySQL-сервер, Apache-сервер, маршрутизаторы, специальный Appliance для обеспечения об-

щего подключения к Интернету, прокси-серверы, просто установленные Linux различных версий... всего не перечислишь. Это надо видеть!

К сожалению, многие инструменты имеют довольно большой объем, но современный Интернет позволяет скачивать такие объемы.

Теперь, имея достаточно мощный компьютер, вы можете установить на него несколько серверов или вспомогательных систем. Можно просто своими руками "потрогать" уже настроенные системы. И все это без нарушения лицензий, если вы имеете одну официально приобретенную ОС Windows.

## Виртуальные технологии в нашей сети

Необходимые программы определили, с установкой разобрались. Разберем теперь применение этих программ с пользой для нас и нашей сети и с учетом особенностей рассматриваемых программ.

VMware Player позволяет "проигрывать" имеющиеся у вас виртуальные машины. Следовательно, его можно устанавливать на компьютеры, где не предполагается что-либо изменять в конфигурации виртуальной машины. Если вам определена роль администратора вашей домашней сети, то запланировав применение виртуальной машины на каком-либо компьютере, где работает рядовой пользователь, на него можно установить эту программу. Использовать *виртуальный компьютер* сможет только локальный пользователь.

Если же требуется создание своей виртуальной машины или предполагается удаленное ее администрирование (в рамках вашей сети), то необходим VMware Server.

VMware Server имеет две составляющие. Это собственно сервер, работу которого визуально вы не обнаружите, и консоль управления сервером. Консоль управления может быть запущена на любом компьютере сети и подключена по сети к компьютеру, где установлен VMware Server. При закрытии консоли управления виртуальный компьютер продолжает работать в невидимом режиме. При этом с ним возможен обмен данными по сети. Если ресурсов реального компьютера достаточно для нормальной работы виртуального, пользователь реального компьютера может и не заметить работу виртуальной машины: мешать она не будет.

VMware Server позволяет одновременно запускать более одной виртуальной машины. На современном физическом компьютере одновременно смогут работать два-три виртуальных.

Виртуальные компьютеры, как и обычные, могут быть включены в вашу сеть. Независимо от того, включена консоль управления сервером или нет, в сетевом окружении компьютеры могут быть обнаружены, если их операционные системы загружены.

Гостевые операционные системы на виртуальных компьютерах могут быть любыми. Правда, Windows Vista может работать в VMware Player и VMware Server версий 2 и выше. Текущая стабильная версия VMware Server 1.04 позволяет создать виртуальную машину, на которую можно установить Windows Vista, запустив эту машину в VMware Player.

## Два компьютера в одном

Какую же пользу можно извлечь из виртуальных технологий в домашней сети? Начнем с самого простого. Мы уже говорили о возможности обезопасить себя от атак и вирусов из Интернета путем применения компьютера под Linux для путешествий по глобальной сети. Если у вас нет второго компьютера, вы можете создать виртуальную машину в уже существующем. При этом не придется самостоятельно устанавливать операционную систему. Имея установленный VMware Player или VMware Server, вы можете скачать уже готовый виртуальный компьютер.

### Безопасный браузер

Browser Appliance — так называется *виртуальный компьютер*, предназначенный для посещения Интернета. Его операционная система — Ubuntu Linux, вирусным заражениям практически не подвержен, работает изолированно от основного компьютера. Достаточно проверять на наличие вирусов файлы, которые вы захотите перенести с виртуального компьютера на физический, чтобы обеспечить безопасность работы в Интернете. Адрес, по которому доступен Browser Appliance, — <http://www.vmware.com/appliances/directory/browserapp.html>.

Перед началом скачивания архива вам будет предложено зарегистрироваться, но это не обязательно. От регистрации можно отказаться.

Скачав архив, распакуйте его в любую заранее подготовленную папку.

Теперь запустите VMware Player или VMware Server. Откройте сохраненную виртуальную машину. Система Browser Appliance настроена таким образом, что после загрузки сразу откроется окно интернет-браузера Firefox. Сеть уже настроена. Доступ в Интернет Browser Appliance получит через базовую машину с применением преобразования адресов (NAT). Никаких маршрутизаторов вам не потребуется. Все необходимые устройства созданы в виртуальной машине. Виртуальный компьютер включен в собственную подсеть, которая не имеет прямого выхода в вашу сеть. На рис. 11.12 показано окно запущенной виртуальной машины в программе VMware Server. Никаких дополнительных настроек не выполнялось. Единственное, что выполнил автор после загрузки виртуальной системы, это ввел в адресную строку браузера адрес сайта <http://auto.gismeteo.ru> и выбрал интересующую страницу на нем.

Мы получили инструмент для работы в Интернете, практически изолированный от базовой машины. Эта изоляция гарантирует высокий уровень безопасности для базового компьютера.

Если вы открыли виртуальную машину в VMware Player, то получили инструмент для безопасного посещения Интернета. Если же вы воспользовались VMware Server, то получили дополнительный компьютер, который можно настроить для работы в вашей сети, провести на нем интересующие вас эксперименты.

Причем эксперименты так же безопасны, как посещение Интернета... Если вы запутаетесь в настройках настолько, что не сможете вернуть виртуальной системе рабочее состояние, достаточно удалить файлы виртуальной машины и распаковать ее из архива заново.

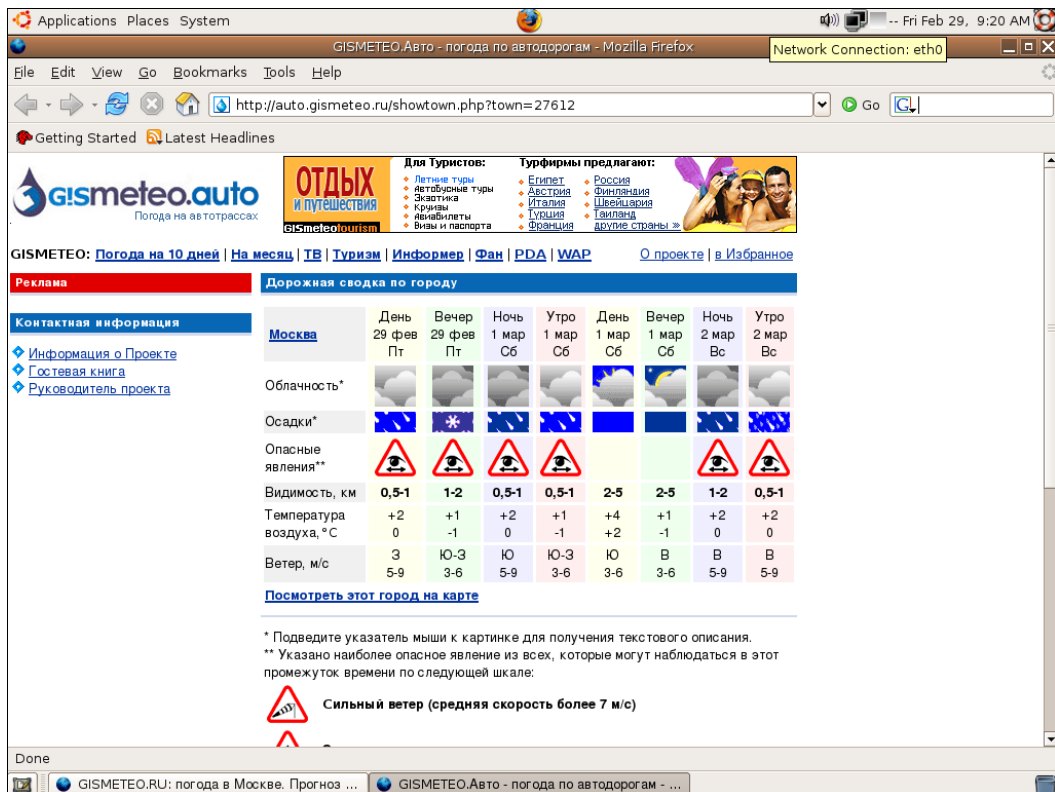


Рис. 11.12. Окно виртуальной машины Ubuntu Linux, запущенной в VMware Server, установленной на базовом компьютере Windows Vista Home Premium

## Виртуальная сеть

Попробуем настроить виртуальную машину с ОС Ubuntu Linux для работы в сети с другими нашими компьютерами. Даже если на данный момент у нас есть только один компьютер, мы можем создать маленькую сеть. Собственно, после установки VMware Server и Browser Appliance у нас уже настроено две сети... Но нас интересует собственная сеть, настройки которой мы выполним самостоятельно.

После установки VMware Server на вашей машине созданы дополнительные сетевые адаптеры. В окне **Сетевые подключения** (рис. 11.13), которое, как вы помните, может быть открыто из **Центра управления сетями и общим доступом**, вы можете увидеть все сетевые подключения вашего компьютера, включая и вновь созданные. В данном случае вновь созданные подключения **VMware Network Adapter VMnet1** и **VMware Network Adapter VMnet8**. Эти адаптеры физически не существуют в вашем компьютере, а созданы программно. Программно в VMware Server созданы DHCP- и DNS-серверы. На адаптерах VMware созданы сразу две сети, а сами адаптеры принадлежат виртуальным устройствам.

Откройте **Virtual Network Editor** (менеджер виртуальных сетей) **Пуск | Программы | VMware | VMware Server | Manager Virtual Networks**. В окне **Virtual**

**Network Editor** на вкладке **Summary** (рис. 11.14) показаны адаптеры и сервисы, которые на них работают.

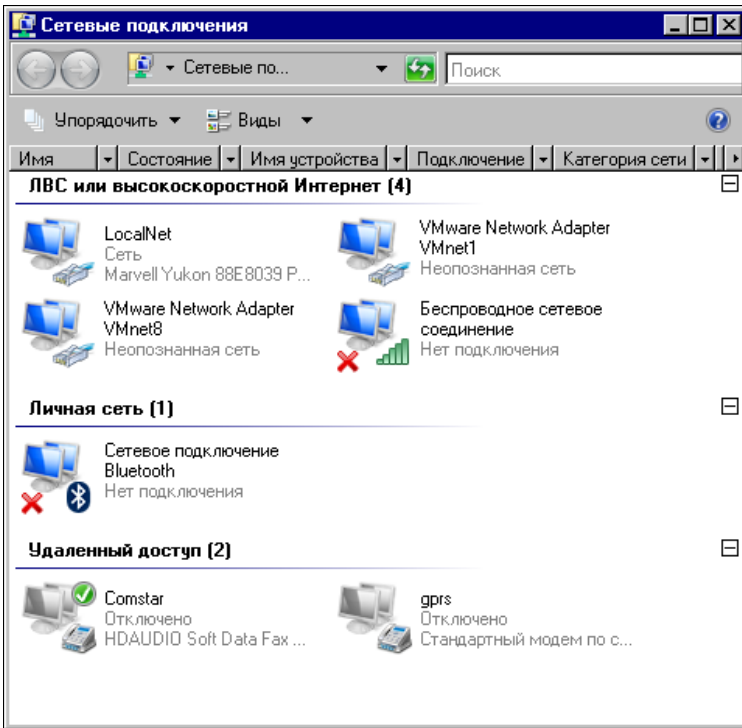


Рис. 11.13. Окно **Сетевые подключения**

**VMnet0 (Bridget)** — адаптер базового компьютера, который может быть использован виртуальной машиной в двух вариантах. Либо, как это по умолчанию настроено, адаптер не используется в созданных виртуальных сетях, либо используется в качестве моста для виртуального адаптера, которому можно присвоить отдельный IP-адрес в вашей сети.

**VMnet1 (Host-only)** — виртуальный адаптер, подключенный к базовому компьютеру, предназначен для связи с виртуальной машиной. Этот адаптер не имеет выхода в реальную сеть и на нем включен сервер DHCP. Сеть, связанная с этим адаптером, существует только внутри базового компьютера.

**VMnet8 (NAT)** — виртуальный адаптер виртуального маршрутизатора, в котором настроено преобразование сетевых адресов. Это позволяет виртуальному компьютеру получать доступ в Интернет через базовый компьютер, используя его IP-адрес вместо своего.

Наша задача — выполнить такие настройки виртуальной сети, чтобы виртуальный компьютер стал частью нашей домашней сети. IP-адреса нашим компьютерам присваивает DHCP-сервер модема-маршрутизатора или мы их назначаем сами. Значит, дополнительные адаптеры **VMnet1** и **VMnet8** нам не нужны. Кроме того, сетевой адаптер физического компьютера должен быть мостом для виртуального



адаптера виртуального компьютера. На всякий случай пролистайте вкладки окна **Virtual Network Editor** и запомните или запишите увиденные настройки. Хотя, вернуть настройки по умолчанию можно, переустановив VMware Server.

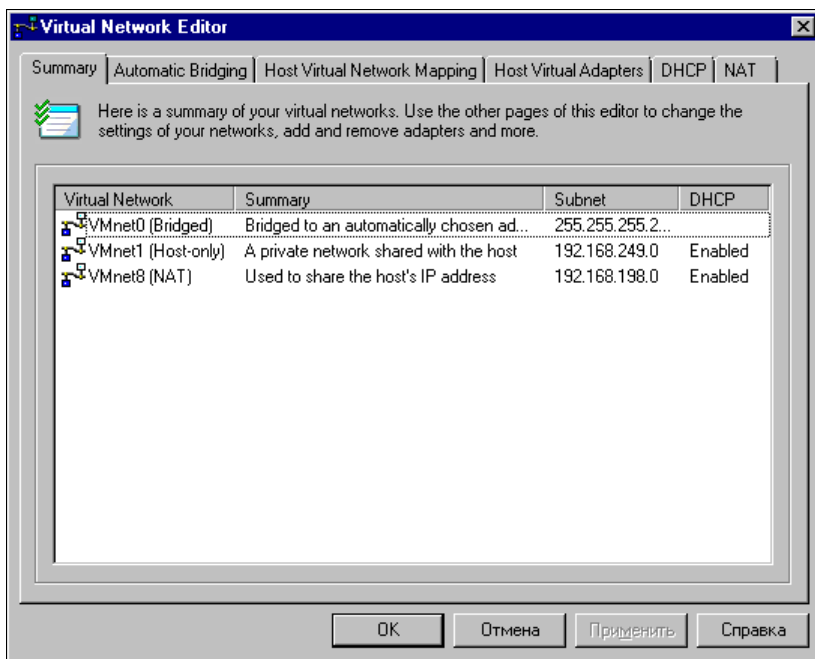


Рис. 11.14. Окно **Virtual Network Editor**, вкладка **Summary**

Для включения виртуального компьютера в реальную сеть проделайте следующее:

1. Перейдите на вкладку **NAT**. Нажмите кнопки **Stop** и **Применить**. В результате вид окна должен получиться как на рис. 11.15.
2. Перейдите на вкладку **DHCP** (рис. 11.16). Нажмите последовательно кнопку **Stop** и кнопку **Применить**, затем, выделяя каждую строку, нажимайте кнопки **Remove** и **Применить**. На вкладке не должно остаться ни одной строки.
3. Теперь перейдите на вкладку **Host Virtual Adapters** (рис. 11.17). Выделяя каждую из имеющихся в окне строк, нажимайте кнопку **Disable**, а затем **Применить**. Этим действием мы отключим не требующиеся в нашем случае адаптеры. При желании их можно удалить совсем, если вы не планируете их использование в дальнейшем. Для этого следует нажимать кнопку **Remove** вместо **Disable**.
4. На вкладке **Host Virtual Network Mapping** в выпадающем списке **VMnet0** (рис. 11.18) следует выбрать сетевой адаптер, через который базовый компьютер подключен к вашей сети.
5. И, наконец, на вкладке **Automatic Bridging** (рис. 11.19) ничего менять не надо. Флажок **Automatically choose an available physical network adapter to bridge to VMnet0** (Автоматический выбор доступного физического сетевого адаптера для

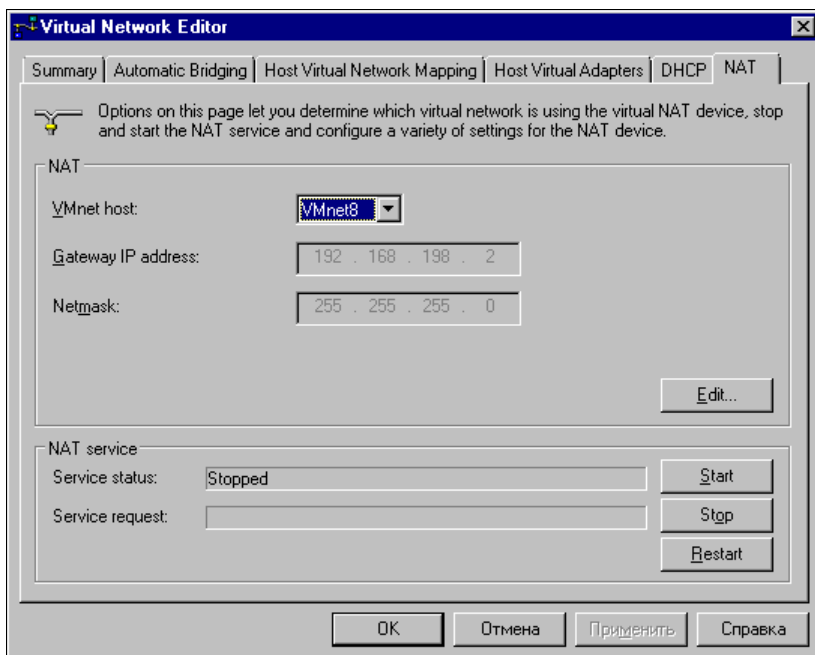


Рис. 11.15. Окно Virtual Network Editor, вкладка NAT

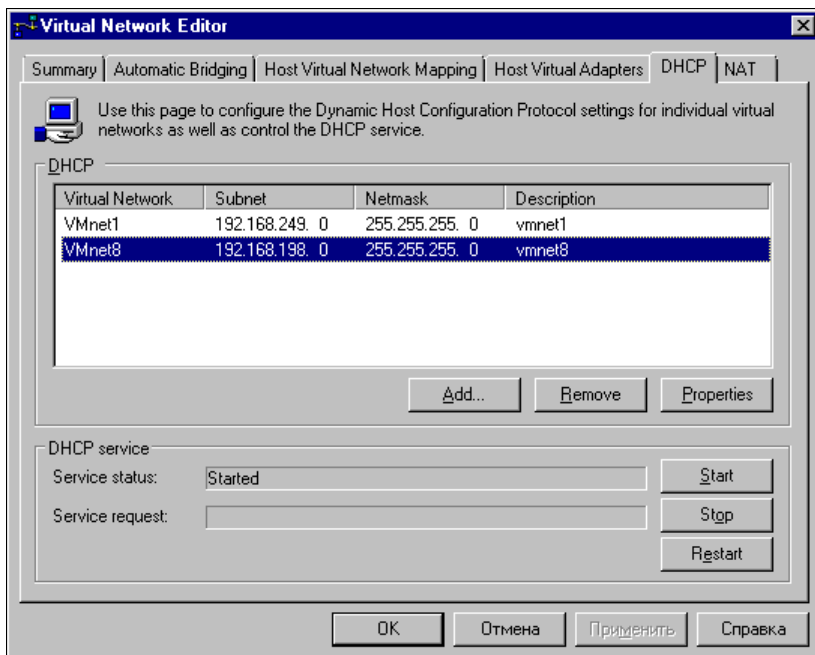


Рис. 11.16. Окно Virtual Network Editor, вкладка DHCP

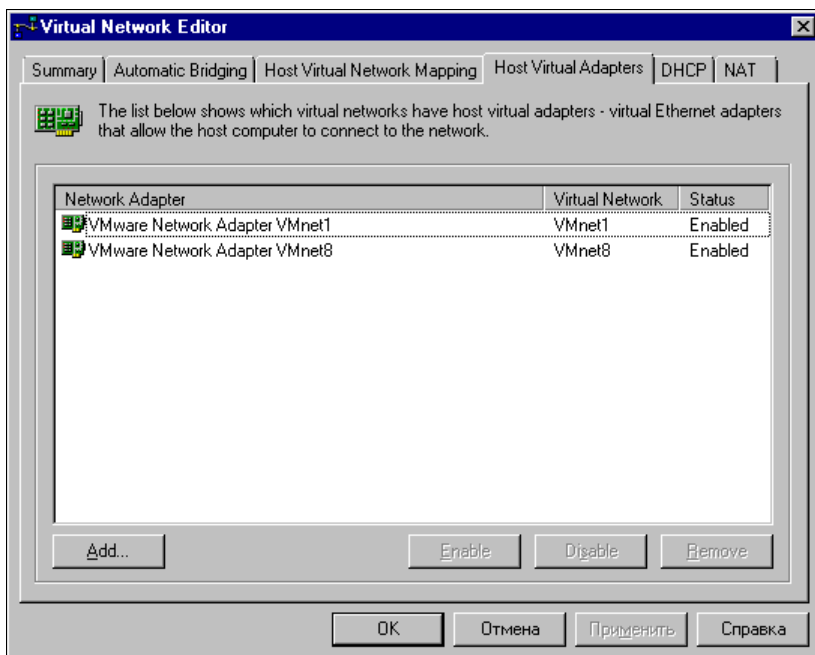


Рис. 11.17. Окно Virtual Network Editor, вкладка Host Virtual Adapters

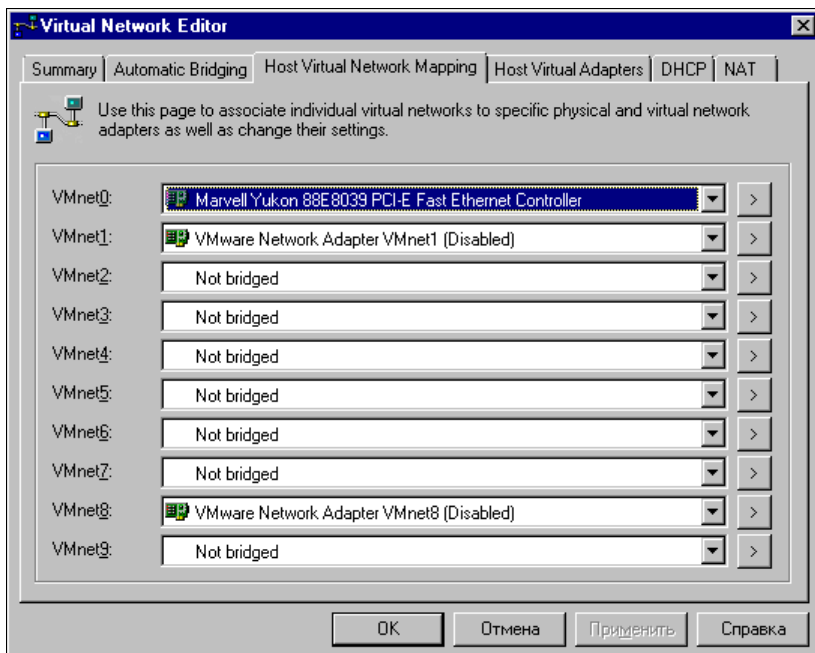


Рис. 11.18. Окно Virtual Network Editor, вкладка Host Virtual Network Mapping

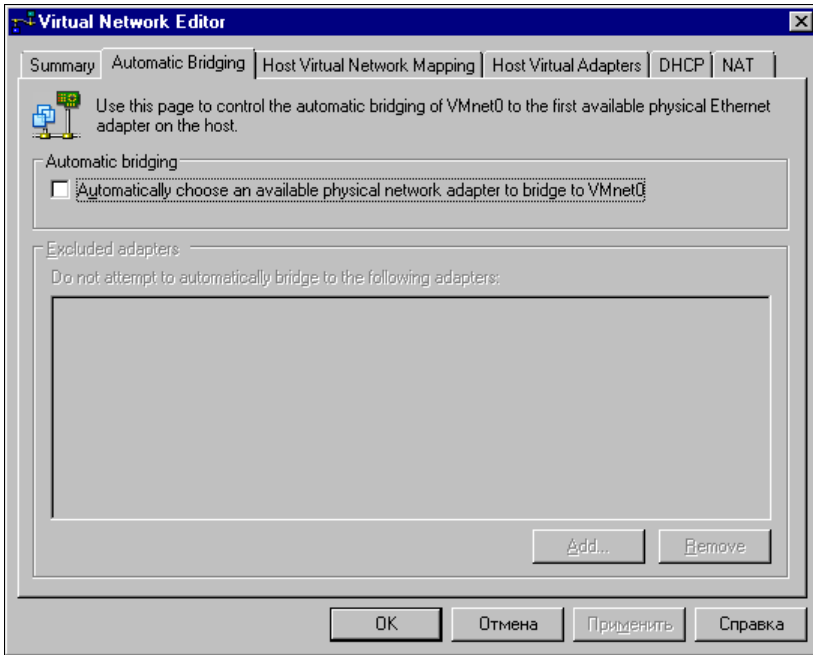


Рис. 11.19. Окно **Virtual Network Editor**, вкладка **Automatic Bridging**

моста на VMnet0) уже снят автоматически после выбора конкретного адаптера на предыдущей вкладке.

Итак, сеть настроена. Остается запустить VMware Server Console, подключив ее к локальному серверу VMware Server (Local host), и поправить конфигурацию виртуальной машины.

6. Откройте окно **Virtual Machine Settings**, выбрав в левой части окна команду **Edit virtual machine settings** — Редактировать установки виртуальной машины (рис. 11.20).
7. В открывшемся окне (рис. 11.21) установите переключатель **Bridged: Connected directly to the physical network** — Мост: подключен к физическому сетевому адаптеру.

Все. Настроена и сеть, и виртуальная машина.

8. Теперь включите виртуальный компьютер командой **Start this virtual machine** (см. рис. 11.20) и настройте сетевое подключение на получение сетевых параметров через DHCP или установите эти параметры вручную, имея в виду, что присвоенный вручную IP-адрес не должен попадать в диапазон адресов, выдаваемых DHCP-сервером.

Убедиться, что виртуальный компьютер подключен к сети, можно, выполнив команду `ping <адрес_виртуального_компьютера> с` базовой машины (рис. 11.22). Если ответов на команду `ping` нет, то проверьте все настройки, описанные ранее.

Если на виртуальном компьютере установлены все необходимые для работы в сети пакеты, через обозреватель сети можно будет увидеть доступные ресурсы

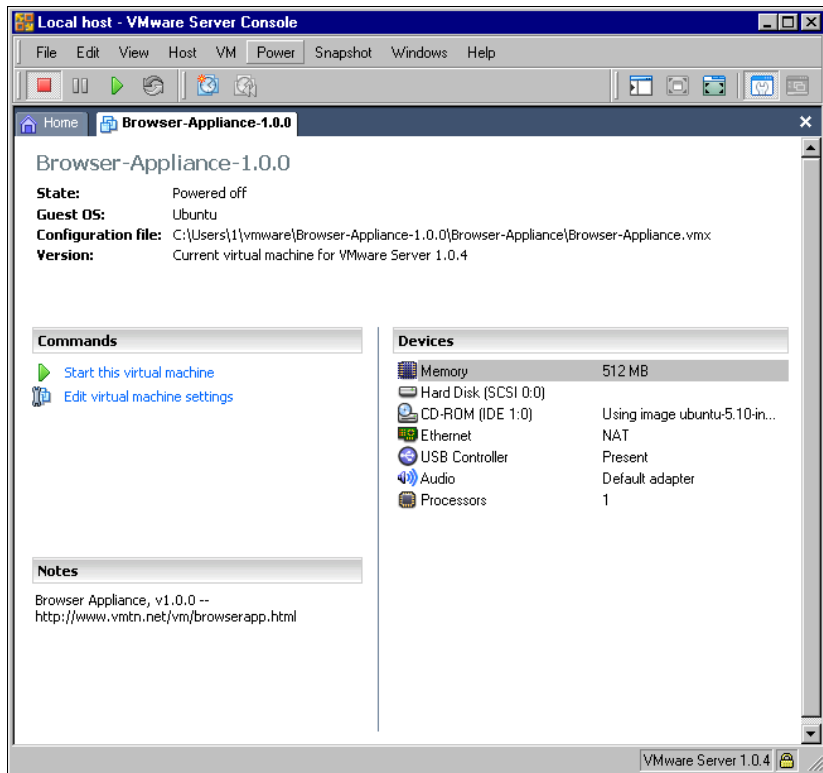


Рис. 11.20. Окно VMware Server Console, вкладка Browser-Appliance

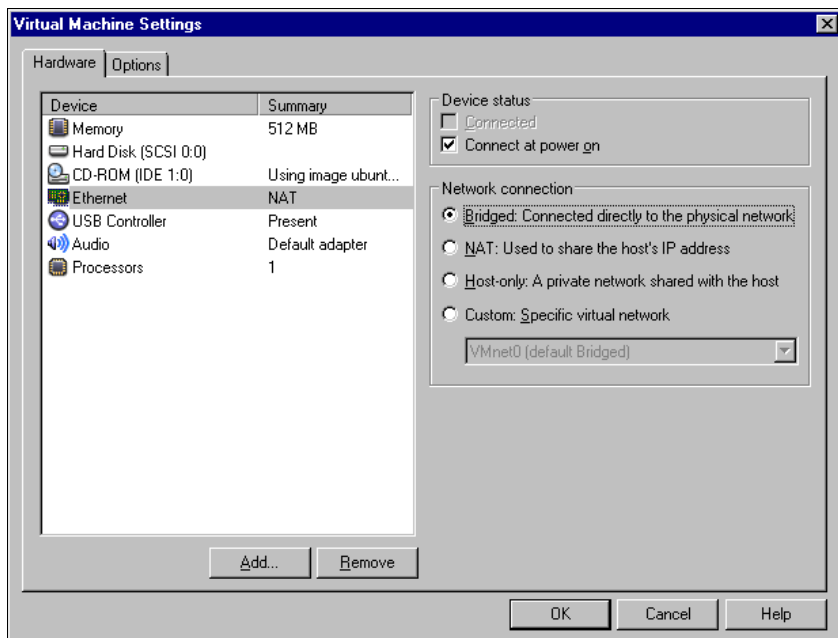


Рис. 11.21. Окно Virtual Machine Settings

```

Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Версия 6.0.6000]
(C) Корпорация Майкрософт, 2006. Все права защищены.

C:\Users\1>ping 192.168.1.133

Обмен пакетами с 192.168.1.133 по с 32 байт данных:

Ответ от 192.168.1.133: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.133: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.133: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.133: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.133:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Users\1>_
  
```

Рис. 11.22. Окно cmd.exe выполнения команды ping

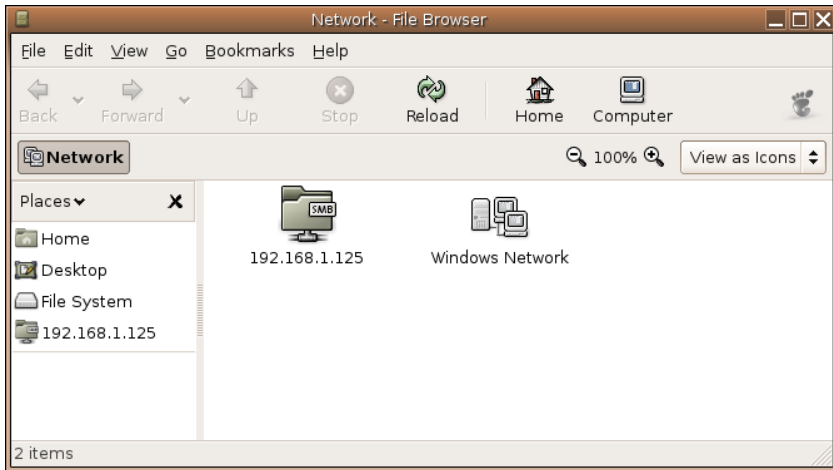


Рис. 11.23. Окно Network — File Browser

(рис. 11.23). Правда, в данном конкретном случае, если у вас нет дистрибутива Ubuntu 5, вы не установите эти пакеты через Интернет, поскольку поддержка этой системы прекращена. Вы можете переустановить систему на виртуальном компьютере, воспользовавшись более свежим дистрибутивом любой версии Linux.

## Запуск виртуальной машины по сети

Имея в своей сети более одного физического компьютера, можно выполнять подключение к виртуальным машинам на любом из них, включать виртуальные машины, выполнять их настройку. В сети автора виртуальный сервер установлен как на компьютере под управлением Windows Vista, так и на машине с ASPLinux, где в качестве виртуальной системы работает Windows XP. Виртуальный сервер,

установленный на любом компьютере, работает всегда. Виртуальные компьютеры, установленные на нем, могут работать, но без запуска консоли управления виртуальным сервером их работа может быть не видна локальному пользователю. В то же время, получая доступ к виртуальному серверу по сети, вы можете управлять виртуальными компьютерами и работать на них.

Посмотрим пример такой работы в сети автора.

В данном случае консоль управления виртуальным сервером запускается на машине под Windows Vista, а виртуальная машина установлена на компьютере под ASPLinux.

При попытке подключения к удаленному компьютеру (**Remote host**) необходимо ввести его имя или IP-адрес, имя и пароль пользователя удаленного компьютера (рис. 11.24).

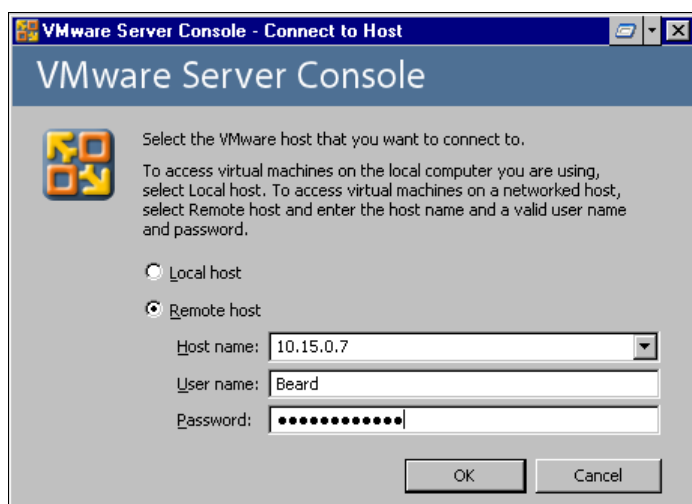


Рис. 11.24. Окно VMware Server Console — Connect to Host

После ввода регистрационных данных откроется консоль управления виртуальным сервером на удаленном компьютере (рис. 11.25). Как и при работе на локальном компьютере, мы можем выполнять любые задачи по управлению виртуальным сервером, в том числе и открыть существующую виртуальную машину (**Open Existing Virtual Machine**), что нам сейчас и требуется.

В окне **Open Virtual Machine** (рис. 11.26) необходимо выбрать одну из существующих виртуальных машин. Выбираем **Windows XP Professional** и нажимаем кнопку **OK**.

Теперь в окне (рис. 11.27) **VMware Server Console** появилась вкладка **Windows XP Professional**. Выбираем **Start this virtual machine**, и через некоторое время видим экран входа в систему Windows XP (рис. 11.28).

Процедура входа в виртуальную систему ничем не отличается от процедуры входа в реальную локальную систему. Более того, на виртуальные системы распространяются все правила лицензирования, как и на реальные. Для использования операционной системы на виртуальной машине необходимо иметь обычную лицензию.

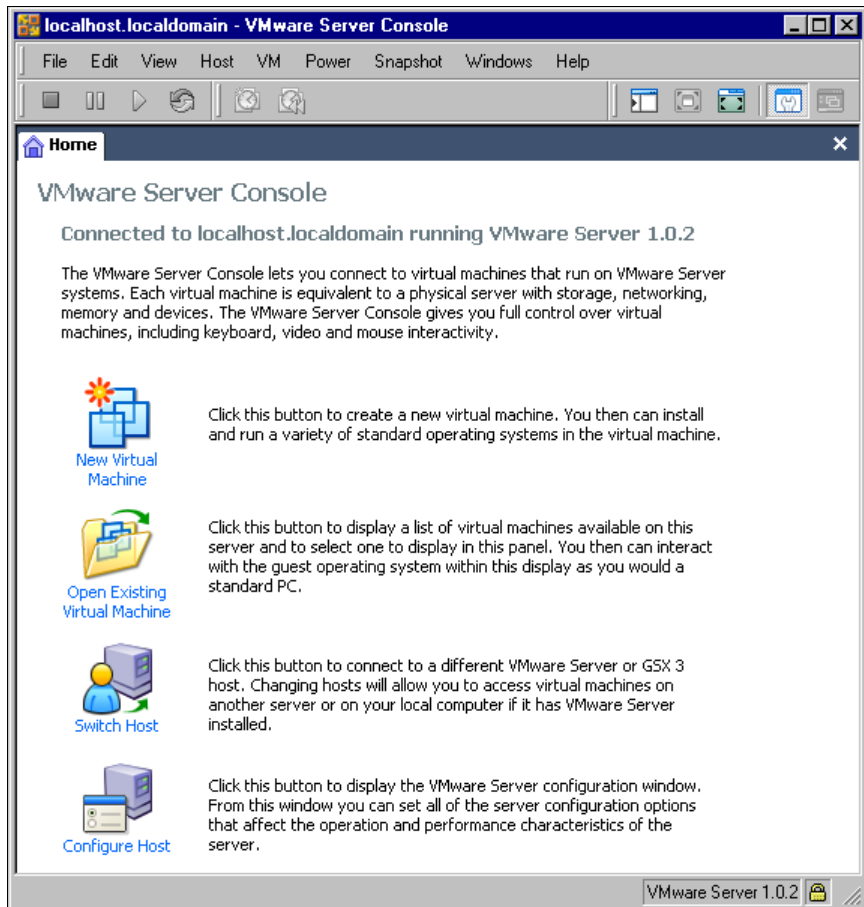


Рис. 11.25. Окно VMware Server Console, вкладка Home

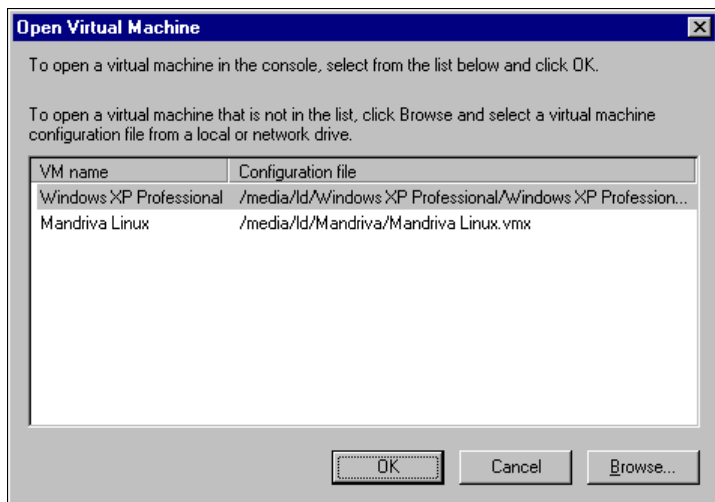


Рис. 11.26. Окно Open Virtual Machine



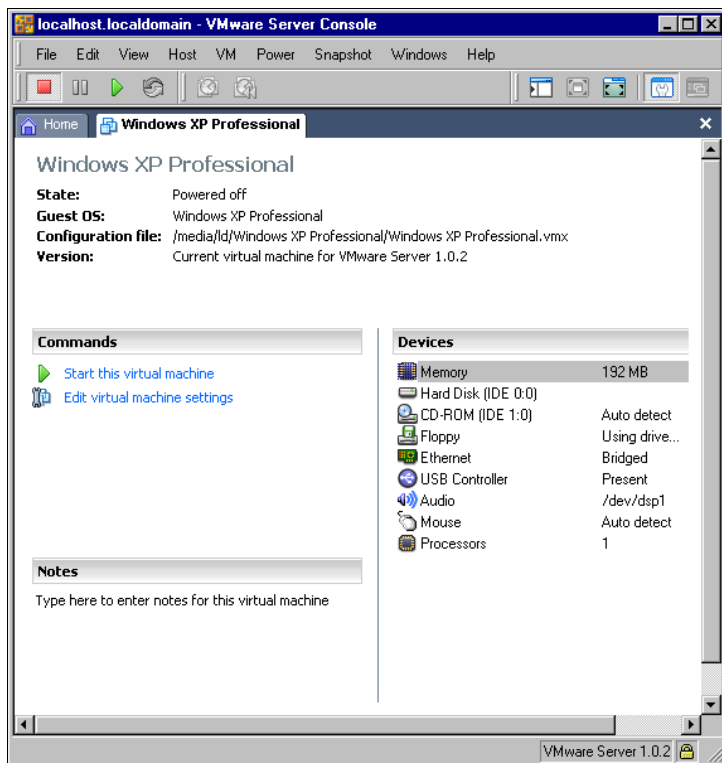


Рис. 11.27. Окно VMware Server Console, вкладка Windows XP Professional

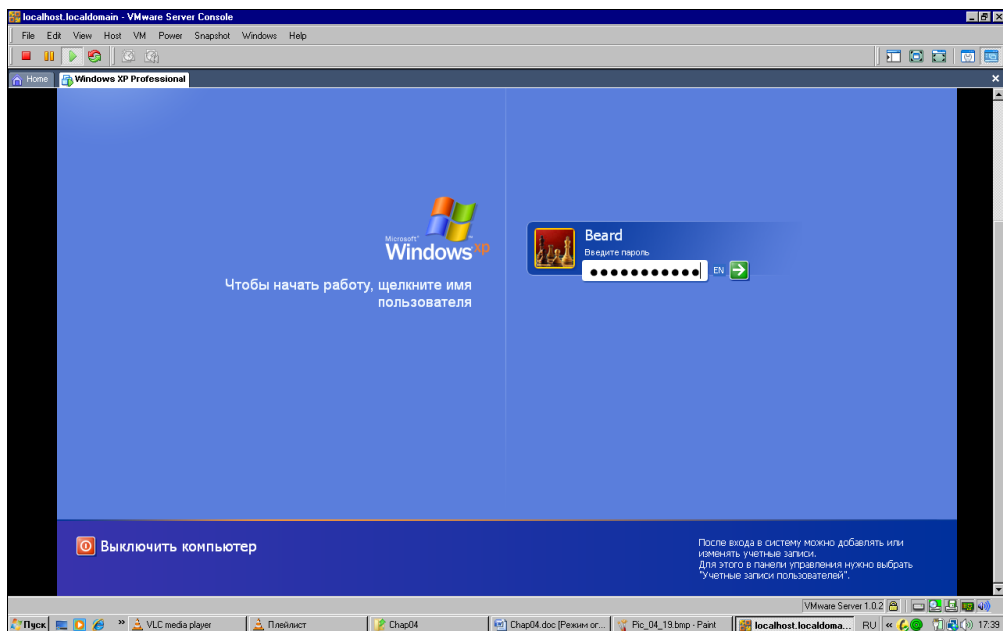


Рис. 11.28. Окно VMware Server Console, вкладка Windows XP Professional (экран входа в систему)

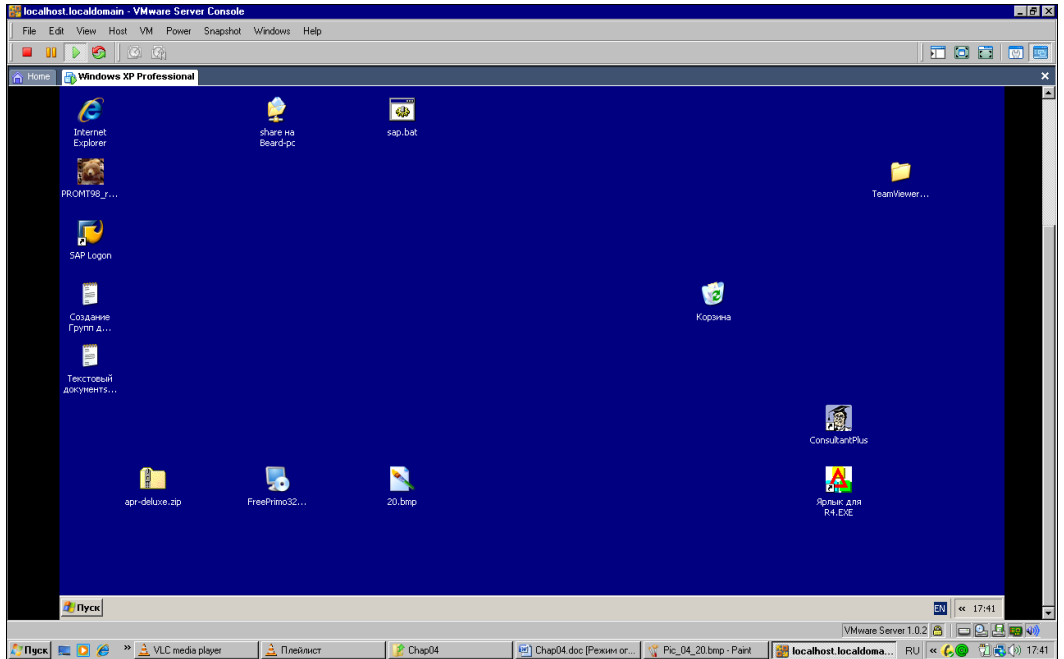


Рис. 11.29. Окно VMware Server Console, вкладка Windows XP Professional (экран загруженной системы)

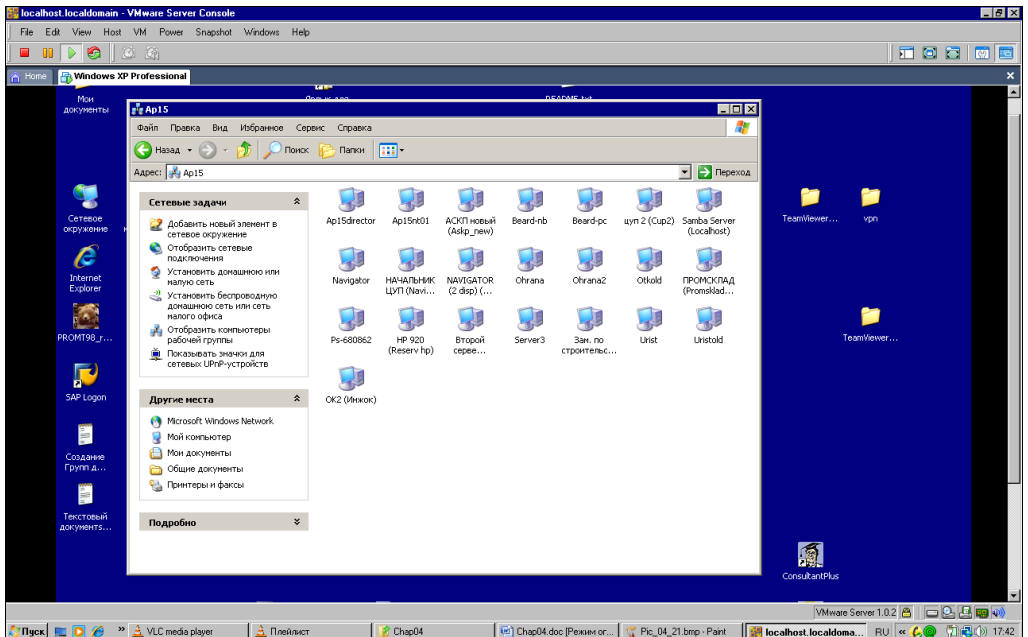


Рис. 11.30. Окно VMware Server Console, вкладка Windows XP Professional (экран загруженной системы — Сетевое окружение)

Рабочий стол виртуального компьютера может не помещаться в окне консоли управления на экране локального компьютера (рис. 11.29). С помощью полос прокрутки можно перемещать виртуальный рабочий стол в окне.

Как и любой реальный компьютер, виртуальная машина работает в сети (рис. 11.30). Для всех компьютеров сети виртуальный компьютер просто один из узлов сети.

Работая на виртуальном компьютере, следует выполнять все правила управления им, как на реальном. Так, например, выключение компьютера следует выполнять через меню **Пуск**, как на реальной машине (рис. 11.31). Если вместо выключения закрыть окно консоли управления, то виртуальный компьютер будет продолжать работать в скрытом виде. Вы сможете к нему подключиться снова как в удаленном, так и в локальном режиме.

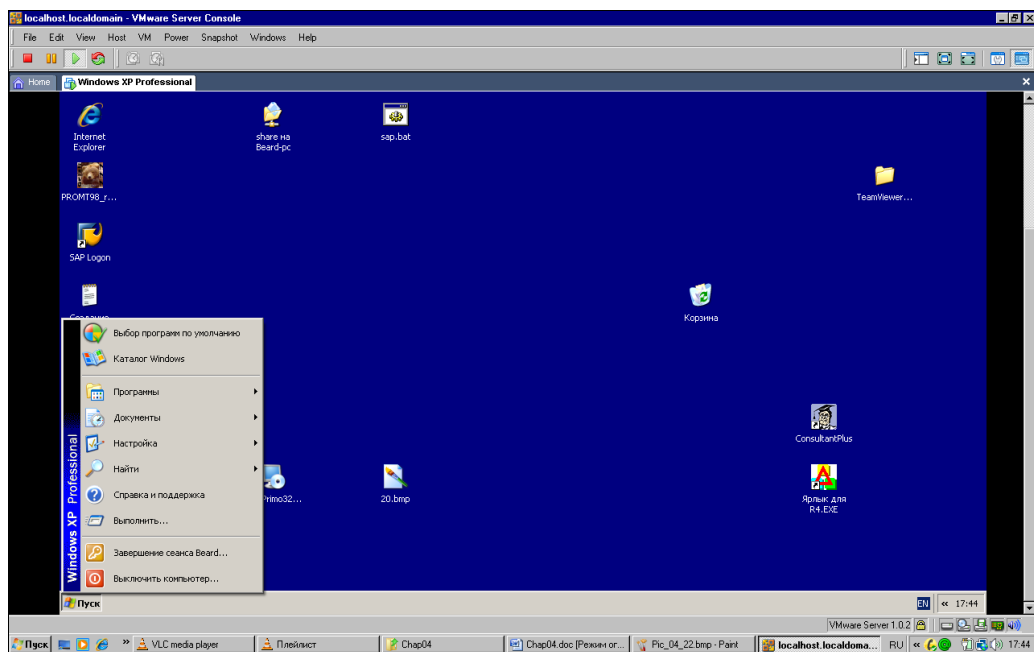


Рис. 11.31. Окно VMware Server Console, вкладка Windows XP Professional (экран загруженной системы — Выключение)

## Задачи для виртуальной машины

Виртуальная машина позволяет решать задачи, которые сложно решить при наличии только одного физического компьютера.

Все большее число пользователей ПК применяют платежные системы, работающие через Интернет. Webmoney, например, одна из самых популярных в наше время. Многие банки позволяют клиентам управлять своими счетами через Интернет. Но в большинстве случаев корректная работа таких систем возможна только под управлением Windows. Часто под управлением других ОС вообще невозможно

использовать эти сервисы. В Linux существуют специальные программы — эмуляторы других операционных систем. Наиболее продвинутые эмуляторы имеют определенную специализацию. Одни рассчитаны на установку игровых программ, разработанных для Windows, другие на использование офисного пакета от Microsoft, третьи позволяют запускать простые программы, такие как, например, Блокнот. Виртуальная машина на основе VMware Server позволяет не эмулировать работу операционной системы, а устанавливать ее. Две операционные системы можно установить на один компьютер и без продуктов VMware или подобных. Но тогда потребуется двойная загрузка системы. В каждый момент времени можно будет работать только с одной ОС. Виртуальная машина позволяет одновременно работать с двумя и более операционными системами. Если вам нравится работать в Linux, но некоторые задачи не могут быть решены в этой ОС, устанавливайте виртуальный компьютер с Windows, и наоборот. Включив виртуальные компьютеры в сеть, вы можете без проблем вести обмен файлами между ними. Таким образом, результаты работы в одной системе будут доступны программам в другой ОС.

Особый интерес представляет возможность сохранять весь виртуальный компьютер в виде файлов. После продолжительной работы по настройке операционной системы на виртуальном компьютере вы можете сохранить весь этот компьютер на съемных носителях и восстановить на любом компьютере. Возможно и клонирование систем. Виртуальный компьютер с особыми настройками, необходимыми в вашей сети, можно раздавать клиентам сети для установки или восстановления после краха системы. Базовый компьютер при этом может даже не быть клиентом вашей сети. Он будет лишь носителем виртуальной машины, входящей в сеть.

Возможно, что вам приходится часто работать в нескольких сетях со своим ноутбуком. Иногда настройки компьютера и сетевого окружения для определенной сети (даже маленькой домашней) весьма специфичны. Если задачи, решаемые в других сетях, не требуют очень много ресурсов от компьютера, вы можете создать и сохранить по виртуальному компьютеру на каждую сеть. Меняя ноутбук (приобретая новый или получая другой служебный), вам не придется снова выполнять настройки и установку программ. Скопируйте файлы виртуального компьютера и продолжайте работать. На новом компьютере должна быть лишь какая-нибудь операционная система, под управлением которой может работать VMware Server. В примере, рассмотренном ранее в этой главе, мы подключались к виртуальному компьютеру под управлением Windows XP, который работал на базовой машине ASPLinux. Появилась необходимость воспользоваться этим виртуальным компьютером в другом помещении. Автор скопировал файлы виртуального компьютера на ноутбук под управлением Windows Vista. Не пришлось переносить в другое помещение стационарный компьютер, Windows XP со всеми настройками и даже сохраненными документами была запущена с ноутбука.

Во время запуска ранее созданной виртуальной машины на новом месте система выдаст запрос о необходимости создания нового уникального идентификатора виртуального компьютера (рис. 11.32). Если это перемещенная копия системы, то можно оставить старый идентификатор (**Keep**).

Бывают ситуации, когда необходимо использовать дистрибутивные диски или диски с программами, работающими с них. Для виртуальной машины вполне подойдут образы таких дисков, сохраненные в доступной папке.

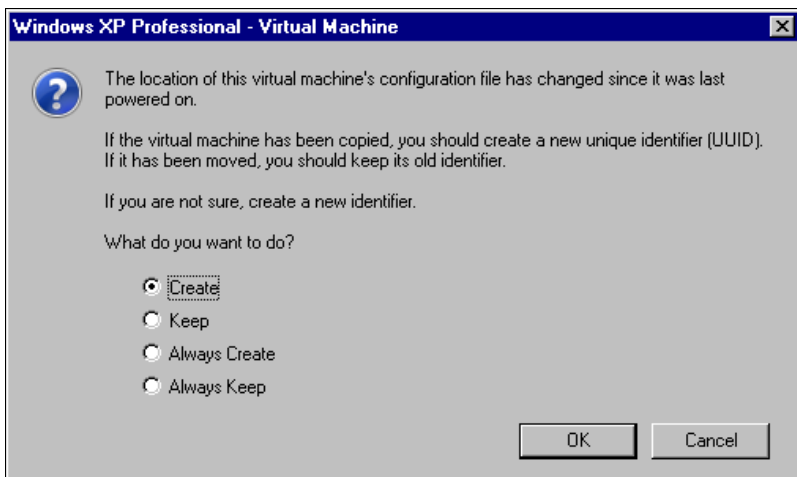


Рис. 11.32. Окно **Windows XP Professional — Virtual Machine** (создание нового уникального идентификатора)

## Установка Oracle VirtualBox

Еще недавно эта виртуальная машина называлась SUN VirtualBox. Причины переименования, наверное, понятны.

Это бесплатная виртуальная машина имеет версии для Windows и Linux. Выбрать необходимую версию и загрузить на компьютер можно со страницы <http://www.virtualbox.org/wiki/Downloads>. Установка Oracle VirtualBox не вызывает затруднений. Даже в Linux программа установки все выполняет сама. Возможности и интерфейс в Windows и в Linux практически одинаковы. После установки и запуска Oracle VirtualBox вы увидите окно программы и сможете приступить к созданию виртуальной машины. В рассматриваемом примере две виртуальные машины уже созданы. Мы используем их для более полного понимания возможностей Oracle VirtualBox и создадим еще один виртуальный компьютер.

Окно программы приведено на рис. 11.33. В правой части окна на вкладке **Детали** можно видеть свойства созданных виртуальных машин. Изменить их можно только для выключенных машин. В левой части представлены все уже созданные машины и информация об их состоянии.

Нажатие на имя раздела свойств дублирует кнопку **Свойства**, но сразу открывает необходимый раздел.

Oracle VirtualBox может работать с реальными приводами CD/DVD и образами жестких дисков, CD/DVD и дискет. Жесткие диски создаются вместе с виртуальными машинами. Загруженные из Интернета образы CD/DVD вы можете собрать в коллекцию и сделать ее доступной для виртуальных машин, добавив с помощью окна **Менеджер виртуальных носителей** (рис. 11.34). Если виртуальный диск подключен к виртуальной машине, то доступна кнопка **Освободить**, если же не подключен, то кнопка **Удалить**. Первая отключает диск от виртуального ком-

пьютера, а вторая от всей виртуальной машины. Физически файл диска не удаляется.

USB-устройства, в том числе и флэш-карты, определяются автоматически и могут быть подключены из меню виртуального компьютера или заранее добавлены

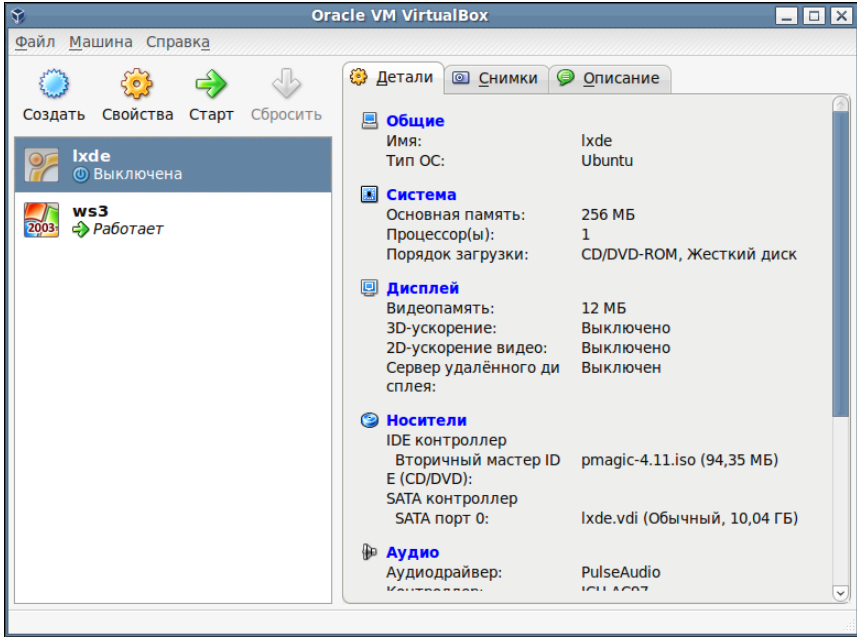


Рис. 11.33. Окно Oracle VM VirtualBox

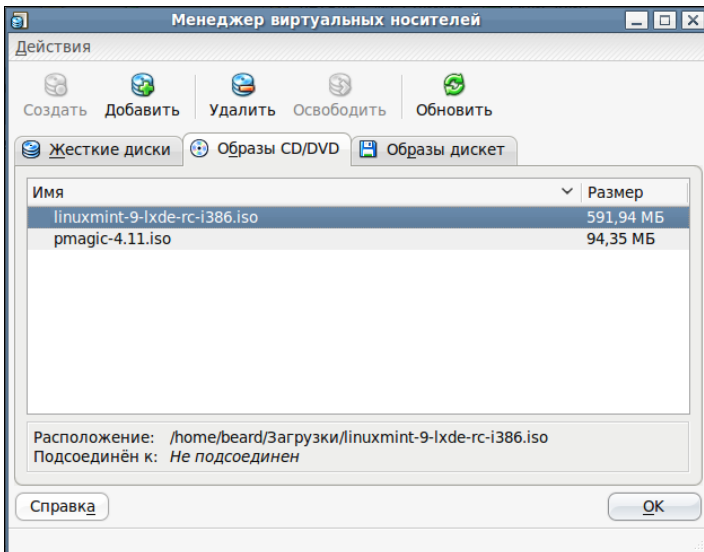


Рис. 11.34. Окно Менеджер виртуальных носителей

к нему. В этом случае устройство будет подключено сразу при запуске виртуального компьютера.

Одно из замечательных свойств Oracle VirtualBox (рис. 11.35) — возможность включить удаленный дисплей.

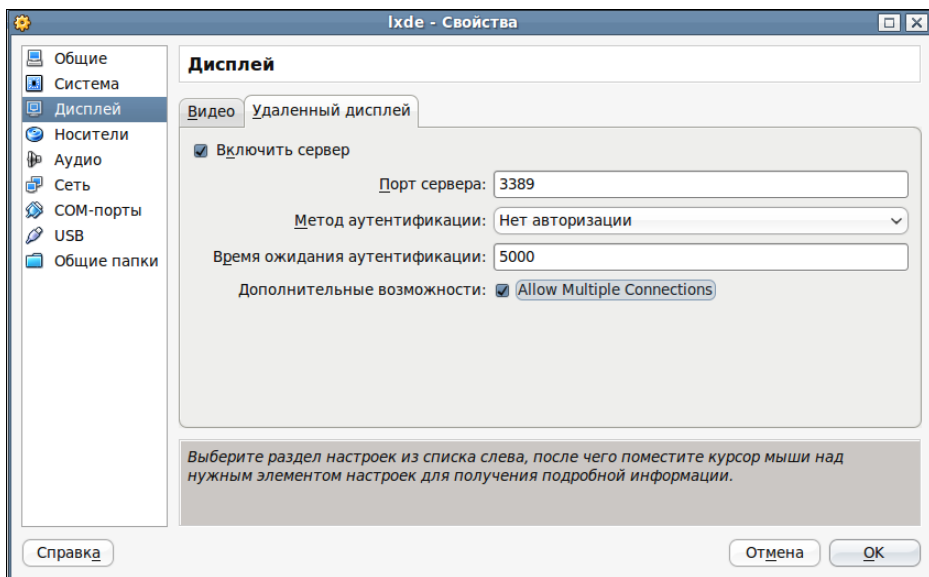


Рис. 11.35. Окно Lxde — Свойства

Удаленный дисплей работает по протоколу *VRDP* (VirtualBox Remote Desktop Protocol), который включен и в *RDP5*. Это значит, что с любого компьютера можно подключиться к виртуальному компьютеру, причем без авторизации. Удаленный компьютер доступен сразу после включения. Вы можете удаленно работать даже с текстовой консолью Linux или с DOS-машиной. Как дополнительная возможность предлагается множественное подключение, когда к одному виртуальному компьютеру могут подключиться несколько пользователей.

Для захвата клавиатуры, мыши (если не установлены Дополнения гостевой ОС), а также для отправки сочетания клавиш `<Alt>+<Ctrl>` по умолчанию используется правая клавиша `<Ctrl>`. Для того чтобы на виртуальном компьютере выполнить команду с помощью комбинации клавиш `<Alt>+<Ctrl>+<Del>`, достаточно нажать `<Ctrl>+<Del>`.

Настройка сети для виртуального компьютера (рис. 11.36) позволяет использовать:

- NAT* (по умолчанию), когда виртуальный компьютер сразу после создания получает доступ в Интернет через базовую машину;
- сетевой мост*, когда виртуальный компьютер использует имеющийся сетевой адаптер. При этом параметры сети настраиваются, как и в обычном компьютере. Виртуальный компьютер виден из локальной сети как отдельная машина;

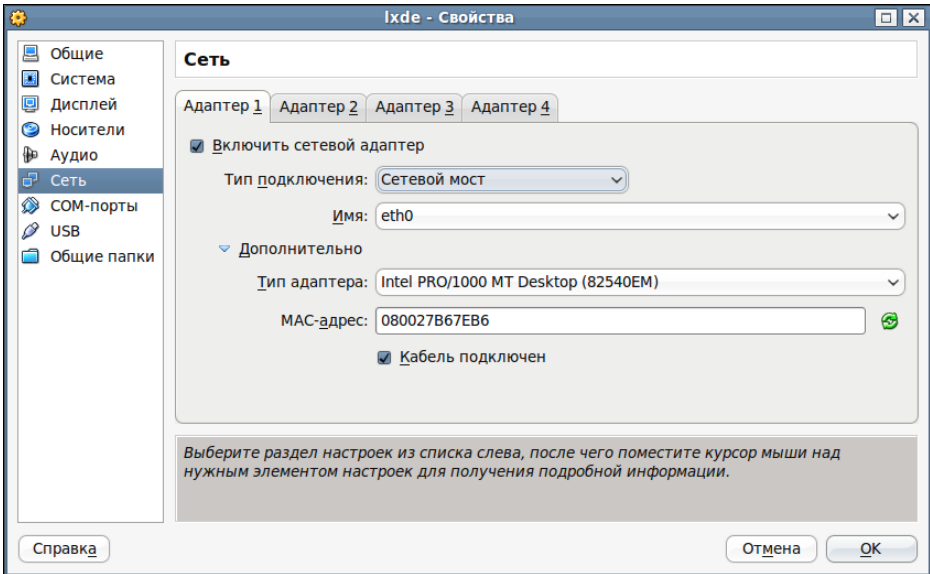


Рис. 11.36. Окно Lxde — Свойства — Сеть

- *внутреннюю сеть*. В этом случае сеть может быть организована только между виртуальными компьютерами;
- *виртуальный адаптер хоста*. Виртуальный компьютер получает сетевой доступ к базовому через виртуальный адаптер.

Как видим, простор для творчества "сетестроителя" огромный.

Для настройки порядка загрузки нет необходимости входить в BIOS. Настройка выполняется в разделе **Система** свойств виртуального компьютера (рис. 11.37).

С другими свойствами виртуального компьютера вы можете ознакомиться самостоятельно. Приступим к созданию новой виртуальной машины.

1. Для запуска мастера создания виртуальной машины нажмите кнопку **Создать** (см. рис. 11.33). Откроется окно **Создать новую виртуальную машину** (рис. 11.38).
2. В этом окне для продолжения создания виртуальной машины нажмите кнопку **Вперед**.
3. В следующем окне (рис. 11.39) необходимо указать имя создаваемой виртуальной машины и выбрать тип операционной системы. Oracle VirtualBox позволяет устанавливать практически все известные операционные системы на виртуальные компьютеры. Если вы устанавливаете Linux Mint, то выбирайте версию Ubuntu, на которой основана Linux Mint.
4. На следующем этапе (рис. 11.40) следует определить размер основной памяти, которая будет выделена виртуальному компьютеру. Не рекомендуется отдавать виртуальной машине более 50% памяти базовой машины. Если виртуальная машина устанавливается для решения узкой задачи не требовательной к ресурсам, то лучше указать минимально возможное для устанавливаемой ОС значение.



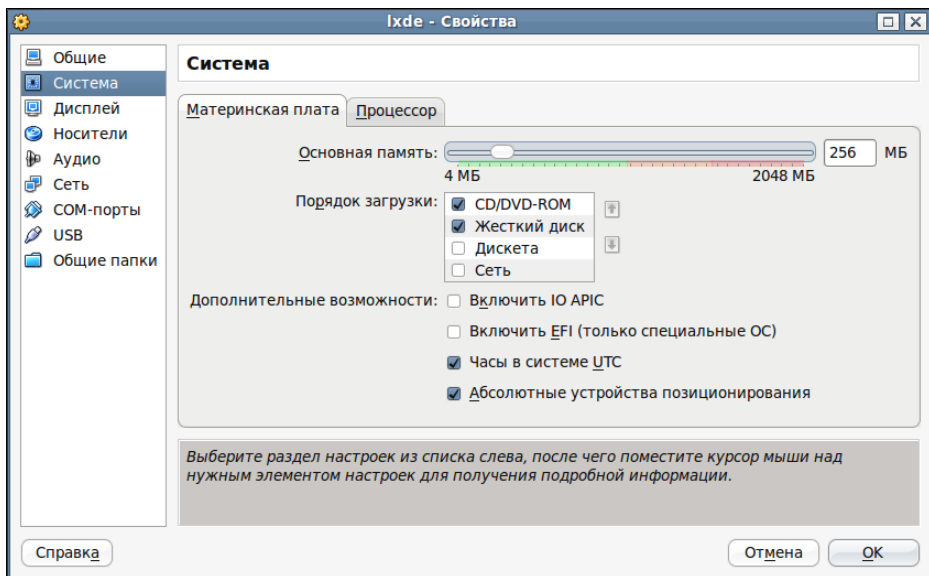


Рис. 11.37. Окно Lxde — Свойства — Система

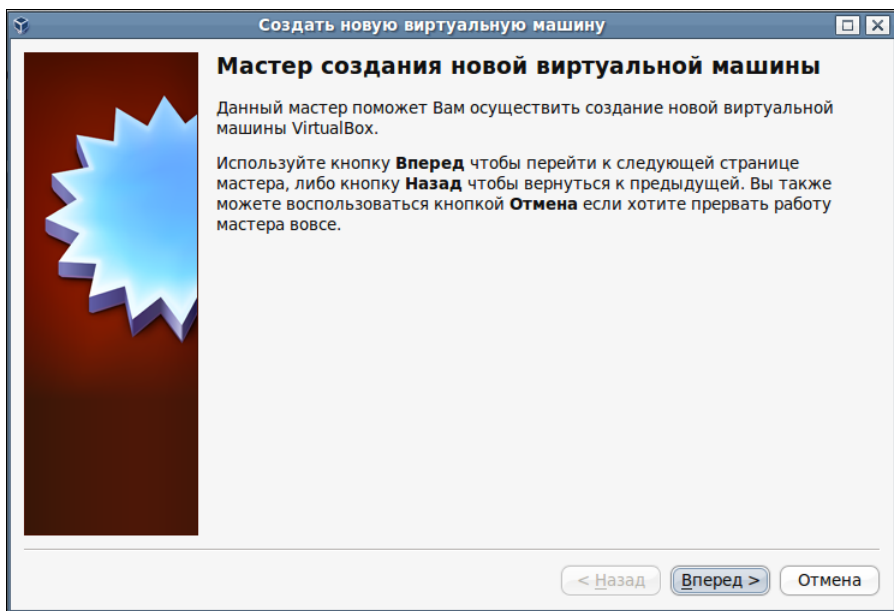


Рис. 11.38. Окно Создать новую виртуальную машину — Мастер создания новой виртуальной машины

5. Пришло время создать жесткий диск (рис. 11.41). По умолчанию предлагается создать новый загрузочный жесткий диск. Если вы уже создавали виртуальный компьютер ранее, можно использовать и существующий в вашей системе виртуальный винчестер, но мы воспользуемся предложением по умолчанию.

6. Мастер создания нового виртуального жесткого диска (рис. 11.42) перед созданием диска предлагает подумать над верностью принятого нами решения. Мы приняли верное решение и нажимаем кнопку **Вперед**.

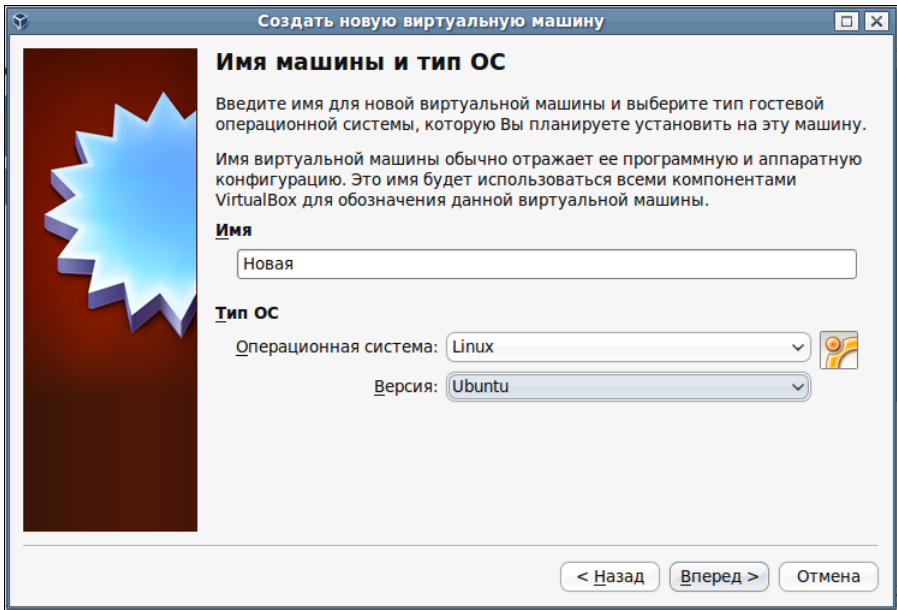


Рис. 11.39. Окно Создать новую виртуальную машину — Имя машины и тип ОС

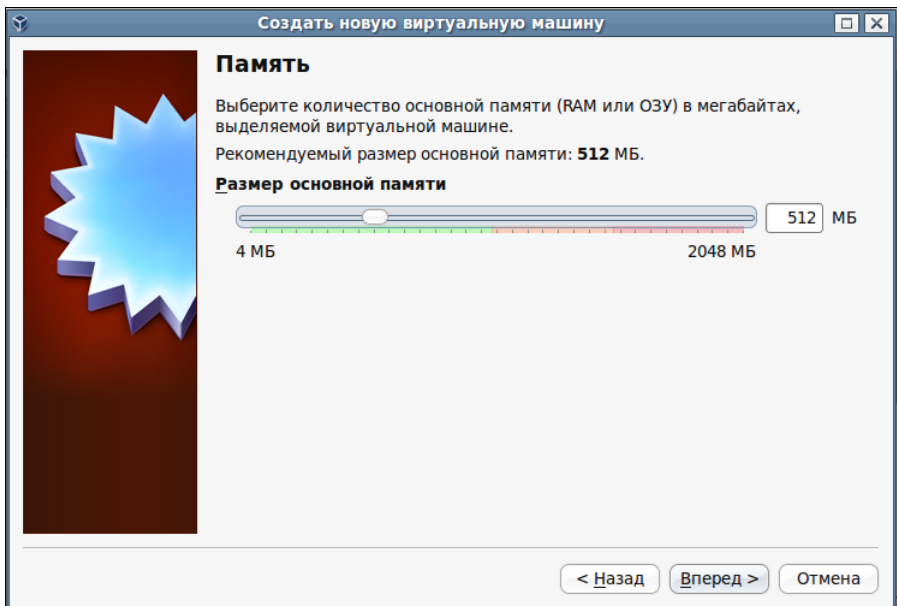


Рис. 11.40. Окно Создать новую виртуальную машину — Память

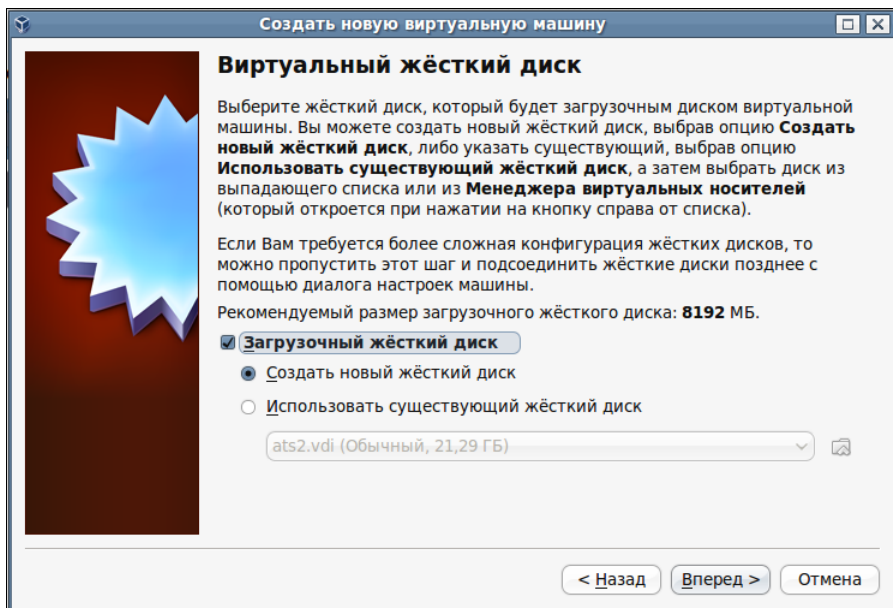


Рис. 11.41. Окно Создать новую виртуальную машину — Виртуальный жёсткий диск

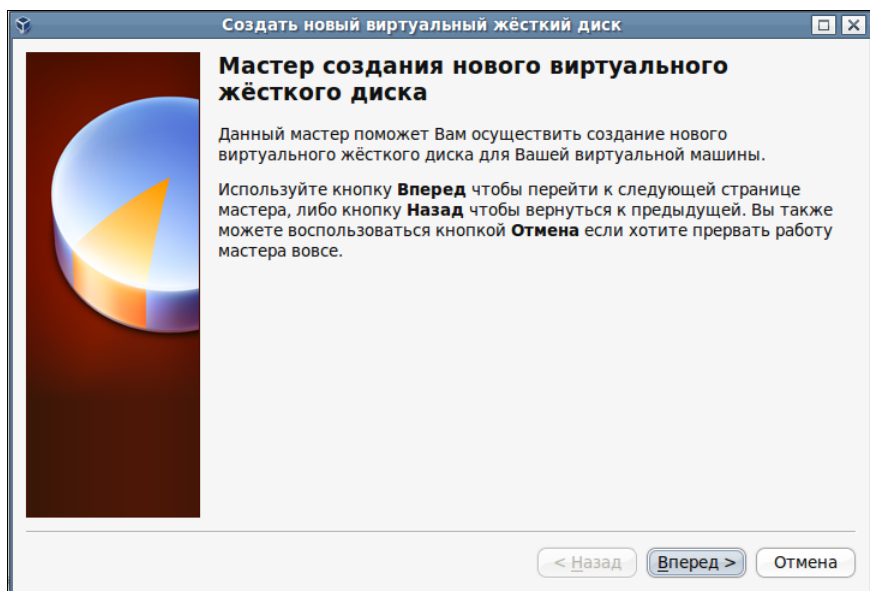


Рис. 11.42. Окно Создать новый виртуальный жёсткий диск — Мастер создания нового виртуального жёсткого диска

7. Выбираем тип виртуального жесткого диска (рис. 11.43). Доступны варианты — **Динамически расширяющийся образ** и **Образ фиксированного размера**. Выберем первый вариант. Файл виртуального жесткого диска будет иметь размер

меньше, чем размер виртуального жесткого диска, и будет увеличиваться по мере заполнения. Переходим к следующему шагу (рис. 11.44).

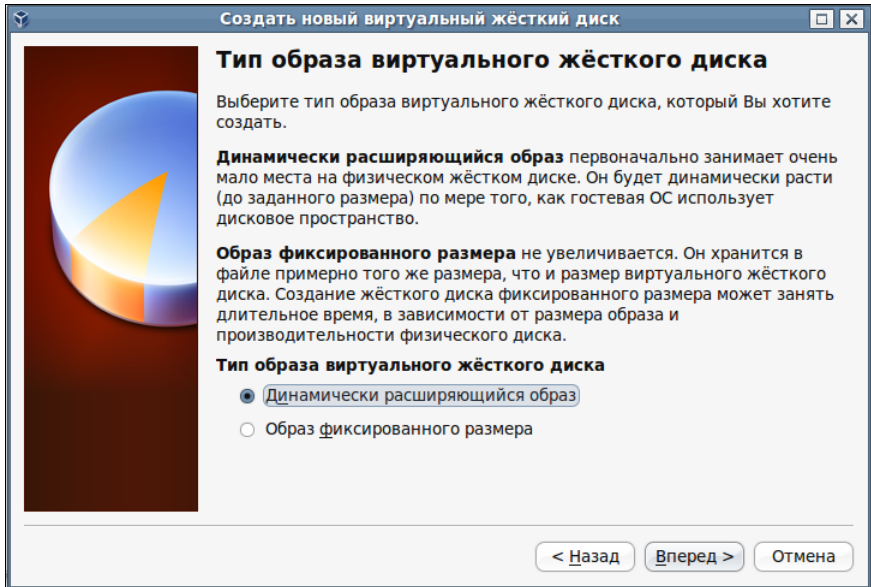


Рис. 11.43. Окно Создать новый виртуальный жёсткий диск — Тип образа виртуального жёсткого диска

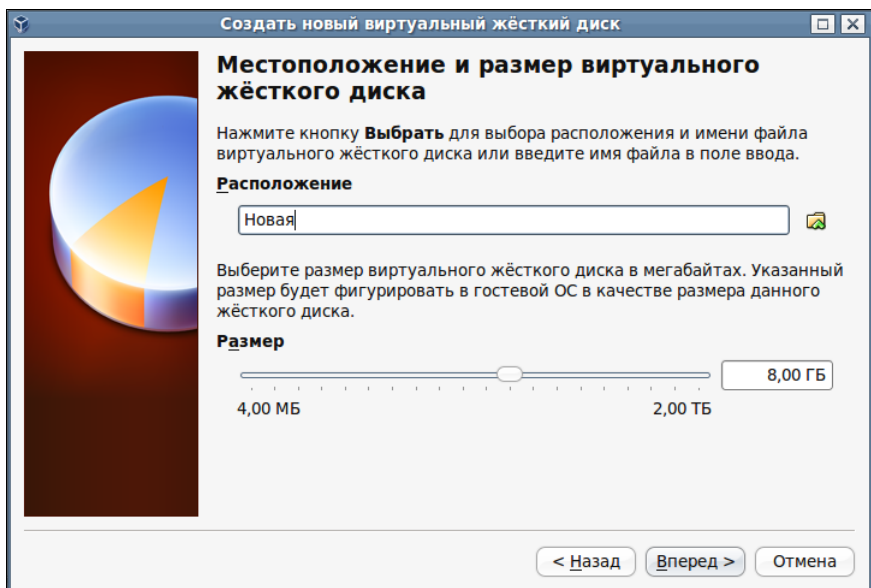


Рис. 11.44. Окно Создать новый виртуальный жёсткий диск — Местоположение и размер виртуального жёсткого диска

8. Расположение диска по умолчанию в каталоге с виртуальной машиной. Имя диска также соответствует имени виртуальной машины. При желании имя и расположение можно изменить, но мы оставим эти параметры по умолчанию. В зависимости от задач будущей машины выбираем размер нового диска. Для первого опыта размер также можно оставить по умолчанию. Нажимаем кнопку **Вперед**.
9. Вот и все. Следующее окно (рис. 11.45) информирует нас о параметрах созданного жесткого диска. Нажимаем кнопку **Финиш**.

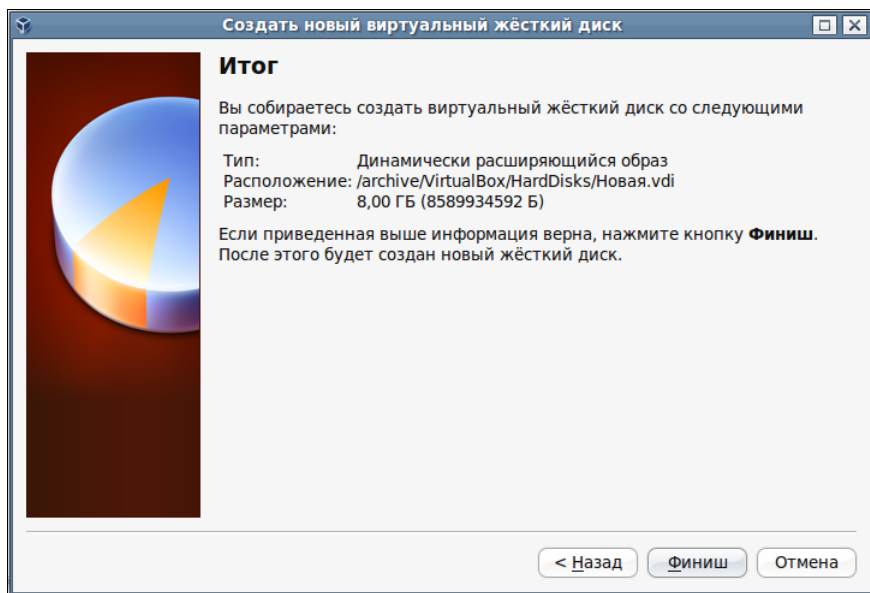


Рис. 11.45. Окно **Создать новый виртуальный жёсткий диск** — Итог

Вновь созданная виртуальная машина появилась в окне **Oracle VM VirtualBox** (рис. 11.46).

Теперь можно устанавливать операционную систему, настраивать сеть, устанавливать программы. Все как на обычном компьютере.

Виртуальный компьютер позволяет использовать для удаленной работы с ним и средства удаленной работы и удаленного администрирования, которые применяются для обычных компьютеров. Например, запустив виртуальный компьютер и выйдя из консоли управления, можно использовать средства удаленного доступа для работы с этим компьютером через Интернет.

Что ж, пожалуй, теперь вы имеете достаточно информации о виртуальных машинах и виртуальных серверах. Нет необходимости приобретать еще один компьютер, когда требуется установить дополнительный сервер, выполняющий какую-либо специальную задачу. А опробовать идею, изучить настройки системы можно на виртуальной машине, предварительно сохранив ее копию.

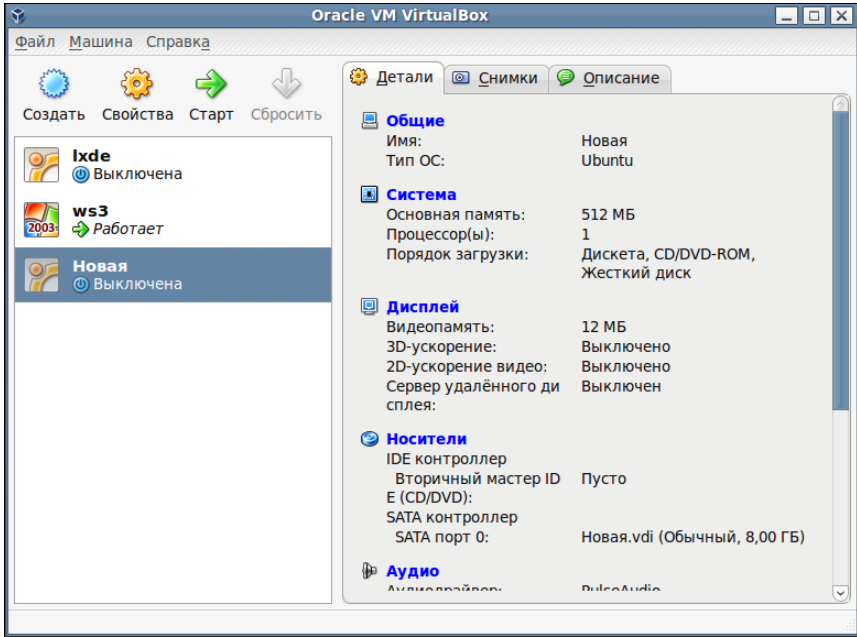


Рис. 11.46. Окно Oracle VM VirtualBox после создания виртуальной машины

Только не забудьте, что виртуальный компьютер, как и обычный, выключать надо правильно, начиная с кнопки **Пуск**...

## ГЛАВА 12



# Настраиваем файловый сервер

Теперь, когда мы знаем о существовании виртуальных машин, мы не будем делать акцент на виде сервера. Виртуальный он или физический — не имеет значения. Важно, что это сервер. Вот и файловый сервер будем описывать просто как сервер. А где и как он будет установлен — это ваше личное дело.

## Каким должен быть файловый сервер?

В общих чертах задачи вытекают из названия сервера. Хранить файлы, осуществлять операции копирования, архивирования, предоставлять доступ к файлам в соответствии с правами пользователей — это, пожалуй, основное, чем должен заниматься файловый сервер.

Просто поместить файлы на диск можно в любой операционной системе. Достаточно объединить в сеть две машины с Windows 98, и вы уже сможете хранить файлы на одной из них. Но такая простая организация хранения файлов не обеспечит ни надежности хранения, ни четкого разграничения прав на файлы, ни обеспечения сохранности файлов в случае сбоя системы. Сеть, в которой работают хотя бы несколько пользователей, требует более серьезного отношения к организации хранения файлов. Каждый пользователь может иметь свой каталог на сервере, к которому другие пользователи могут не иметь доступа вообще или иметь ограниченный доступ. Это может быть важно, когда пользователь готовит документы, в которые другие не имеют права вносить изменения, но могут просматривать их. Возможны и более сложные случаи распределения прав.

Еще одно полезное свойство файлового сервера — возможность установить предельный размер дискового пространства, которое может выделяться одному пользователю. Нет ничего приятного в ситуации, когда пользователь заполнил своими файлами сетевой диск, а другим пользователям места не оставил. Еще хуже, если пользователь заполнил системный диск и сервер отказал...

Надо сказать, что это не выдуманная ситуация. Действительно, автору известен случай, когда отказал контроллер домена, который по совместительству выполнял функции файлового сервера. А причина была в переполнении единственного, а потому системного диска.

Таким образом, можно определить основные требования к нашему файловому серверу, которые следует выполнять, насколько возможно, ближе к тексту.

- Файловый сервер должен быть отдельной машиной. В крайнем случае, если такой возможности нет, диски, предназначенные для хранения данных, не должны быть системными.
- Для управления доступом к файлам и папкам сервер должен входить в какую-либо систему аутентификации. В локальной сети наиболее подходящей системой может быть служба *AD (Active Directory)*, которая обычно располагается на контроллере домена.
- Диски файлового сервера должны быть надежными. Это достигается резервированием дисков в массивах *RAID (Redundant Array of Inexpensive Disks, дисковый массив)* или их *зеркализацией (Mirrored Arrays)*. RAID-массивы могут быть выполнены как отдельные устройства, но в условиях малой сети это достаточно дорого. В таком случае можно просто настроить зеркалирование для двух одинаковых винчестеров, установленных на сервере. Учитывая, что зеркалирование возможно только для динамических томов, у нас появится возможность "горячего" управления этими дисками. При необходимости можно будет подключить дополнительную пару винчестеров.
- Для исключения возможности переполнения дискового пространства бесполезными файлами следует установить разумную квоту на дисковое пространство. Это не позволит отдельным пользователям помещать на диски файлового сервера больше информации, чем было заранее предусмотрено.
- Ранее нами это не оговаривалось, но следующее условие также очень важно. IP-адрес файлового сервера должен быть статическим. Он не должен меняться, как меняются адреса обычных рабочих станций, когда они получают их от DHCP-сервера. Это позволит обращаться к серверу и клиентам, которые не могут в полной мере использовать возможности AD, например с Linux-машин.

Требования описаны в качественном выражении. Здесь не указываются необходимые размеры дисков, величина квоты, параметры сервера. Все это зависит от конкретных условий. Но одно можно сказать точно — для файлового сервера необходимо применять операционную систему не ниже чем Windows 2000 Server. Хотя, в отдельных случаях может быть использована ОС Windows XP Professional. В этой системе тоже возможно создание динамических дисков и их зеркалирование. Но серверная операционная система будет работать устойчивее, и сервер будет более надежным.

В Интернете можно встретить немало описаний того, как настроить файловый сервер под управлением Linux. Возможно, что через некоторое время действительно это будет лучшим выбором. Но до тех пор, пока подавляющее большинство пользователей ПК работают в Windows, файловый сервер под Linux больше подошел бы для сервера, к которому открыт доступ из Интернета. Но если у вас есть большое желание попробовать настроить такой сервер для вашей локальной сети, можно порекомендовать для начала прочитать статью в Интернете по адресу <http://www.linuxrsp.ru/artic/sambal.html> и еще [http://www.opennet.ru/base/net/slackware\\_samba\\_ad.txt.html](http://www.opennet.ru/base/net/slackware_samba_ad.txt.html).



Пока даже не совсем начинающему пользователю Linux, думаю, будет не очень просто выполнить предлагаемые в статьях настройки.

В Windows большинство необходимых настроек выполняется достаточно просто. Можно больше внимания уделить настройке аппаратной части — дискового массива.

## Настройка сервера

Описание предполагает, что служба AD в вашей сети уже работает. Даже если у вас всего два-три компьютера, все равно имеет смысл использовать Active Directory, поскольку выгоды от AD значительно больше, чем проблем с ее установкой. Пусть имеется операционная система файлового сервера — Windows 2000 Server.

Итак, компьютер на роль файлового сервера выбран, пара одинаковых винчестеров приобретена. Перед настройкой сервера винчестеры следует установить в системный блок. Когда будете готовы, включите компьютер.

После загрузки компьютера новые диски еще не отображаются в окне **Мой компьютер**. Их следует подключить в оснастке **Управление компьютером**. Как только вы перейдете к узлу оснастки **Управление дисками**, запустится окно **Мастер подписывания и обновления дисков** (рис. 12.1).

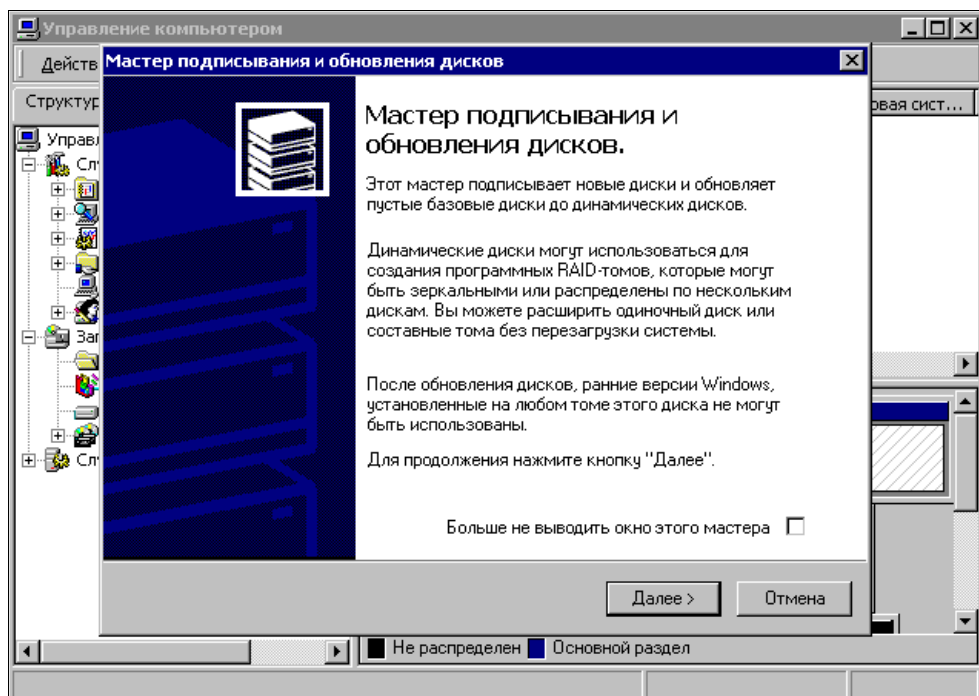


Рис. 12.1. Окна **Управление компьютером** и **Мастер подписывания и обновления дисков** (первое сообщение)

Задержитесь на несколько мгновений на этом сообщении, чтобы прочитать его. Возможно, что информация из этого сообщения будет вам полезна. Прочитав сообщение мастера, нажмите кнопку **Далее**.

Появится информационное сообщение мастера создания тома (рис. 12.2). Нажмите кнопку **Далее**.

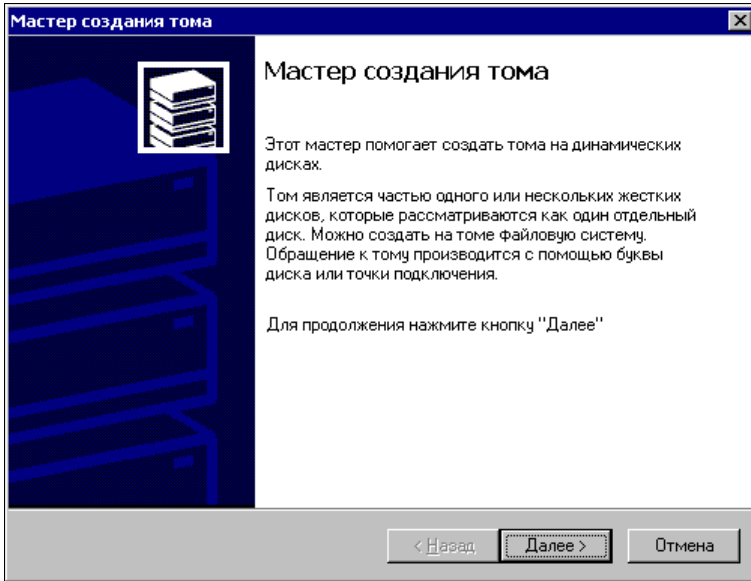


Рис. 12.2. Окно **Мастер создания тома**

Теперь перед нажатием кнопки **Далее** следует выбрать тип создаваемого тома. Выбираем **Зеркальный том** (рис. 12.3). Нам необходимо заставить оба винчестера работать как один, каждый должен содержать полностью идентичные данные.

В следующем окне (рис. 12.4) необходимо выбрать динамические диски, которые будут работать в зеркальном томе. Естественно, мастер предложит выбор из наших новых винчестеров. Выбираем оба.

В следующем окне мастера (рис. 12.5) назначаем нашему тому букву, как это обычно требуется в Windows.

Теперь следует отформатировать том, как обычный логический диск (рис. 12.6).

После завершения работы мастера и окончания процедуры форматирования тома в окне **Управление компьютером** (рис. 12.7) вы увидите два физических диска, которым присвоена одна буква диска и одна метка. Два винчестера составили один новый том.

Все почти готово, чтобы наш файловый сервер заработал. Теперь можно создать необходимые каталоги на новом томе, определить на них права пользователей. Вот здесь и окажется полезной служба AD. Централизованное управление пользовательскими учетными записями позволяет оперативно определить для каталогов необходимые права. Появление новых пользователей, необходимость изменения настроек прав существующих пользователей не вызывает никаких проблем. Однако

во хорошо настраивается доступ для клиентов как Windows XP, так и Windows 98 и даже Linux.

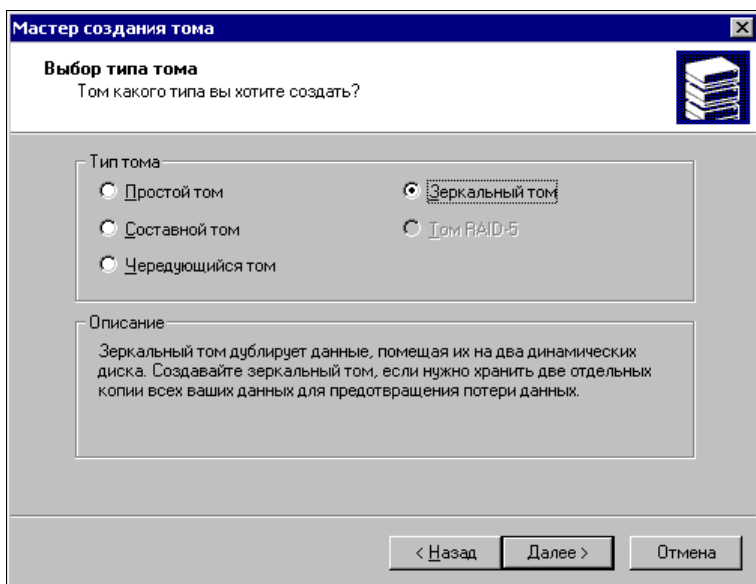


Рис. 12.3. Окно Мастер создания тома — Выбор типа тома

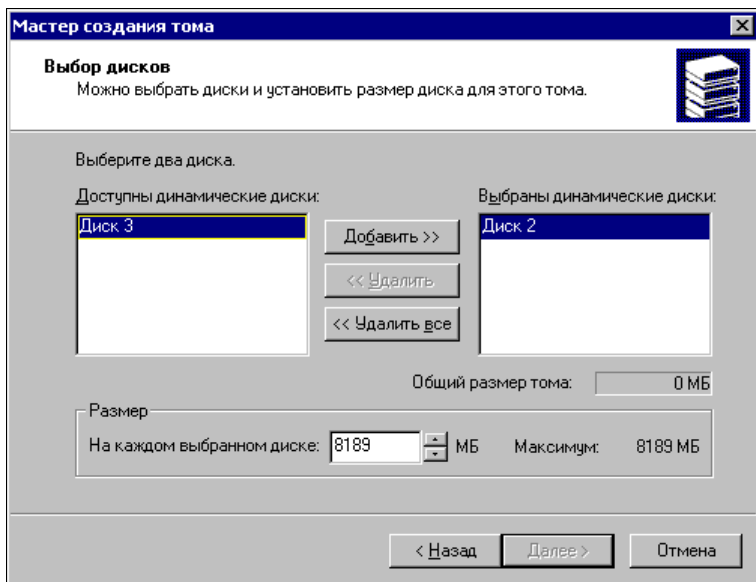


Рис. 12.4. Окно Мастер создания тома — Выбор дисков

Теперь остается еще одна операция. Желательно определить квоту на дисковое пространство нового тома. Ведь объем даже очень больших дисков не безграничен. Найдется пользователь, который решит сохранить на вашем файловом сервере

свою коллекцию фото- и видеофайлов и при этом займет все свободное пространство на томе. Ограничив объем дисковой памяти, который может использовать один пользователь, вы столкнетесь с нехваткой места на диске не в аварийной ситуации, а в спокойном диалоге с пользователем. Возможно, что для этого пользователя вы создадите еще один динамический том.

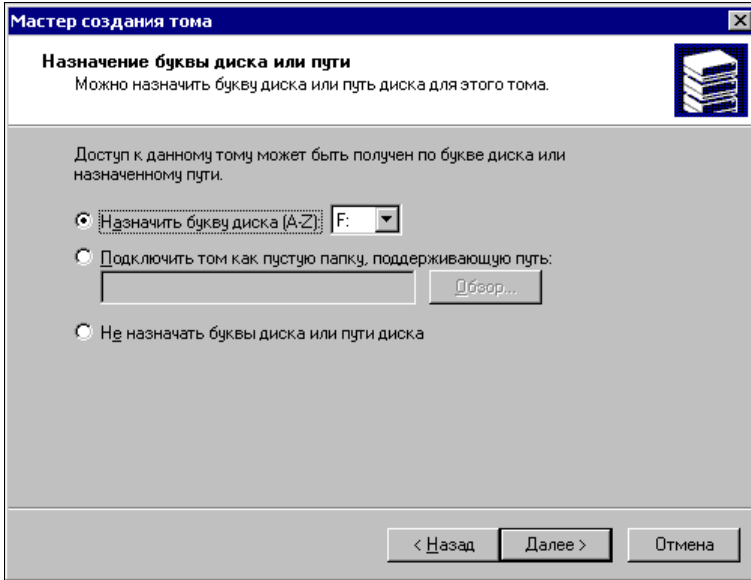


Рис. 12.5. Окно Мастер создания тома — Назначение буквы диска или пути

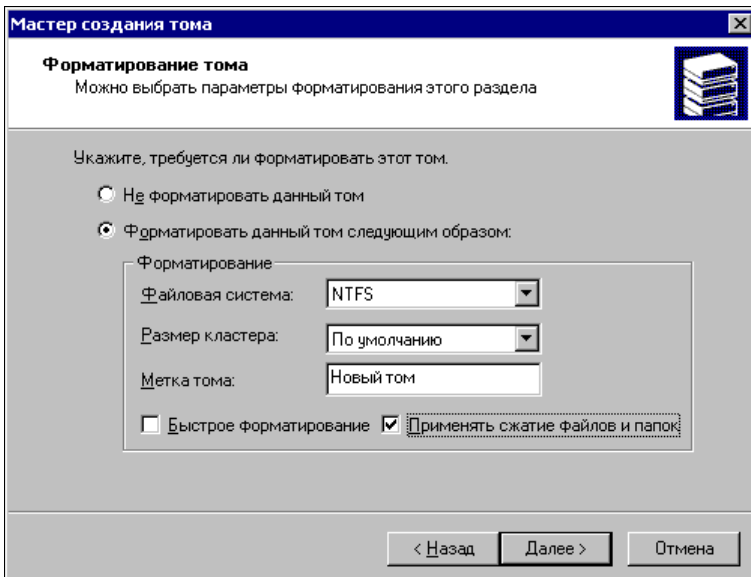


Рис. 12.6. Окно Мастер создания тома — Форматирование тома

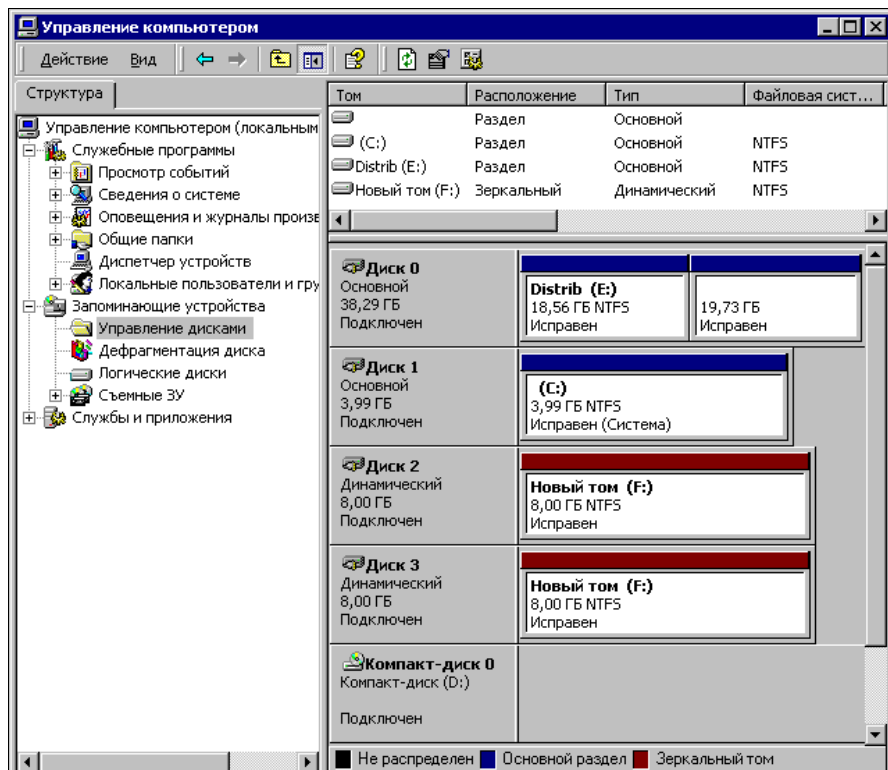


Рис. 12.7. Окно Управление компьютером — Управление дисками

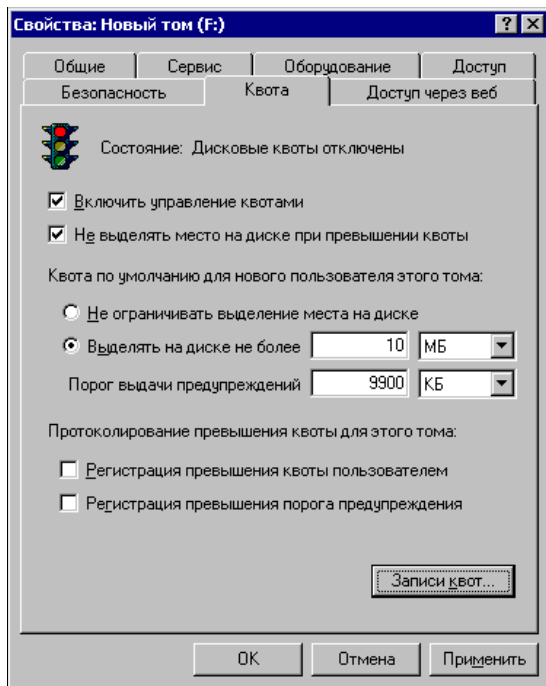


Рис. 12.8. Окно Свойства созданного тома, вкладка Квота

Для создания квоты достаточно в окне свойств тома (рис. 12.8) установить необходимые параметры квоты. При этом следует помнить, что квота выделяется не в определенном каталоге, а на диске в целом.

Вот теперь ваш сервер может хранить данные на новом томе. Выход из строя одного винчестера не приведет к катастрофе. Данные не будут потеряны. Потребуется лишь замена неисправного винчестера и некоторое время на синхронизацию данных.

## Настраиваем файловый сервер под Linux

Чтобы для простой сети настроить файловый сервер под управлением Linux, можно воспользоваться готовыми примерами файлов конфигурации и вместе с пакетами, относящимися к Samba, установить пакет SWAT и использовать Web-интерфейс для дальнейшей настройки файлового сервера.

После установки Samba введите в группу sambashare пользователей, которые должны иметь полный доступ к файлам сервера. В Linux Mint это можно выполнить через графический интерфейс, пройдя по пути **Меню | Центр управления | Система | Пользователи и группы | Управление группами**. В открывшемся окне **Параметры групп** (рис. 12.9) выберите группу sambashare и с помощью кнопки **Добавить** добавьте в эту группу необходимых пользователей компьютера.

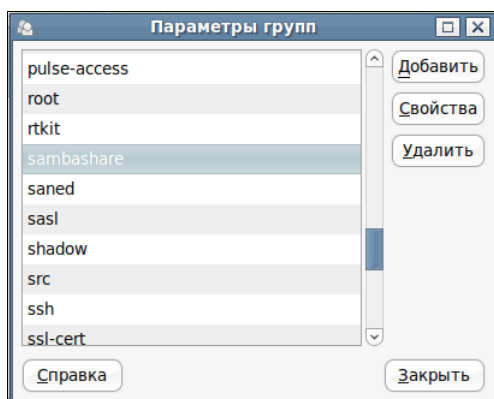


Рис. 12.9. Окно Параметры групп

Теперь создайте текстовый файл на основе примера из листинга 12.1.

### Листинг 12.1. Содержание файла smb.conf

```
[global]
workgroup = BOARD
server string = %h server (Samba, LinuxMint)
encrypt passwords = No
map to guest = Bad User
obey pam restrictions = Yes
pam password change = Yes
```

```
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n ↵
*Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully*
unix password sync = Yes
syslog = 0
log file = /var/log/samba/log.%m
max log size = 1000
dns proxy = No
usershare allow guests = Yes
panic action = /usr/share/samba/panic-action %d
admin users = root, beard
```

```
[beard_lt]
comment = my share
path = /home/beard/share
valid users = beard
force user = beard
read only = No
guest ok = Yes
```

Вместо `beard` введите имя своей учетной записи, вместо `beard_lt` — имя файлового ресурса, который должен быть виден в сети.

Переименуйте файл в `smb.conf` и поместите его в каталог `/etc/samba/`.

Создайте в каталоге вашей учетной записи папку `share` и поместите в нее какой-нибудь файл.

Откройте Web-браузер и введите адрес **<http://localhost:901>**.

При открытии страницы введите имя пользователя `root` и ваш пароль. На открывшейся странице нажмите кнопку **STATUS** (рис. 12.10), а затем кнопку **Перезапустить smbd**.

Теперь с другого компьютера вашей сети вы сможете увидеть созданный файловый ресурс.

На страницах **Глобальные параметры** (рис. 12.11) и **Параметры общих ресурсов** (рис. 12.12) вы можете поэкспериментировать, изменяя параметры вашего сервера.

Создавая новый ресурс с помощью кнопки **Создать ресурс**, надо учесть следующее:

1. Папка нового ресурса должна быть создана предварительно вручную.
2. Перед нажатием кнопки **Создать ресурс** в поле рядом с ней следует вписать полный путь и имя уже созданной папки.

Полезные ссылки:

- <http://www.compress.ru/Archive/CP/2005/1/36/>;
- <http://liski.vsi.ru/ubuntu/index.php?page=95>;
- <http://www.a-byte.ru/node/248>.

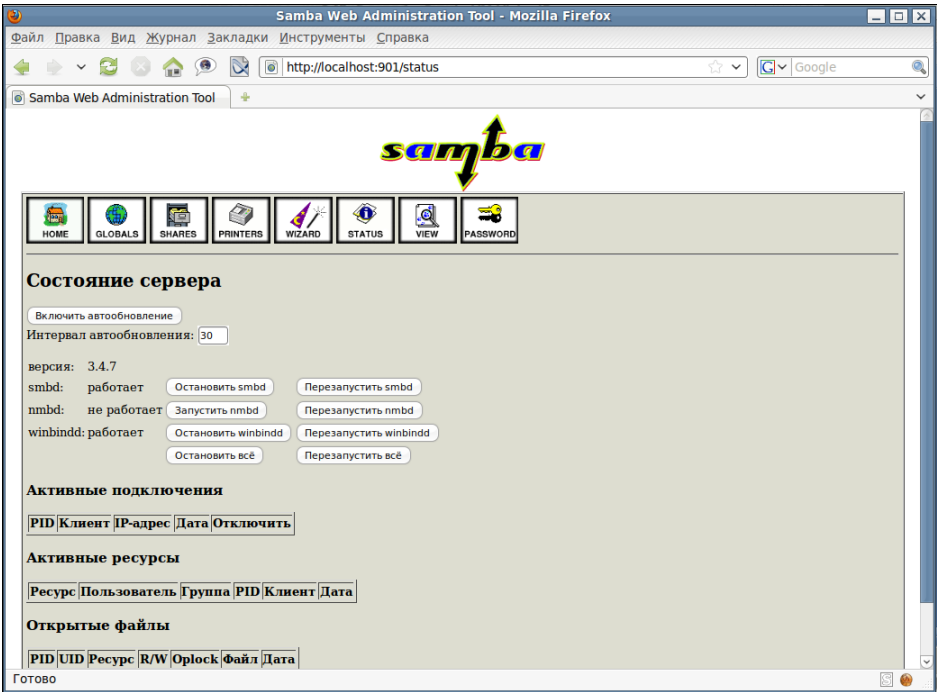


Рис. 12.10. Окно Samba Web Administration Tool — Состояние сервера

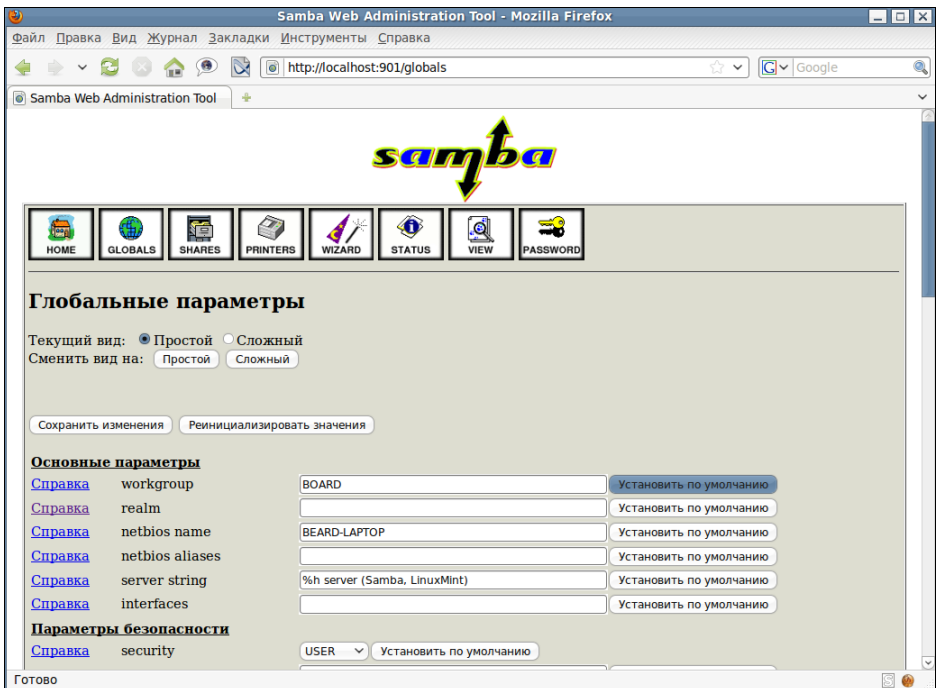


Рис. 12.11. Окно Samba Web Administration Tool — Глобальные параметры



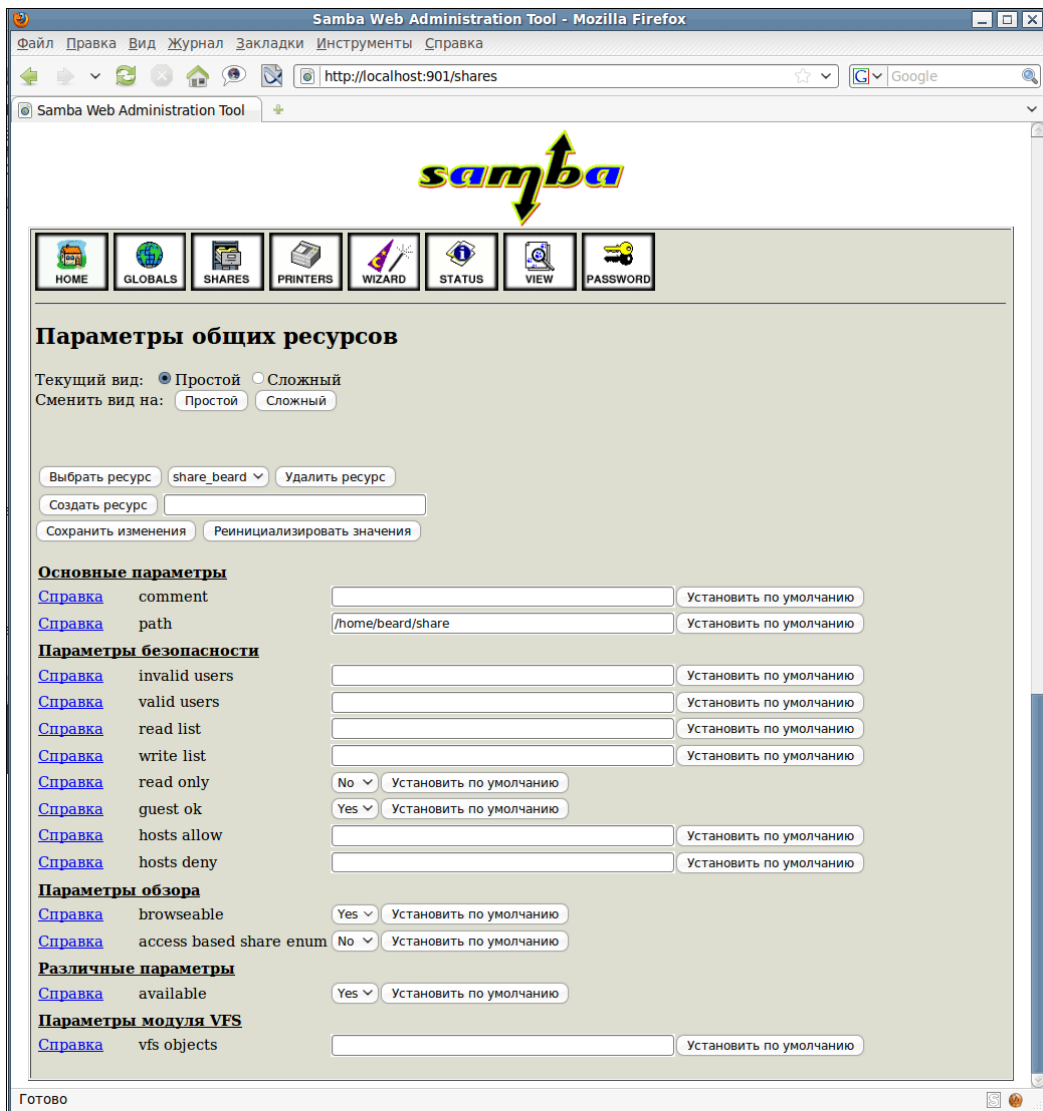


Рис. 12.12. Окно Samba Web Administration Tool — Параметры общих ресурсов

## ГЛАВА 13



# Настраиваем FTP-сервер

FTP-сервер может применяться как в локальной сети, так и в Интернете, если ваша сеть имеет реальный адрес в Интернете. В какой-то степени этот сервер похож на файловый сервер. Но работает он несколько иначе. Для получения доступа к такому серверу требуется специальный FTP-клиент. Одним из самых распространенных являются FTP-клиент, входящий в состав популярного файлового менеджера FAR, а также клиент, встроенный в браузер (browser) Internet Explorer. FTP-сервер удобно применять для хранения файлов, которые должны быть доступны большому числу пользователей, а также для управления файлами на Web-сервере (о Web-сервере разговор будет в *главе 14*).

Для создания FTP-сервера существует множество программ, как платных, так и бесплатных. Ссылки на эти программы можно найти в конце этой главы. Но современные операционные системы Windows имеют в своем составе средства, чтобы создать вполне работоспособный FTP-сервер. В Windows XP, Windows 2000, Windows 2003 эти средства практически не отличаются. Для того чтобы использовать их, необходимо убедиться, что в системе установлен *File Transfer Protocol (FTP) Service*. Этот компонент находится в составе *Internet Information Services (IIS)* (рис. 13.1).

После установки компонента File Transfer Protocol (FTP) Service останется только настроить FTP-сервер, который уже функционирует на вашем компьютере.

Только что установленный FTP-сервер имеет корневой каталог C:\Inetpub\ftproot (рис. 13.2).

Изменить расположение корневого каталога и выполнить другие настройки можно, если перейти по пути **Пуск | Программы | Администрирование | Диспетчер ISS**.

Найдя в открывшемся окне **Узлы FTP**, а в них **Default FTP Site** (FTP-узел по умолчанию) (рис. 13.3), можно через контекстное меню открыть окно свойств нашего FTP-узла (рис. 13.4).

В этом окне, переходя по вкладкам, можно настроить и размещение на диске корневого каталога FTP-сервера, и установить необходимые разрешения на этот каталог.

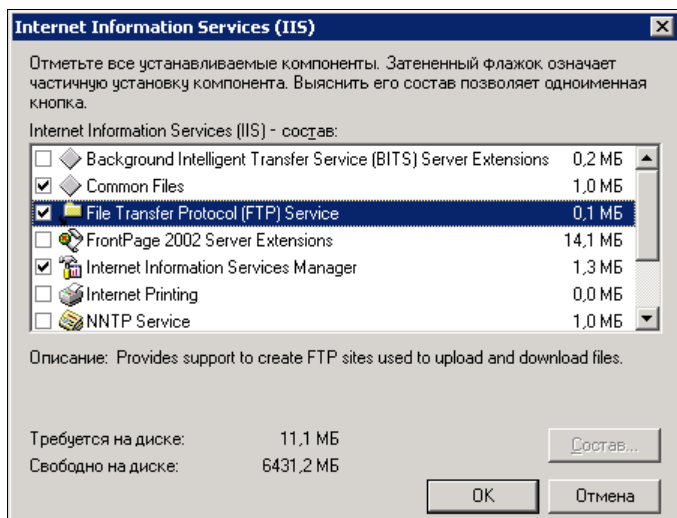


Рис. 13.1. Окно Internet Information Services (IIS) — выбор File Transfer Protocol (FTP) Service

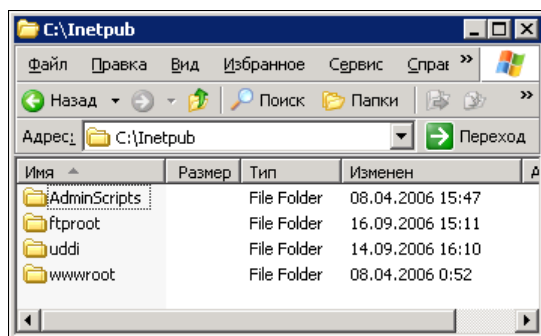


Рис. 13.2. Окно каталога C:\inetpub

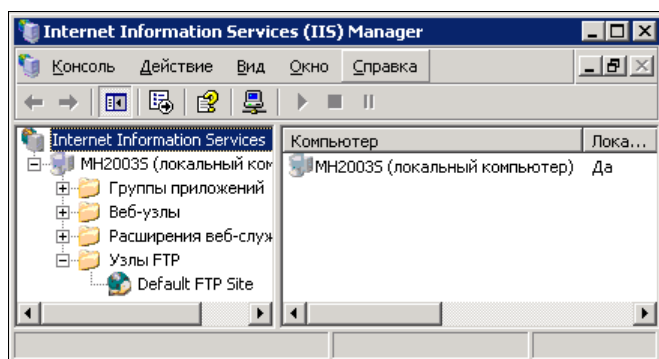


Рис. 13.3. Окно Internet Information Services (IIS) Manager — Узлы FTP

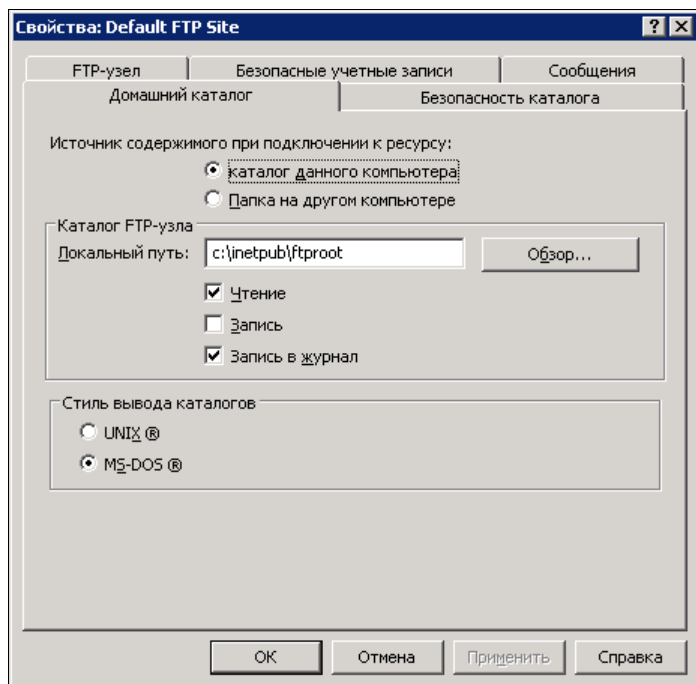


Рис. 13.4. Окно **Свойства: Default FTP Site**, вкладка **Домашний каталог**

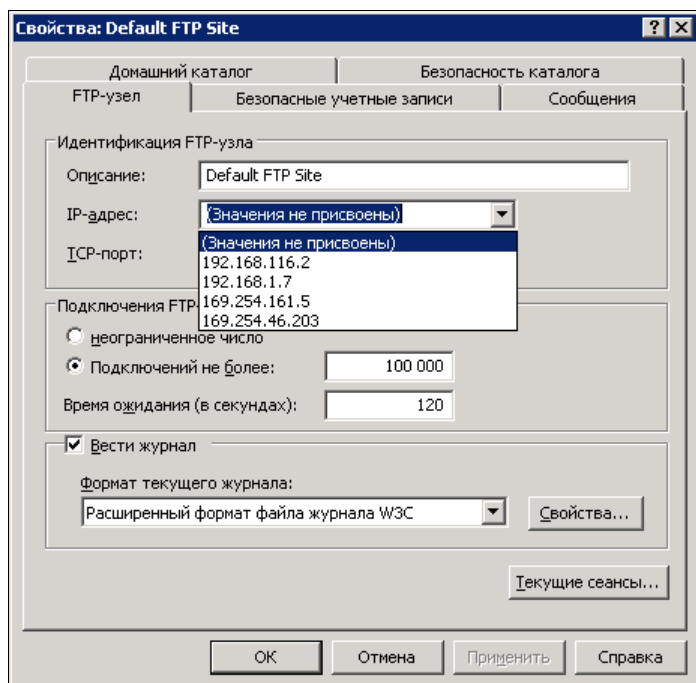


Рис. 13.5. Окно **Свойства: Default FTP Site**, вкладка **FTP-узел**

На вкладке **FTP-узел** (рис. 13.5) можно определить IP-адрес FTP-сервера. Сервер физически может быть подключен к различным сегментам сети и к Интернету. Указав, какой именно IP-адрес принадлежит нашему FTP-серверу, мы ограничим возможность его использования из других сегментов сети.

Остальные настройки сервера можно оставить по умолчанию, а можно на вкладке **Безопасность каталога**, если это необходимо, дополнительно настроить ограничение на число подключений к серверу, настроить сервер на возможность подключения к нему анонимных пользователей или разрешить подключение только определенным учетным записям.

В большинстве случаев, в небольшой сети этих настроек вполне достаточно.

## Клиент FTP

Раз уж мы решили настроить FTP-сервер, необходимо определиться и с клиентом. С помощью какой же программы можно подключаться к FTP-серверу, чтобы получить доступ к файлам? Самый простой путь — использовать браузер Internet Explorer.

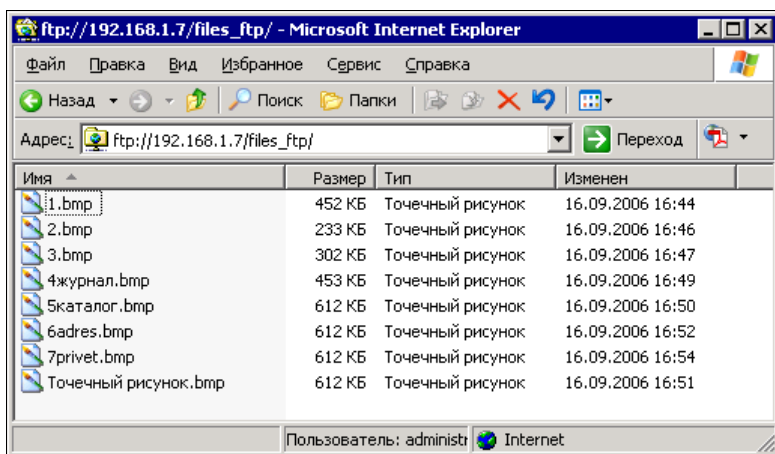


Рис. 13.6. Окно Microsoft Internet Explorer

Достаточно в адресной строке набрать адрес FTP-сервера, указав подкаталог с файлами, и в окне браузера появятся файлы, лежащие на сервере. При наличии разрешений вы сможете использовать это окно как окно обычной папки.

Но многим больше нравятся другие FTP-клиенты. Один из распространенных клиентов входит в состав бесплатного менеджера файлов FAR. Менеджер имеет два окна, в одном из которых при подключении к FTP-серверу будут видны файлы, лежащие на нем, а в другом может быть открыто содержание любого локального каталога (рис. 13.7).

Для того чтобы иметь возможность быстрого доступа к FTP-серверу, адрес сервера можно сохранить в FAR (рис. 13.8).

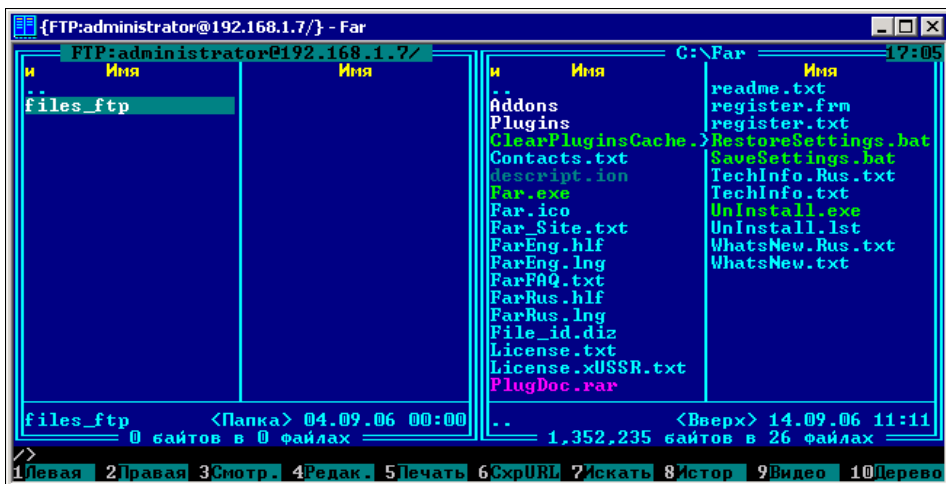


Рис. 13.7. Окно файлового менеджера FAR с открытым окном FTP-клиента

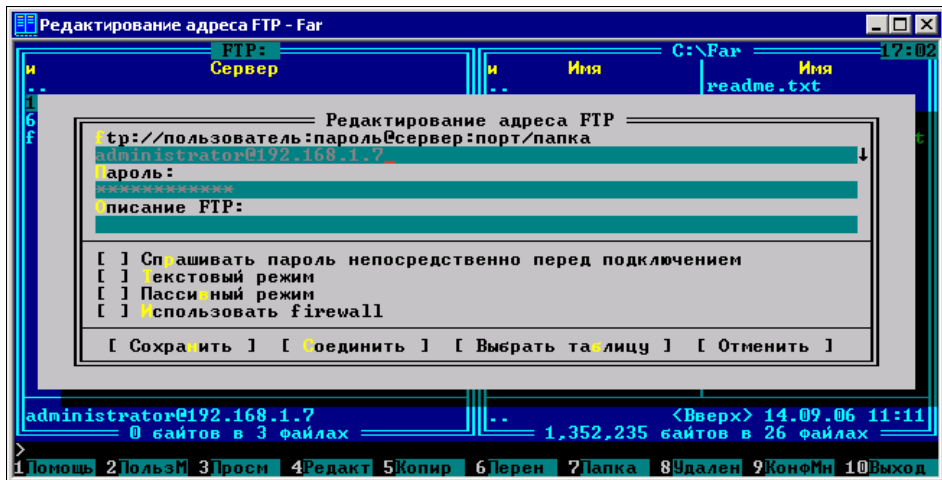


Рис. 13.8. Окно файлового менеджера FAR — Редактирование адреса FTP

FTP-сервер может применяться не только как хранилище файлов, но и как средство оперативного обмена файлами. Достаточно настроить такой сервер в локальной сети и создать каталоги для пользователей сервера. Конечно, в наше время есть немало других средств обмена файлами, но испытанный временем FTP-сервер еще долго не сойдет с арены сетевого обмена.

Для лучшего освоения FTP-сервера и клиента желательно почитать дополнительную литературу, ознакомиться с рекомендациями по настройке других вариантов FTP-сервера, включая и сервер на Linux. Это можно сделать, начав со ссылок, приведенных далее:

- <http://www.computerra.ru/gid/rtfm/internet/37948/>;
- <http://linux4u.jinr.ru/docs/master.doc/admin-html/ch09s03.html>;
- <http://www.citforum.ru/internet/ftp/serv-u/>.

## TFTP-сервер

Этот сервер используется в тех случаях, когда не требуется проверка подлинности пользователя. Существуют версии TFTP-серверов под Windows и Linux. Под Windows распространена программа `tftpd32`, описание которой и сама программа доступны по адресу <http://tftpd32.jounin.net>.

Для работы с сервером должен быть и клиент. В качестве клиентов TFTP могут работать некоторые устройства, например маршрутизаторы. Так, маршрутизаторы Allied Telesis позволяют загружать на них файлы конфигураций с TFTP-сервера.

Версию TFTP-клиента для Windows можно загрузить по адресу <http://www.winagents.ru/products/tftp-client>.

Операционные системы Linux обычно содержат в своих репозиториях несколько версий TFTP-серверов и клиентов. Наиболее совершенными на сегодняшний день можно считать сервер `atftpd` и клиент `atftp`. Вы без труда можете установить эти программы на свой компьютер с Linux.

Проверить работоспособность программ очень просто. Достаточно ввести команды в окне терминала. Для проверки клиента вводим `atftp`, а затем `help`. При этом будет выведена справка по работе с клиентом:

```
beard@beard-laptop ~ $ atftp
tftp> help
Available command are:
connect      connect to tftp server
mode         set file transfer mode (netascii/octet)
option       set RFC1350 options
put          upload a file to the host
get          download a file from the host
mtftp        set mtftp variables
mget         download file from mtftp server
quit         exit tftp
verbose      toggle verbose mode
trace        toggle trace mode
status       print status information
timeout      set the timeout before a retry
help         print help message
?            print help message
tftp>
```

Введя `tftpd`, получим справку по работе с сервером.

```
beard@beard-laptop ~ $ atftpd
Usage: tftpd [options] [directory]
[options] may be:
-t, --tftp-timeout <value>: number of second of inactivity before exiting
-r, --retry-timeout <value>: time to wait a reply before retransmission
-m, --maxthread <value>    : number of concurrent thread allowed
-v, --verbose [value]      : increase or set the level of output messages
```

```

--trace                : log all sent and received packets
--no-timeout           : disable 'timeout' from RFC2349
--no-tsize             : disable 'tsize' from RFC2349
--no-blksize          : disable 'blksize' from RFC2348
--no-multicast         : disable 'multicast' from RFC2090
--logfile <file>      : logfile to log logs to ;-)
--pidfile <file>      : write PID to this file
--listen-local         : force listen on local network address
--daemon               : run atftpd standalone (no inetd)
--no-fork              : run as a daemon, don't fork
--user <user[.group]>  : default is nobody
--group <group>       : default is nogroup
--port <port>          : port on which atftpd listen
--bind-address <IP>   : local address atftpd listen to
--mcast-ttl           : ttl to used for multicast
--mcast-addr <address list>: list/range of IP address to use
--mcast-port <port range> : ports to use for multicast transfer
--pcrc <file>         : use this file for pattern replacement
--pcrc-test <file>    : just test pattern file, not starting ↵
server
--mtftp <file>        : mtftp configuration file
--mtftp-port <port>   : port mtftp will listen
--no-source-port-checking : violate RFC, see man page
--mcast-switch-client : switch client on first timeout, see man ↵
page
-V, --version         : print version information
-h, --help            : print this help

```

Для реальной проверки работоспособности при передаче файлов необходимо в каталог, где установлен TFTP-сервер поместить файл, предназначенный для передачи клиенту. В случае с Linux Mint 9 и atftp этот каталог находится по пути /srv/tftp/.

Создадим и поместим в него файл test.txt. Теперь в окне терминала выполним команды, как в примере:

```

beard@beard-laptop ~ $ atftp 127.0.0.1
tftp> get test.txt
tftp>

```

Файл из каталога tftp загружен в каталог пользователя.

Для выгрузки из каталога пользователя в каталог tftp применяется команда put.

Пользуясь справкой и дополнительной информацией со страницы <http://feyhoa.org.ua/archives/1045>, вы можете настроить работу сервера и клиента по вашему желанию.

Если сервер и клиент установлены на разных компьютерах, то при запуске клиента следует указывать адрес компьютера с установленным сервером.

Возможно, что в вашей сети TFTP-сервера будет достаточно для обмена файлами.



## ГЛАВА 14



# Настраиваем Web-сервер

Для чего нужен Web-сервер, думаю, объяснять не вам. И в Интернете, и в локальных сетях день ото дня растет число Web-страниц и сайтов. В последнее время все больше сайтов и страниц открываются не организациями, а физическими лицами, т. е. обычными пользователями ПК. При хорошем подключении к Интернету Web-страницу или сайт можно разместить даже на своем домашнем сервере. А внутри локальной сети просто и нет другой возможности. Windows 2000 Server и Windows Server 2003 позволяют без проблем настроить Web-сервер.

## Web-сервер средствами ОС

Windows 2000 Server и Windows Server 2003 очень похожи, и в части настройки Web-сервера почти не отличаются. Рассмотрим настройку Web-сервера на основе Windows 2000 Server.

Прежде всего нужно убедиться, что на сервере установлен компонент Internet Information Services (IIS, служба информации Интернета — Web-сервер разработки Microsoft). Если вы сами инсталлировали операционную систему, выбрав вариант установки по умолчанию, то этот компонент должен быть уже установлен. Если нет, то добавить его несложно с помощью диалогового окна **Установка и удаление программ** (его значок находится на Панели управления). Мы будем считать, что основные составляющие этого компонента уже установлены. Для того чтобы удостовериться в этом, сделайте следующее:

1. Выберите **Пуск | Настройка | Панель управления**.
2. Двойным щелчком мыши на значке **Установка и удаление программ** откройте одноименное окно.
3. Нажмите левой кнопкой мыши область **Добавление и удаление компонентов Windows**.
4. В открывшемся окне (рис. 14.1) мастера компонентов Windows посмотрите на состояние флажка **Internet Information Services (IIS)**. Если флажок установлен, то компонент уже есть, если нет, то установите его, установив флажок и нажав кнопку **Далее**.

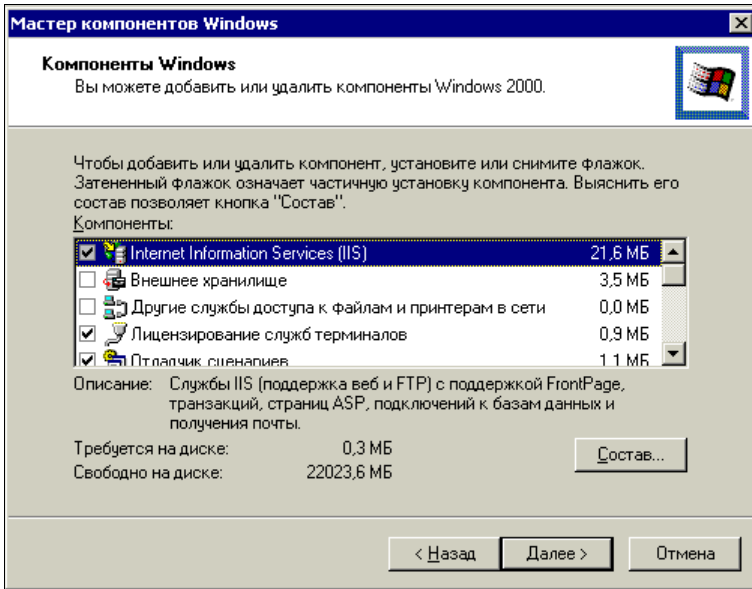


Рис. 14.1. Мастер компонентов Windows

5. С помощью кнопки **Состав** выберите все составляющие компонента Internet Information Services.

После установки IIS, как и в случае его обнаружения в системе, можно приступить к его настройке. Для настройки IIS:

1. Откройте консоль управления Internet Information Services (рис. 14.2). Для этого необходимо выполнить **Пуск | Программы | Администрирование | Диспетчер служб Интернета**.

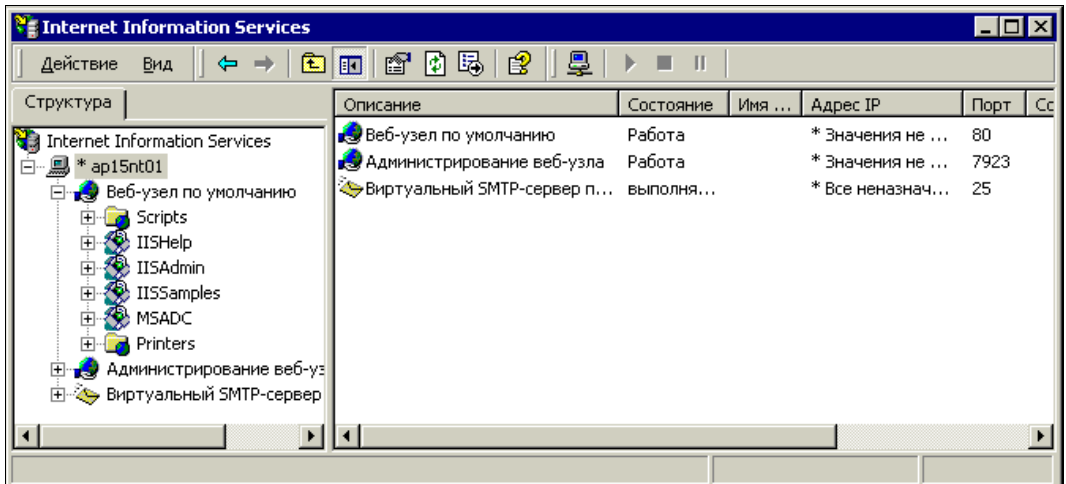


Рис. 14.2. Окно Internet Information Services

- Щелкнув правой кнопкой мыши по имени вашего сервера в левой части консоли, выберите пункт меню **Свойства**. Откроется окно свойств сервера (рис. 14.3).

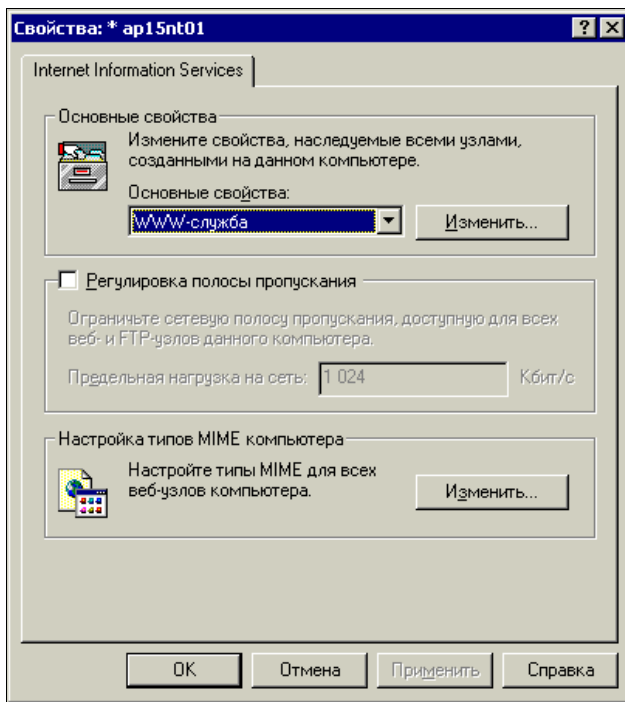


Рис. 14.3. Окно **Свойства: <Имя сервера>**

- Если в раскрывающемся списке **Основные свойства** стоит значение **WWW-служба** — нажмите кнопку **Изменить**. Иначе выберите из раскрывающегося списка это значение и нажмите кнопку **Изменить**.
- Практически все свойства в открывшемся окне **Основные свойства WWW-службы для <Имя сервера>** по умолчанию уже установлены верно, вам следует перейти на вкладку **Документы** (рис. 14.4).
- Установите флажок **Задать документ, используемый по умолчанию**.
- Нажмите кнопку **Добавить**.
- В открывшемся диалоговом окне с единственным полем введите — `Default.htm` и нажмите кнопку **ОК**. Закройте все открытые окна.
- По умолчанию домашним каталогом для вашей страницы назначен `\inetpub\wwwroot`. Найдите его на диске и поместите в него файл `Default.htm`. Это может быть любая созданная вами HTML-страница, названная `Default.htm`.
- Если подготовленной страницы нет, вы можете создать временную, используя текстовый редактор Блокнот. Для этого откройте Блокнот и введите следующий текст:

```
<html>
<head>
</head>
<body>
<h1>
```

На этом месте будет размещена страница нашей организации.

В настоящее время сайт находится в стадии разработки.

```
</h1>
</body>
</html>
```

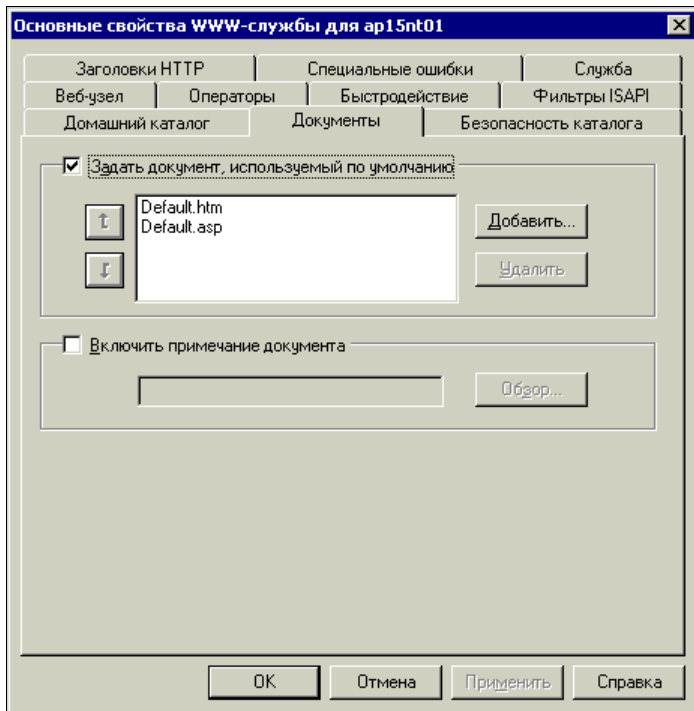


Рис. 14.4. Окно Основные свойства WWW-службы для <Имя сервера>, вкладка Документы

10. Сохраните файл как Default.htm в каталоге \InetPub\wwwroot.
11. Теперь с любого компьютера сети подключитесь к вашему WWW-серверу, набрав в строке адреса имя или IP-адрес вашего сервера. На экране должна появиться страница, показанная на рис. 14.5.

Можно увидеть эту страницу и на экране консоли сервера, введя в качестве адреса — **http://127.0.0.1/**.

Сервер работает. Остается разработать настоящую Web-страницу или сайт и разместить их на сервере.

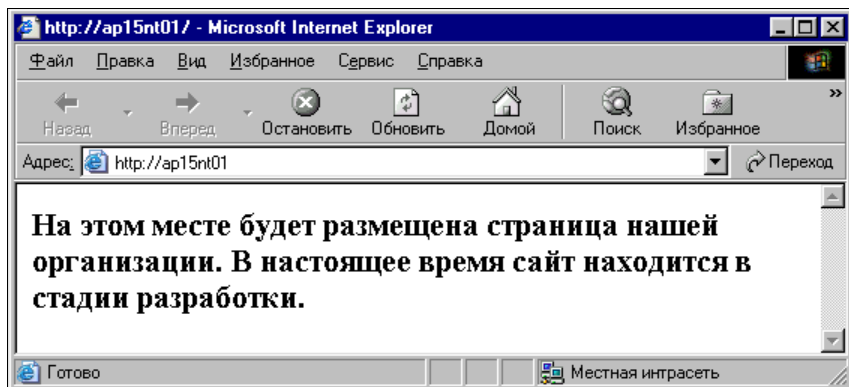


Рис. 14.5. Окно Microsoft Internet Explorer с изображением только что созданной страницы

## Простой Web-сервер другими средствами

Программ для создания Web-сервера разработано немало. Среди них есть достаточно сложные, которые предназначены для организации мощных Web-серверов в Интернете, но есть и совсем простые, на основе которых можно создать Web-сервер даже на компьютере с ОС Windows 98.

Бесплатная программа Analogx Simple Server, которая находится по адресу [www.analogx.com](http://www.analogx.com) как раз одна из таких. Она позволяет создать Web-сервер на любом компьютере вашей сети, если на нем установлена операционная система семейства Windows. Перед установкой программы создайте на диске компьютера каталог WWW и поместите в него уже созданную страницу, но под именем Index.htm.

Установите программу. Установка ее настолько проста, что описания не требует. От регистрации программы можно отказаться, особенно если с данного компьютера нельзя подключиться к Интернету. После установки программы перезагрузите компьютер.

Далее проделайте следующее:

1. Выполните **Пуск | Программы | Analogx | SimpleServer | WWW | SimpleServer.WWW**. Откроется окно программы (рис. 14.6), в котором вы увидите логотип программы и четыре кнопки.
2. Нажав нижнюю длинную кнопку, выберите в окне Проводника файл вашей страницы и нажмите кнопку **OK**.
3. Затем нажмите кнопку **Start**, надпись на которой изменится на **Stop**.
4. На верхней кнопке вы можете прочитать IP-адрес компьютера. Сверните окно (не закрывайте).
5. В строке адреса в окне интернет-браузера на любом компьютере сети наберите имя или IP-адрес компьютера с установленным WWW-сервером. В результате вы увидите созданную вами страницу.

Если все получилось, то создание Web-сервера можно считать завершенным. Этот сервер обладает несколько меньшими возможностями, чем тот, что мы созда-

вали ранее, но тем не менее с успехом может применяться в качестве внутреннего Web-сервера. Сервер поддерживает работу с некоторыми видами скриптов. Сохранив полностью Web-страницу, на которой был размещен калькулятор для расчета стоимости услуг некоторой фирмы, и создав ссылку на нее с основной страницы внутреннего сайта, я мог пользоваться этим калькулятором, не подключаясь к сайту фирмы.

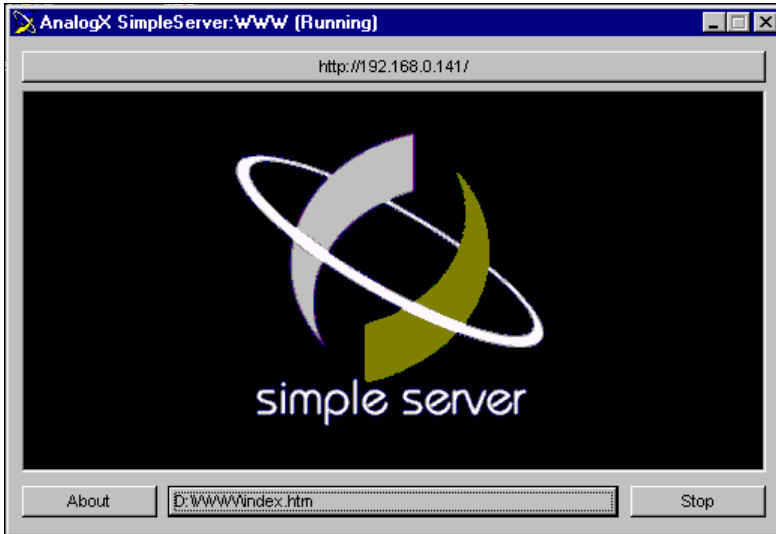


Рис. 14.6. Окно программы AnalogX SimpleServer

Простой Web-сервер для Linux (на английском языке) можно найти по адресу: <http://www.acme.com/software/thttpd/>.

По этой ссылке можно найти не только сервер, но и множество рекомендаций по работе с ним: <http://www.sysoev.ru/nginx/>.

А это форум, где обсуждается проблема домашнего сервера: <http://www.sysadmin.mail.ru/pforum/viewtopic.php?p=77255>.

Об установке Web-сервера Apache под Windows можно прочитать на странице <http://www.xakep.ru/magazine/xs/022/038/1.asp>.

## ГЛАВА 15



# Настраиваем DHCP-сервер

DHCP<sup>1</sup>-сервер позволяет существенно облегчить жизнь администратору сети, а иногда это вообще единственная возможность для реализации очень полезных функций в сети. Например, без DHCP-сервера, скорее всего, не удастся организовать бездисковую загрузку рабочих станций.

Но и в самых обычных сетевых буднях DHCP-сервер может выполнять настройку рабочих станций для работы в сети и для доступа в Интернет.

Установка DHCP-сервера в Windows 2000 Server или Windows Server 2003 не представляет никакого труда. Это всего лишь один из компонентов серверной системы Windows. Можно установить DHCP-сервер и на другую операционную систему, если воспользоваться программами сторонних разработчиков, правда, отдельно он не поставляется и может быть в комплекте с другими продуктами. Кроме того, DHCP-сервер может быть в составе Linux и аппаратных маршрутизаторов.

Существует и отдельная версия сервера ссылки, которую можно найти в статье "DHCP под Windows XP: полет нормальный" по адресу [http://www.citforum.ru/operating\\_systems/windows/dhcp\\_winxp/](http://www.citforum.ru/operating_systems/windows/dhcp_winxp/).

В моей домашней (квартирной) сети есть Windows-сервер, но DHCP работает в ADSL Router D-Link DSL-500T, обеспечивая раздачу IP-адресов и передавая рабочим станциям адрес DNS-сервера и адрес шлюза в Интернете. Причем, используют этот сервер как рабочие станции Windows, так и рабочие станции, на которых загружена ОС Linux.

Все же, самый простой путь получить DHCP-сервер в локальной сети — это использовать встроенный в операционную систему сервер.

## DHCP-сервер Windows Server 2003

Итак, DHCP-сервер должен передавать рабочим станциям значения параметров сети. Тем не менее, значения этих параметров определяются администратором сети

---

<sup>1</sup> Dynamic Host Configuration Protocol — протокол динамического конфигурирования узла (хост-машины).

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 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 совершенно произвольно лишь для иллюстрации возможностей настраиваемого DHCP-сервера. В качестве шлюза в Интернете в сети работает ADSL-модем с IP-адресом 192.168.1.1. DNS-сервер используем с адресом 195.34.32.116.

## Установка

Для установки DHCP-сервера можно воспользоваться мастером настройки сервера (рис. 15.1) (**Администрирование | Мастер настройки сервера**). Следует добавить очередную роль для нашего сервера. В данном случае это DHCP-сервер.

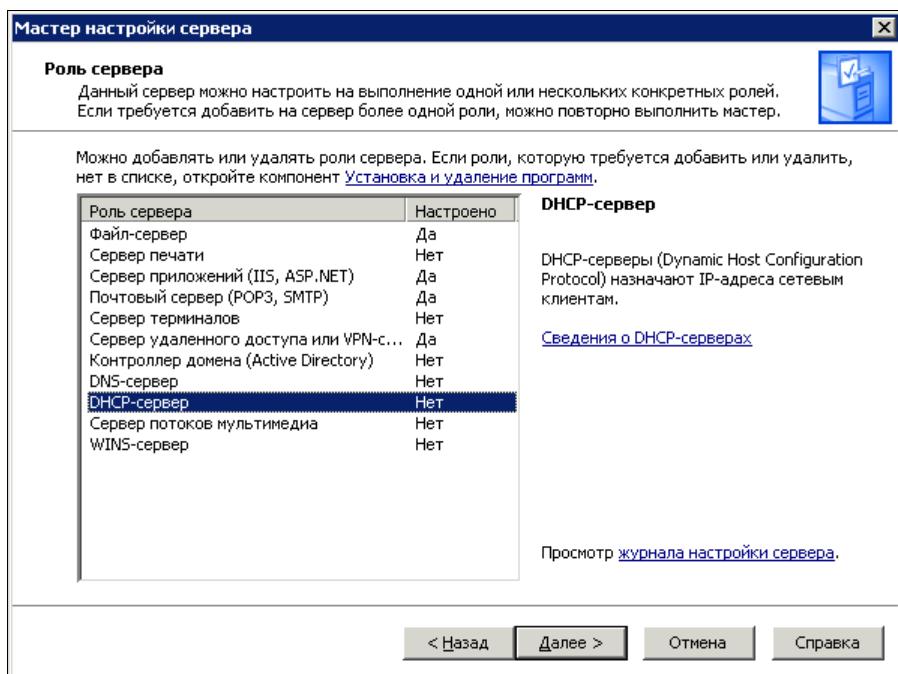


Рис. 15.1. Окно Мастер настройки сервера



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. 15.2).

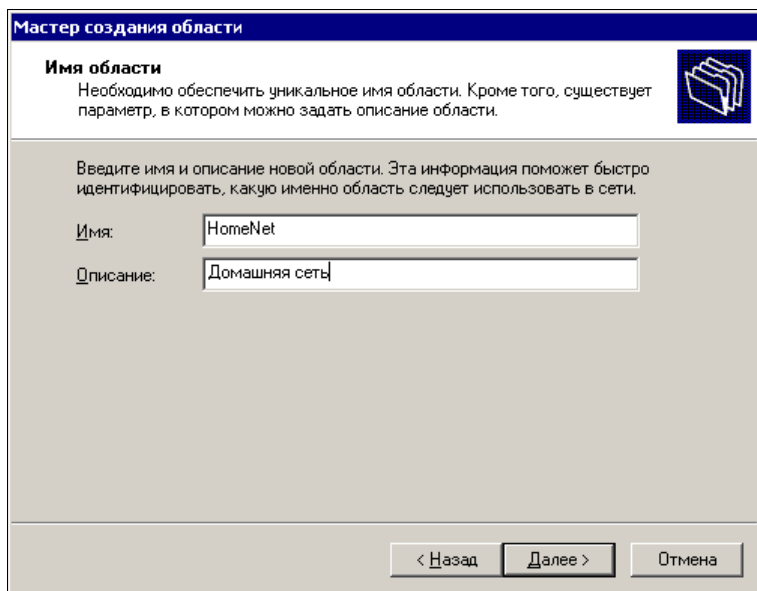


Рис. 15.2. Окно **Мастер создания области**, раздел **Имя области**

В следующем окне (рис. 15.3) следует 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.

В следующем окне (рис. 15.4) 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 потребуются сведения о домене и DNS-сервере. Но мы еще не включали свой сервер в домен, а в качестве DNS-сервера используем тот, что рекомендован провайдером. Поэтому адрес DNS-сервера указываем 195.34.32.116 (рис. 15.5) 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.

Окно с сообщением об успешной установке DHCP-сервера представлено на рис. 15.6.

**Мастер создания области**

**Диапазон адресов**

Определить диапазон адресов области можно задавая, диапазон последовательных IP-адресов.

Введите диапазон адресов, который описывает область.

Начальный IP-адрес:

Конечный IP-адрес:

Маска подсети определяет, сколько битов IP-адреса использовать для идентификации сети, а сколько битов использовать для идентификации узла внутри этой сети. Можно определить маску, задавая IP-адрес или ее длину.

Длина:

Маска подсети:

< Назад    Далее >    Отмена

Рис. 15.3. Окно Мастер создания области, раздел Диапазон адресов

**Мастер создания области**

**Добавление исключений**

Исключения являются адресами или диапазонами адресов, которые исключаются из распределения DHCP-сервером.

Введите диапазон IP-адресов, который необходимо исключить. Если требуется исключить один адрес, введите его только в поле "Начальный IP-адрес".

Начальный IP-адрес:     Конечный IP-адрес:    

Исключаемый диапазон адресов:  
   

< Назад    Далее >    Отмена

Рис. 15.4. Окно Мастер создания области, раздел Добавление исключений

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 она получит IP-адрес из указанного нами диапазона, адрес DNS-сервера и адрес шлюза в Интернете. Это можно увидеть, посмотрев состояние сетевого подключения (рис. 15.7).

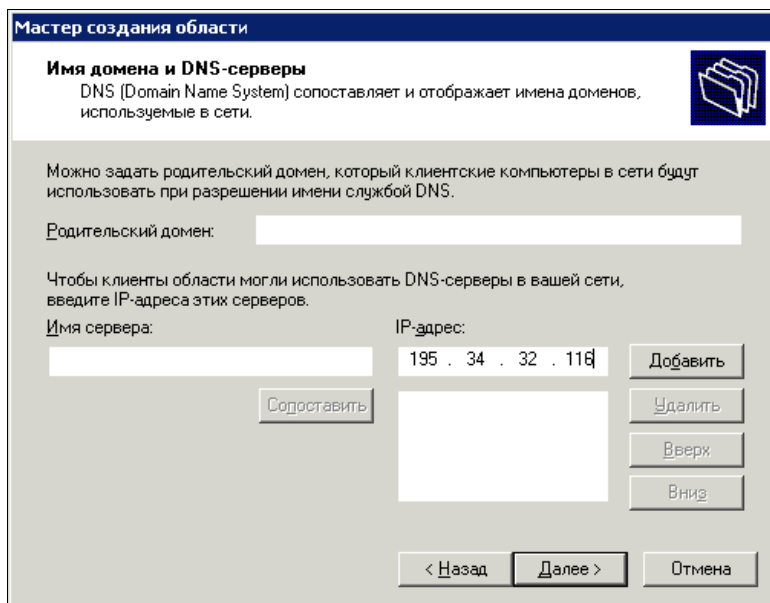


Рис. 15.5. Окно **Мастер создания области**, раздел **Имя домена и DNS-серверы**

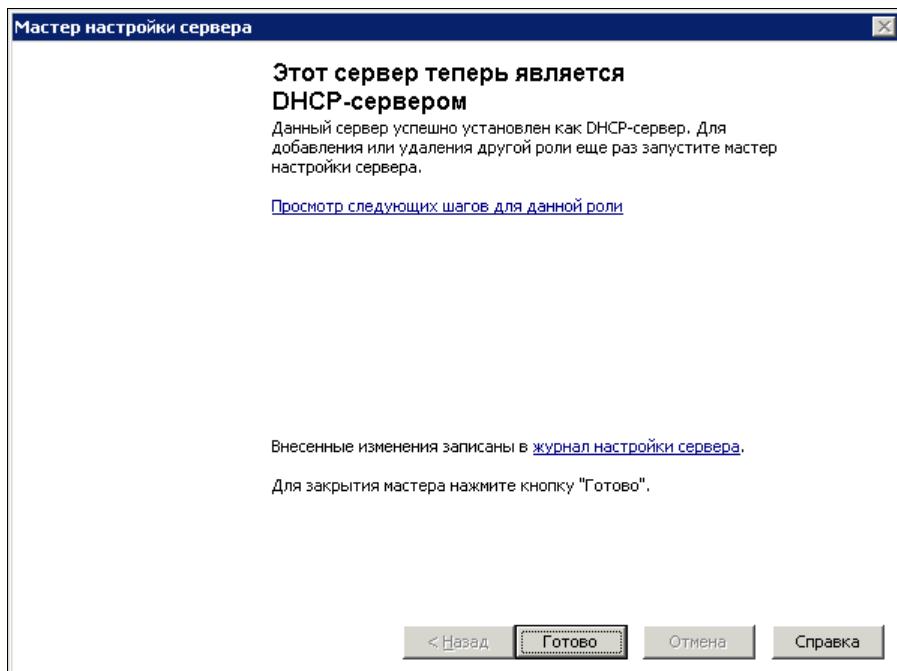


Рис. 15.6. Окно **Мастер настройки сервера**, сообщение об успешной настройке

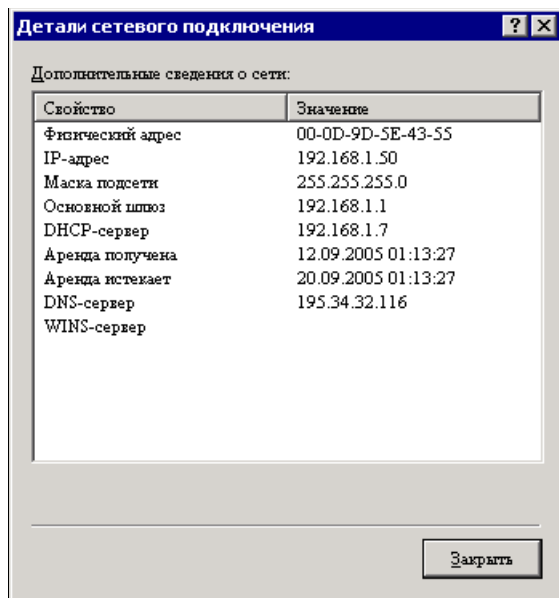


Рис. 15.7. Окно **Детали сетевого подключения**

DHCP-сервер работает. Теперь не потребуется перенастраивать параметры TCP/IP-протокола на моем ноутбуке, когда я буду приходить домой. Достаточно просто подключить его к сети, а DHCP-сервер все настроит самостоятельно.

## Резервирование IP-адреса на DHCP-сервере

В отдельных случаях бывает необходимо, чтобы IP-адрес рабочей станции никогда не изменялся в сети. Для этого следует настроить резервирование IP-адреса на

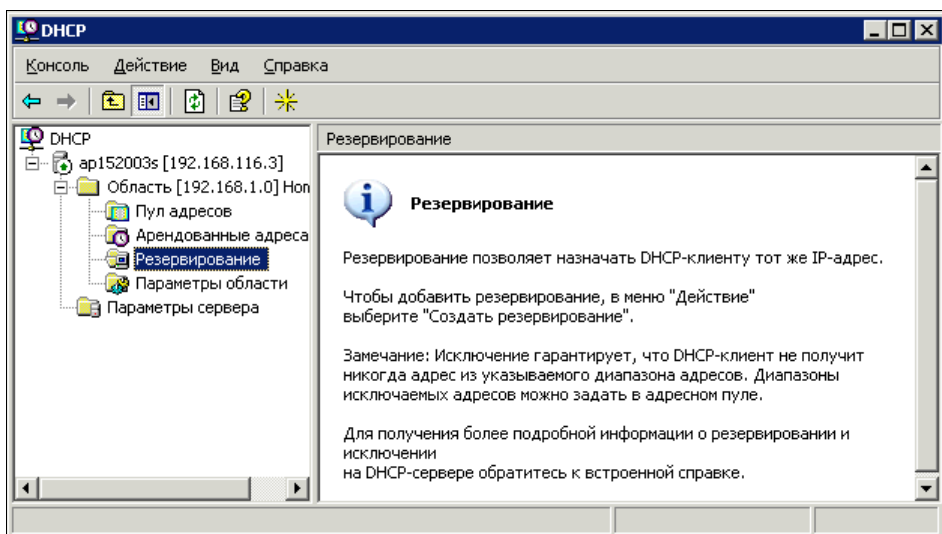


Рис. 15.8. Окно DHCP, узел **Резервирование**

DHCP-сервере. Чтобы получить доступ к его настройкам, достаточно открыть окно **DHCP (Администрирование | DHCP)**. На рис. 15.8 показано это окно при первом обращении к узлу **Резервирование** в дереве объектов консоли DHCP. В контекстном меню этого объекта следует выбрать пункт **Создать**. При этом на экран будет выведено окно **Создать резервирование** (рис. 15.9).

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 в командной строке (рис. 15.10).

Если на вашем компьютере установлено несколько сетевых адаптеров, то следует выбрать тот, что подключен в данный момент к вашей сети.

После ввода всех необходимых данных резервирование будет создано (рис. 15.11).

Теперь при каждом подключении к сети компьютер будет получать один и тот же IP-адрес, а в перечне **Арендованные адреса** (рис. 15.12) напротив адреса вашего компьютера будет указано, что это активное резервирование.

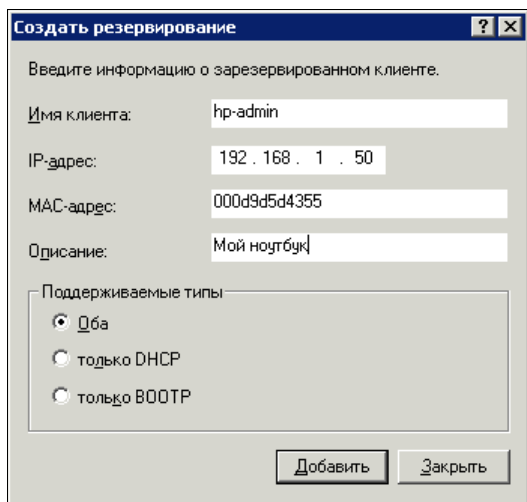


Рис. 15.9. Окно **Создать резервирование**

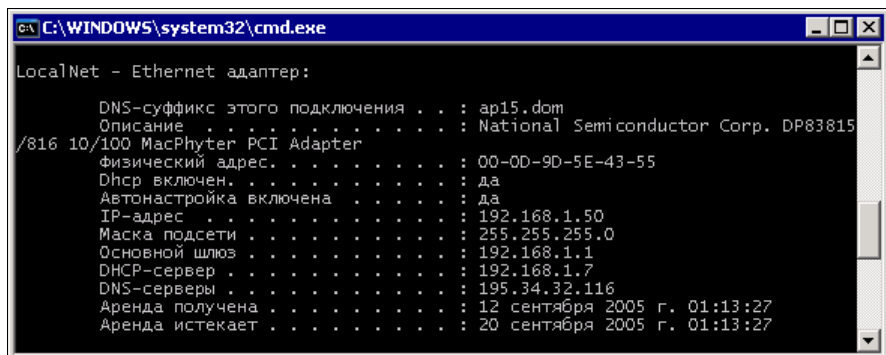


Рис. 15.10. Окно командной строки со значением физического (MAC) адреса

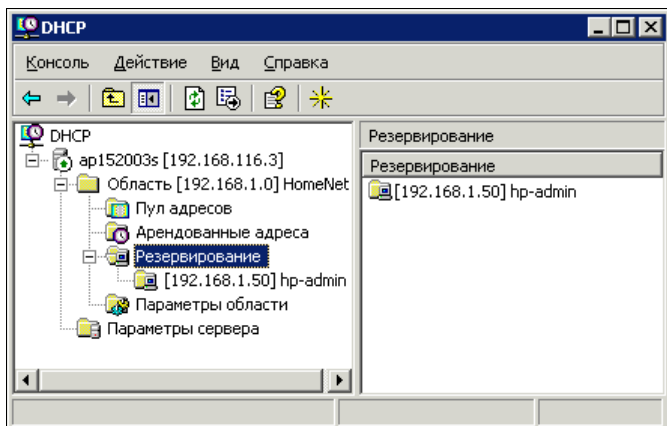


Рис. 15.11. Окно DHCP с созданным резервированием

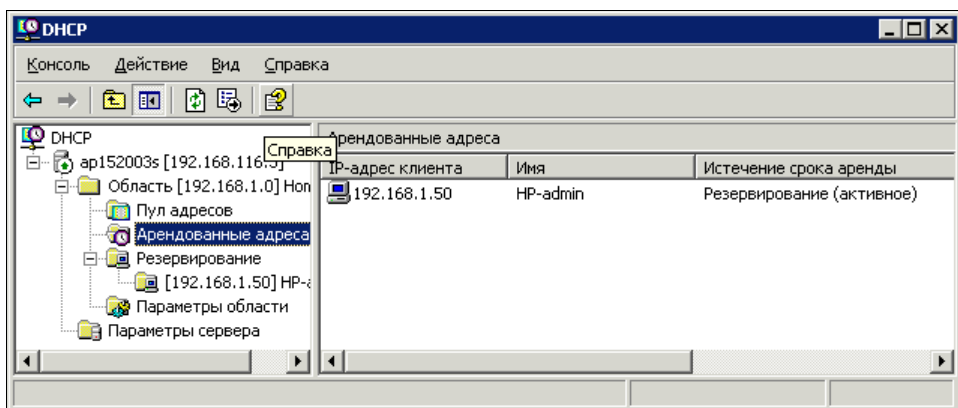


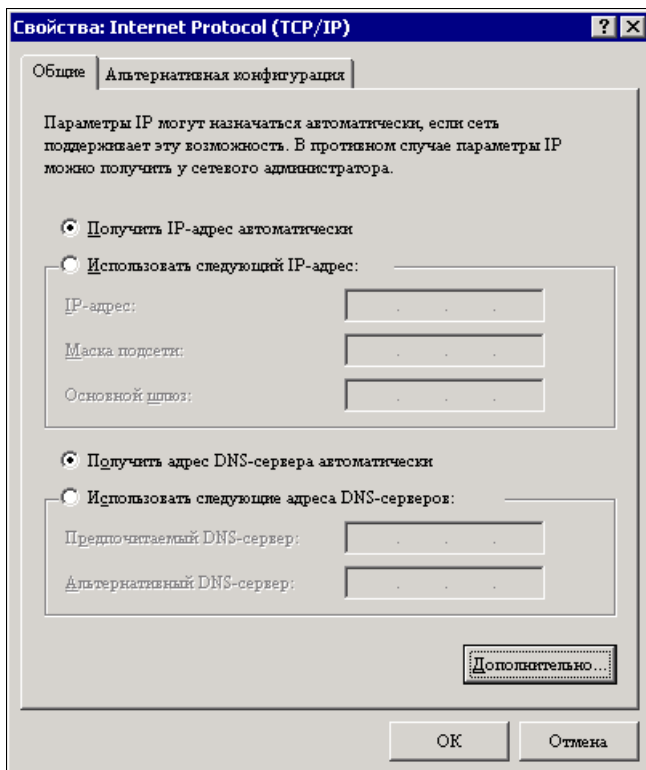
Рис. 15.12. Окно DHCP, узел Арендные адреса

## Дополнительные настройки

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 завершенной. Некоторые дополнительные настройки могут потребоваться после установки DNS- и WINS-серверов для того, чтобы клиенты могли автоматически получать их IP-адреса.

Наличие DHCP-сервера в сети избавит вас от множества проблем в период преобразований в 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. 15.13).



**Рис. 15.13.** 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.

В заключение главы следует сделать одно важное замечание. В сети обычно не должно быть двух DHCP-серверов. Если же появилась такая необходимость, каждый DHCP-сервер должен обслуживать свою область адресов. Не должно быть возможности у серверов выдавать одинаковые IP-адреса компьютерам сети. Конфликт адресов в сети приводит к неработоспособности рабочих станций с повторяющимися адресами, возможны и более серьезные проблемы.

DHCP-серверы в других реализациях могут быть и сложнее и проще в настройках. DHCP-сервер, встроенный в ADSL Router D-Link DSL-500T, имеет совсем немного настроек. На рис. 15.14 показано окно Web-интерфейса настройки DHCP-сервера, встроенного в этот ADSL Router.

У этого DHCP-сервера есть возможность назначить IP-адреса из определенного диапазона, передать адрес DNS-сервера и установить время аренды IP-адреса клиентами. В данном случае, через час отсутствия активности рабочей станции в сети ее адрес может быть выдан другой рабочей станции.

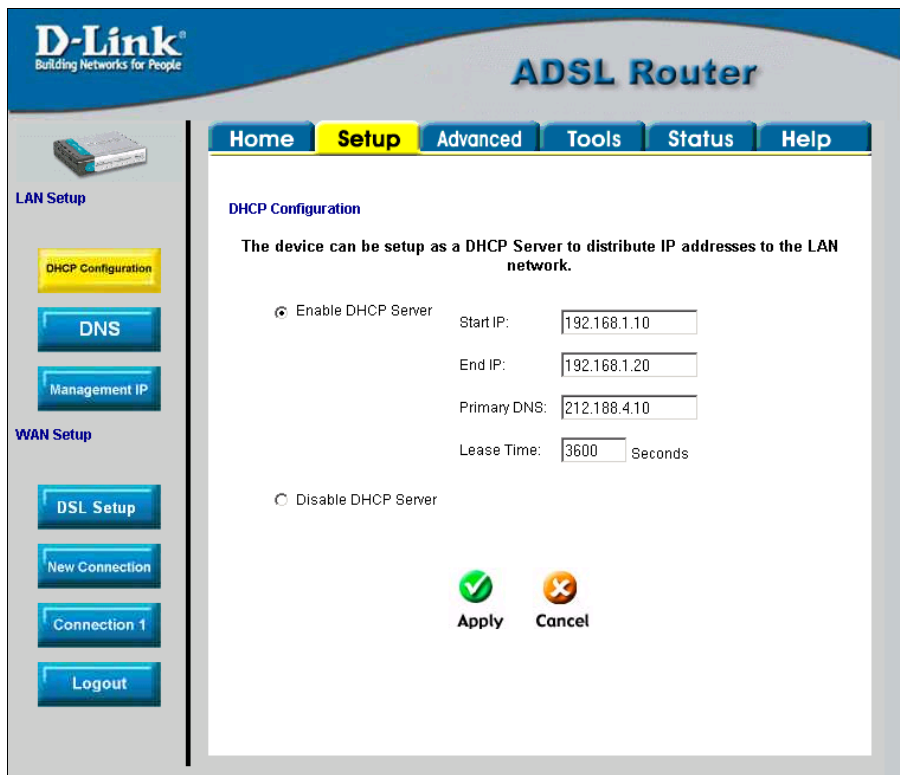


Рис. 15.14. Окно **Setup DHCP Configuration** DHCP-сервера, встроенного в DSL-500T

Далее приведены ссылки на страницы в Интернете, где можно узнать некоторые подробности о работе DHCP-сервера:

- DHCP для терминальных решений

<http://www.wtware.ru/netman/netman1.html>;

- установка DHCP-сервера

[http://www.thg.ru/howto/20040731/windows\\_server-04.html](http://www.thg.ru/howto/20040731/windows_server-04.html);

- где взять DHCP

<http://xpoint.ru/forums/searching/thread/32063.xhtml>;

- развертывание DHCP

[http://oszone.net/3973\\_2#0.1\\_01000011](http://oszone.net/3973_2#0.1_01000011).

## Простой DHCP-сервер на базе Linux Ubuntu

Если вы устанавливаете в качестве шлюза в Интернет для других компьютеров сети отдельный компьютер, то в качестве DHCP-сервера может работать программа Firestarter (см. главу 2). Если вы не используете Firestarter, а выполняете настройки классическим для Linux способом, то потребуется установка и настройка DHCP-



сервера, который будет обеспечивать получение IP-адресов компьютерами сети через интерфейс, который "смотрит" в локальную сеть. В примере этот интерфейс eth0.

Предполагается, что вы уже присвоили этому интерфейсу адрес 192.168.0.1 в сети 192.168.0.0/24.

Устанавливаем DHCP-сервер:

```
apt-get install dhcp3-server
```

В файле /etc/default/dhcp3-server необходимо определить интерфейс, на котором будет работать сервер:

```
INTERFACES="eth1"
```

Настраиваем DHCP-сервер. Для этого в файле /etc/dhcp3/dhcpd.conf меняем параметры domain-name и domain-name-server на свои значения:

```
option domain-name "uadomain.dom";
option domain-name-servers 192.168.0.1;
```

В конце файла добавляем секцию, описывающую нашу сеть:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.2 192.168.0.254;
    option domain-name-servers <адрес DNS-сервера вашего провайдера>;
    option routers 192.168.0.1;
}
```

При необходимости можно указать MAC-адрес сетевой карты компьютера, который всегда должен получать один и тот же IP-адрес:

```
host first {
    hardware ethernet 00:E0:4C:B7:C2:59;
    fixed-address 192.168.0.200;
}
```

Остается перезапустить DHCP-сервер:

```
/etc/init.d/dhcp3-server restart
```

Теперь нет необходимости каждому компьютеру сети присваивать IP-адрес и вести учет этих адресов.

### **ПРИМЕЧАНИЕ**

Если компьютер общего доступа к сети Интернет не используется для работы на нем, то можно применить серверную версию Ubuntu, которая не имеет графического интерфейса. Но настройки верны и для других операционных систем на базе Ubuntu.

## ГЛАВА 16



# Настраиваем WINS-сервер

Еще один сервер, который может функционировать на нашем физическом или виртуальном сервере — WINS-сервер.

## WINS-сервер Windows Server 2003

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 этих 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 нетрудно установить на вашем сервере. Процедура установки аналогична установке других рассмотренных серверов, но совершенно не требует настроек. Окно WINS-сервера (рис. 16.1) содержит информацию о зарегистрировавшихся клиентах.

Внеся в свойства области DHCP-сервера, сведения о WINS-сервере, рабочие станции получают 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 по доступности в сети, содержащей WINS-сервер. Но и для новых ОС дополнительный сервер имен не помещает. Клиентов в нашей сети не очень много, и компьютер, содержащий несколько серверов имен, не будет испытывать затруднений при обработке регистраций.

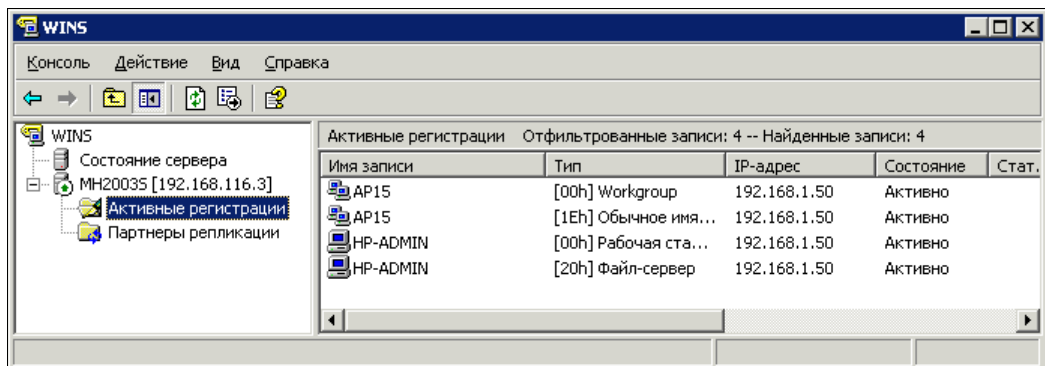


Рис. 16.1. Окно WINS, узел Активные регистрации

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 протокола NetBIOS через TCP/IP (рис. 16.2).

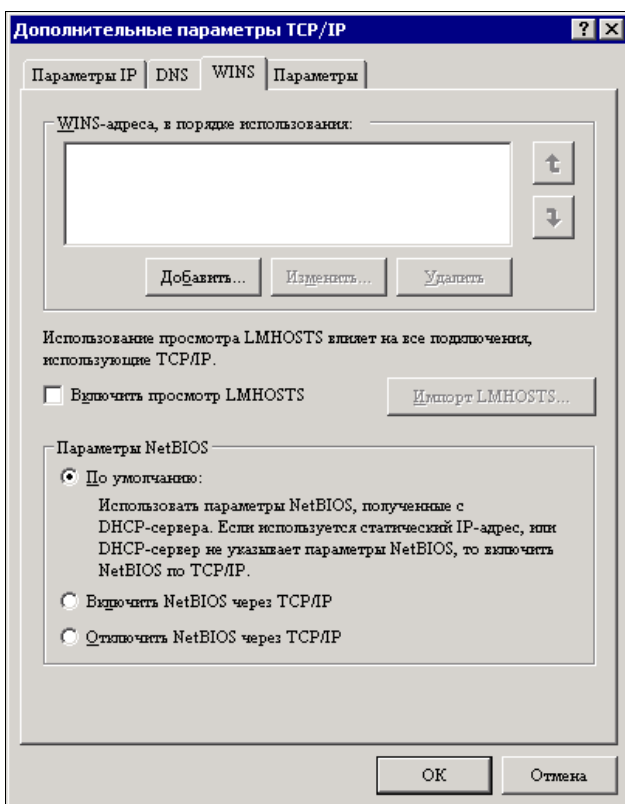


Рис. 16.2. Окно Дополнительные параметры TCP/IP

## Пример локальной сети с WINS-сервером

Для более глубокого осмысления и понимания приведенных настроек рассмотрим дополнительно схему локальной сети, в которой эти настройки проводились. Клиентская рабочая станция этой сети получает все сетевые параметры с DHCP-сервера, которые могут быть прочтены из окна **Детали сетевого подключения**, доступного через контекстное меню этого подключения — **Состояние** (рис. 16.3).

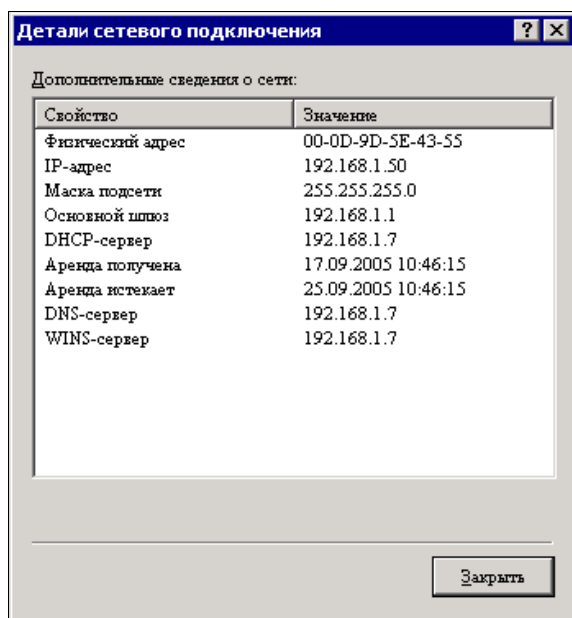


Рис. 16.3. Окно **Детали сетевого подключения**

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. 16.4.

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. Таким образом, 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.

На рис. 16.2 вы могли заметить, что не отмечен флажок **Включить просмотр LMHOSTS**. При включении 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 станет доступной всем рабочим станциям.

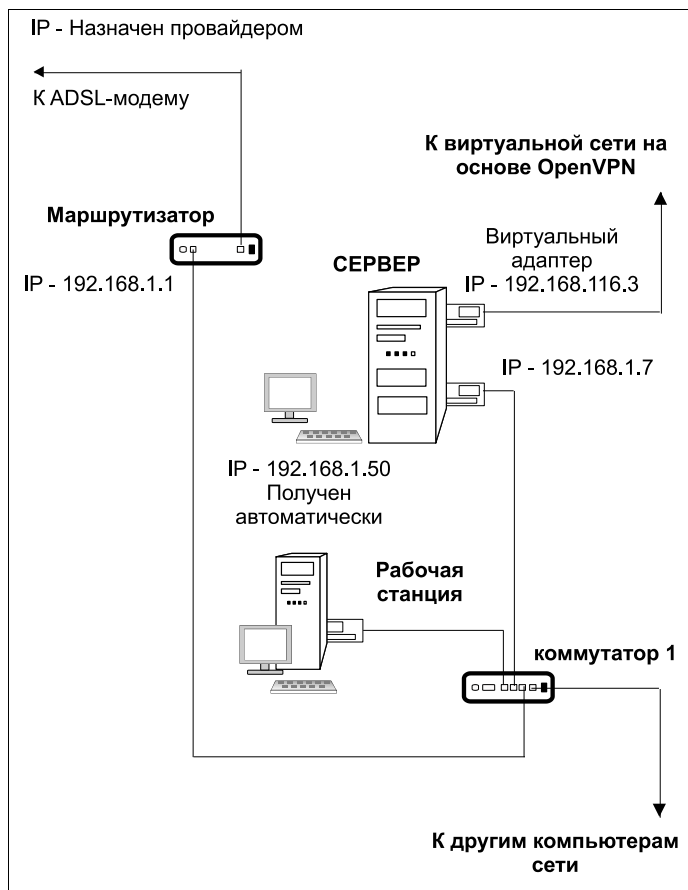


Рис. 16.4. Схема тестовой сети

Для того чтобы внести сведения о таком соответствии, можно в консоли WINS-сервера в контекстном меню значка **Активные регистрации** выбрать команду **Создать статическое сопоставление**. При этом откроется окно (рис. 16.5), в котором следует указать имя компьютера и его IP-адрес. Поле **Область NetBIOS** заполнять не обязательно.

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.

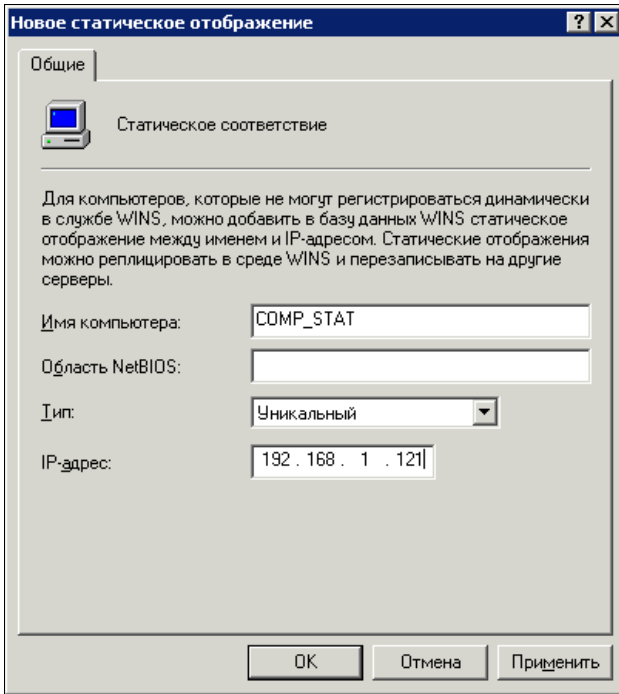


Рис. 16.5. Окно Новое статическое отображение

Как было сказано ранее, настройки WINS-серверу после установки не требуются. Тем не менее в сети могут возникать проблемы при работе с этим сервером. Все они обычно решаются достаточно просто, если есть понимание того, как работает WINS-сервер. Но иногда возникают проблемы, решение которых не совсем очевидно. В этом случае следует обратиться к народному опыту.

Вот ссылки, которые помогут правильно применить WINS-сервер:

- ❑ [http://ptk.vrn.ru/lib/win/nt\\_5.2/book/Glava13/Index43.html](http://ptk.vrn.ru/lib/win/nt_5.2/book/Glava13/Index43.html);
- ❑ <http://info.mitht.rssi.ru/wins/>;
- ❑ <http://forum.ixbt.com/post.cgi?id=print:86:17>;
- ❑ <http://www.icomf.ru/index.php?name=PNphpBB2&file=viewtopic&p=7609>;
- ❑ [http://forums.avalon.ru/forum/topic.asp?TOPIC\\_ID=5507](http://forums.avalon.ru/forum/topic.asp?TOPIC_ID=5507);
- ❑ <http://bugtraq.ru/cgi-bin/forum.mcgi?type=sb&b=4&m=112534>;
- ❑ <http://www.opennet.ru/openforum/vsluhforumID1/38526.html>.

# ГЛАВА 17



## Настраиваем DNS-сервер

### Зачем DNS-сервер в сети

В сети нет ничего лишнего и каждая ее составляющая важна. Важно и то, чтобы эта составляющая была правильно настроена. Вот и DNS-сервер — это обязательная составляющая локальной сети с Active Directory. Без DNS-сервера в сети невозможно установить соответствие IP-адресов их символьным значениям, а Active Directory не сможет собрать сведения о компьютерах и пользователях сети.

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 сможем настроить сетевые программы, а также узнавать компьютеры в сети при необходимости административного воздействия, по именам. 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 далее в *главе 18*. 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 исполь-



зует 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. Имя домена, которое будет содержать DNS-сервер, сразу можно указать такое, которое 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. 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. Более того, в сети может быть не один DNS-сервер, они могут помогать друг другу, снижая нагрузку на физические серверы.

## DNS-сервер Windows Server 2003

Аналогично другим настройкам сервера, устанавливать и настраивать DNS-сервер можно через мастер настройки сервера (**Администрирование** | **Мастер на-**

стройки сервера). После установки DNS-сервера будет вызван мастер настройки DNS-сервера (рис. 17.1).

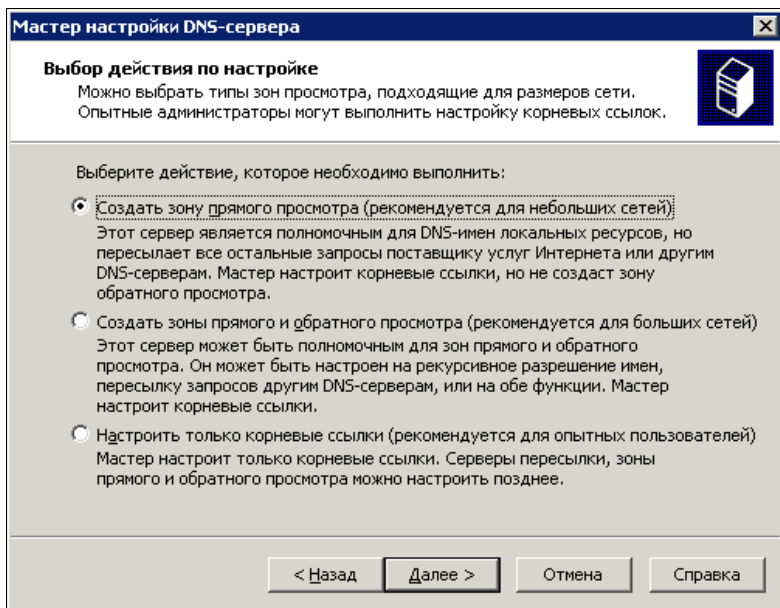


Рис. 17.1. Окно Мастер настройки DNS-сервера

Мастер предлагает варианты настроек, а нам остается выбрать наиболее подходящий. 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, а зоне прямого просмотра дать понятное имя. Если во время установки что-либо настроено не совсем так, как хотелось, то всегда можно исправить ситуацию. Достаточно открыть консоль DNS-сервера (**Администрирование | DNS**) и внести изменения в настройки (рис. 17.2).

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. 17.3), 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.

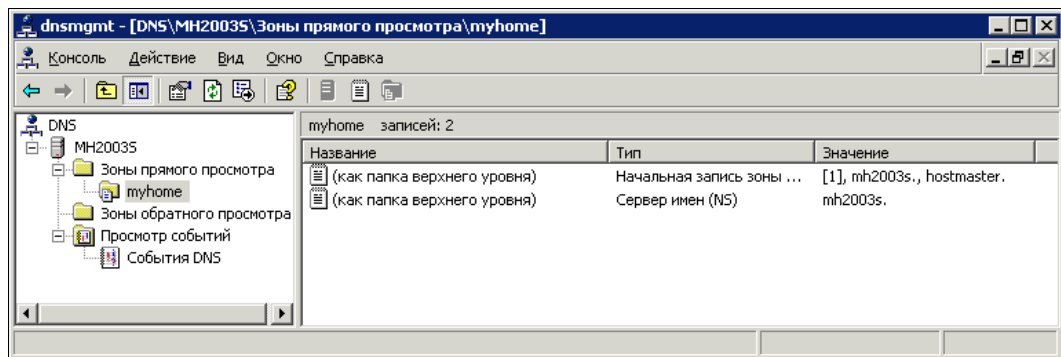


Рис. 17.2. Окно dnsmgmt

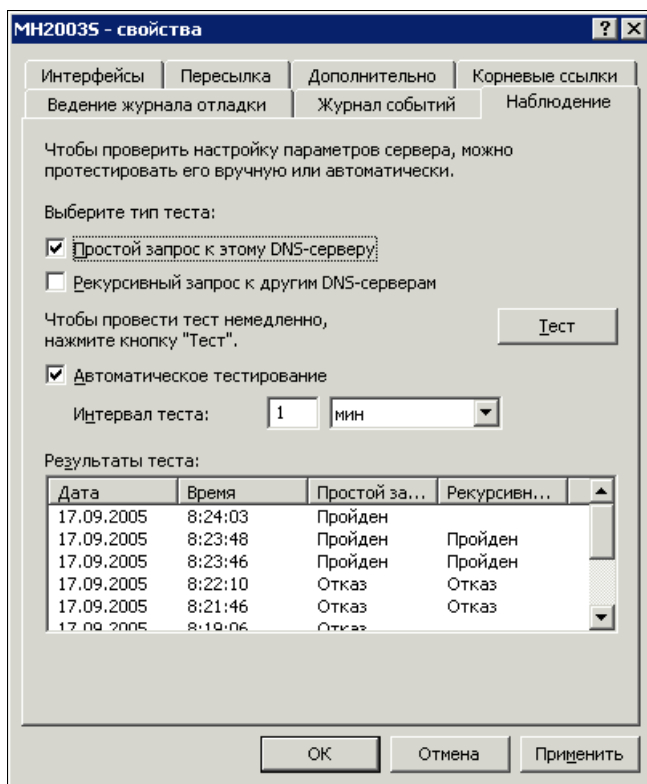


Рис. 17.3. Окно MH2003S — свойства, вкладка Наблюдение

Прежде всего, мы знаем, что наш сервер еще не имеет регистрации в Интернете. Следовательно, ему требуется помощь других DNS-серверов для поиска имен в глобальной сети. Для этого надо указать известные вам адреса DNS-серверов на вкладке **Пересылка** окна свойств сервера (рис. 17.4).

Конечно, убедитесь, что внешние DNS-серверы доступны. Вероятнее всего, потребуется подключение к Интернету.

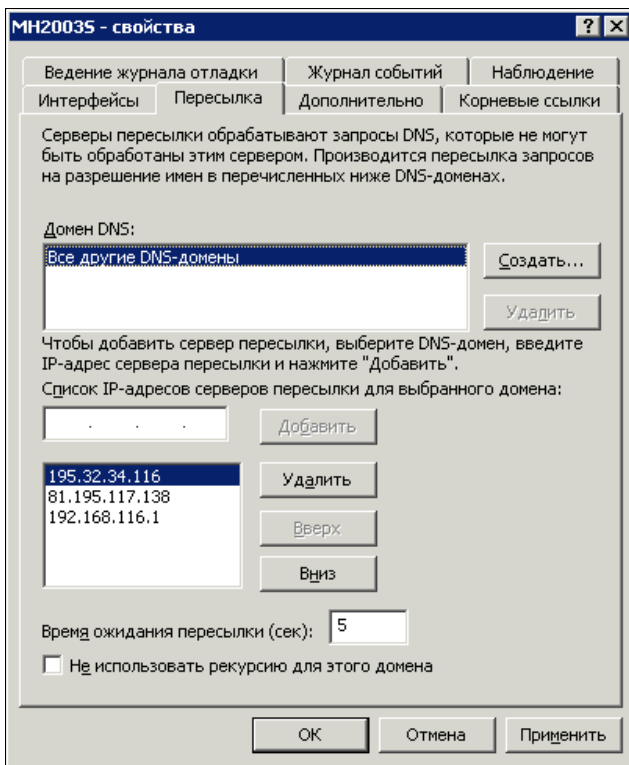


Рис. 17.4. Окно МН2003S — свойства, вкладка Пересылка

Большинство задач DNS-сервера, входящий в ОС Windows Server 2003, выполняет самостоятельно. Как только вы получили положительный результат теста для DNS-сервера, внесите небольшую корректировку в настройки DHCP-сервера (рис. 17.5).

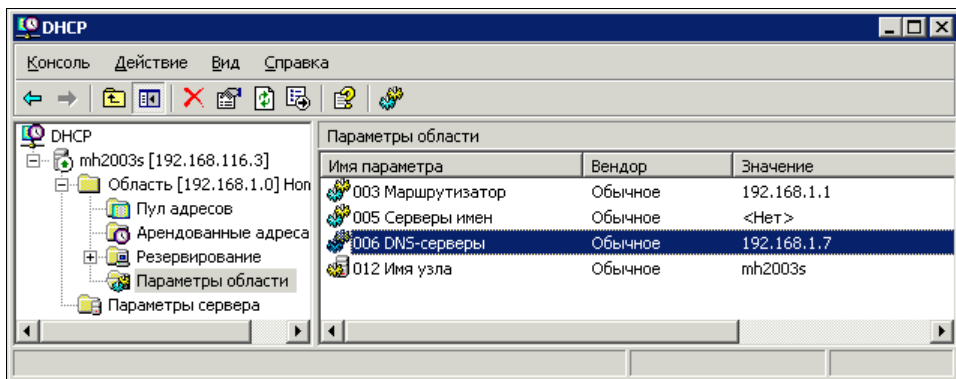


Рис. 17.5. Окно DHCP, узел Параметры области

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 шанс не настраивать рабочие станции в нашей сети, а дать им возможность самостоятельно получить все необходимые сетевые настройки.

В приведенных далее ссылках вы найдете не только информацию о настройке простого DNS-сервера, но и объяснение настроек DNS-сервера в Интернете. В какой-то момент вы наверняка встретитесь с необходимостью если не настраивать, то понять эти настройки. Кто знает, может быть, вы обзаведетесь собственным Web-сервером в Интернете. А это вполне реально, достаточно получить у провайдера выделенный IP-адрес и зарегистрировать доменное имя, а дальше — дело техники.

- ❑ <http://xnets.ru/plugins/content/content.php?content.128>.
- ❑ <http://networkdoc.ru/files/insop/win2003/read.html?dns.html>.
- ❑ [http://forum.smart-soft.ru/forum\\_posts.asp?TID=9166&PN=1](http://forum.smart-soft.ru/forum_posts.asp?TID=9166&PN=1).
- ❑ <http://weec.ovl.ru/xmbforum/viewthread.php?tid=436>.

DNS-сервер в Linux

- ❑ <http://sudouser.com/ustanovka-i-nastrojka-dns-servera-bind9-ubuntu-debian-howto.html>.

## ГЛАВА 18



# Настраиваем media-сервер

В локальных сетях такой сервер встречается не очень часто. Особенно, когда это сеть предприятия. Основное время пользователи занимаются серьезными делами, и им некогда отвлекаться по пустякам. Но на ситуацию можно посмотреть с разных сторон. Во-первых, медиасодержимое сети может применяться и в производственных целях. Различные обучающие или информационные материалы могут транслироваться по сети, и каждый пользователь может подключиться и просмотреть или прослушать эти материалы. Если же сеть домашняя или квартирная, то допустима постоянная трансляция материалов развлекательного характера. Причем трансляция возможна как свободная, так и по подписке. Второй вариант позволит несколько разгрузить сеть от лишнего трафика. Вариантов для организации media-сервера существует несколько. Здесь и решения от Microsoft, и решения на основе свободного программного обеспечения, которое может работать не только на серверной платформе, но и на обычной рабочей станции, которая может стать media-сервером в вашей сети. Это значит, что любой пользователь сети может организовать свою сетевую или интернет-студию для трансляции аудио- и видеоинформации.

## Кодировщик Windows Media 9 Series

Этот кодировщик можно найти по адресу

<http://www.microsoft.com/windows/windowsmedia/ru/9series/encoder/default.aspx>.

Программа позволяет передавать не статические изображения, сменяемые с заданными интервалами, а настоящее видео, сопровождаемое звуком. Сигнал от Web-камеры и микрофона (или другого источника звука) 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, решение которых необходимо для достижения целей.

К сожалению, описание всех шагов создания медиасервера займет очень много места, если начинать с процедуры создания Web-сервера. Об этом много сказано на страницах в Интернете и просто в справке Windows. Примем, как данное, что Web-сервер уже есть или вы его можете создать самостоятельно. Сейчас поговорим только о том, как включить в Web-страницу видеоинформацию, как настроить передачу этой информации в Интернете. С помощью Windows Media 9 Series 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. На принимающем компьютере 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 щелкните правой кнопкой мыши и выберите команду **Свойства страницы**.
3. Задайте необходимый цвет фона, шрифта и другие параметры по желанию.
4. В главном меню программы выберите команду **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 выбираем ячейку 2×2. В своей странице можете выбрать и другую ячейку.
7. Щелкните левой кнопкой мыши на выбранной ячейке.
8. В главном меню программы выберите команду **Вставка | Веб-компонент**, а в открывшейся форме — команду **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 щелкните правой кнопкой на вставленном элементе (он занимает всю ячейку) и выберите команду **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 программа 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 будет указываться в адресной строке браузера. Другой сервер — дополнительный, для трансляции видеопотока. Его адрес должен быть указан в свойствах ActiveX-элемента. 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 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 щелкните 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. Нажимаем 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 с помощью кнопки **Найти свободный порт** определить свободный порт. В этом случае и в свойствах элемента ActiveX на Web-странице потребуется смена значения порта.
7. На следующем экране в поле **Скорость** задайте необходимую скорость. 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 задать минимальную скорость. Можно указать два варианта сразу, у пользователя скорость будет выбрана автоматически.

8. Если на следующем экране отметить опцию **Сохранить копию потока вещания** и указать файл, в который поток будет сохранен, то 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 настройки прямого вещания вы сможете разобраться самостоятельно.
9. Далее будет предложено выбрать файлы для вступления, антракта и финала или производить кодирование только с выбранных устройств. Выбираем кодирование только с выбранных устройств и нажимаем кнопку **Далее**.
10. На следующем экране вводим информацию о заголовке, авторе и другую текстовую информацию или не вводим ничего. Снова нажимаем кнопку **Далее**, а затем — кнопку **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. 18.1).

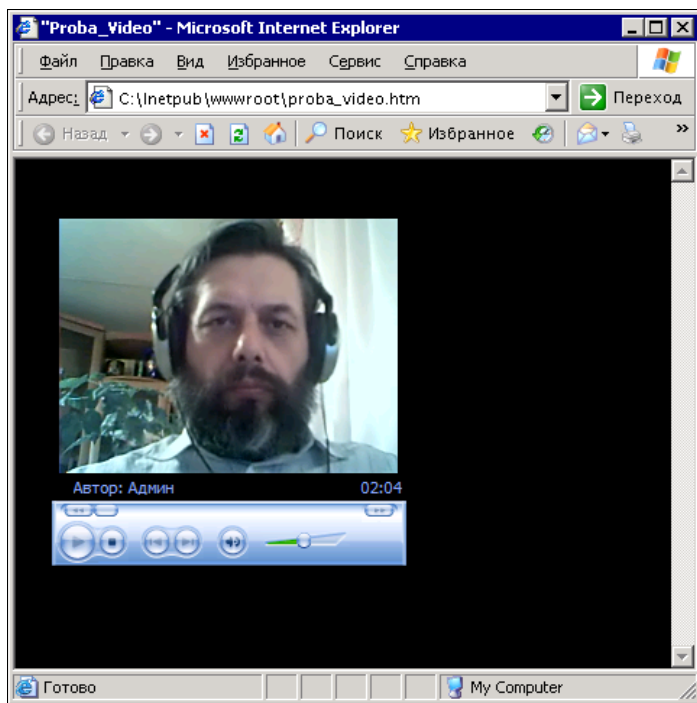


Рис. 18.1. Окно браузера с только что созданной страницей

Теперь, поэкспериментировав с камерой и программами, чтобы добиться желаемого вами результата, вы можете поместить страницу на доступный другим пользователям сервер, настроив 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 также несколько микрофонов и другие источники звука.

Windows Media 9 Series может работать только на платформе Windows. Но в настоящее время все более активно проникает к обычным пользователям Linux. Целая армия разработчиков свободного программного обеспечения создает программы, которые могут соперничать с программами от Microsoft, а нередко оказываются и более удобными, более функциональными, а к тому же и мультиплатформенными. Они могут работать и под Linux, и под Windows.

Одна из таких программ — VLC Media Player.

## VLC Media Player — трансляция по сети

Достаточно подробное описание программы для первого знакомства с ней можно найти на странице <http://chelcom.ru/modules/smartsection/item.php?itemid=95>.

К сожалению, я не нашел в Интернете достаточно подробного описания работы с программой в качестве сервера. Но это не беда. Несмотря на определенную трудоемкость ручных настроек, во многих практических случаях можно запустить мастер настроек, которых в программе предусмотрено довольно много. После завершения работы мастера можно вручную подкорректировать настройки, если что-либо в них вас не устраивает.

### **ВАЖНОЕ ЗАМЕЧАНИЕ**

VLC Media Player содержит множество кодеков, которые необходимы для воспроизведения видео- и аудиофайлов и потоков. Если VLC Media Player используется в качестве media-сервера, то наилучшим средством воспроизведения передаваемого им потока также будет VLC Media Player.

### **ЕЩЕ ОДНО ЗАМЕЧАНИЕ**

Для того чтобы VLC Media Player мог легко находить, а главное сохранять play-листы, их файлы должны располагаться по короткому пути. Лучше создать каталог с подкаталогами в корне диска. Попытка сохранить play-лист в папку Мои документы может не увенчаться успехом.

Установка программы под Windows никаких проблем не вызывает. В Linux возможны некоторые проблемы, зависящие от версии системы. Пока этих версий очень много, и разбираться с установкой вам придется самостоятельно или с помощью службы поддержки вашей версии Linux. Если все установится нормально, то работа с программой не будет иметь серьезных отличий от работы в среде Windows. Программу, скорее всего, вы уже скачали, а если нет, то скачайте перед тем, как читать следующие строки.

## Передача

Давайте теперь настроим VLC Media Player для трансляции видеопотока в сеть. Для этого нам потребуется:

- работающая сеть;
- два компьютера (можно две рабочие станции);
- видеофайл, который мы будем транслировать;
- установленный на обоих компьютерах пакет VLC Media Player.

В описании настроек мы будем использовать файл с записью давнего выступления Аллы Борисовны Пугачевой — `Alla_Pugacheva_Starinnye_chasy.avi`, который поместим в каталог `C:\PlayVLC`. В тот же каталог будем сохранять и `play`-листы. Если у вас нет такого файла, то вы, конечно, можете использовать любой имеющийся.

Программа, запущенная в первый раз, выглядит так просто и компактно (рис. 18.2), что незнакомый с ней человек вряд ли сможет предположить, какие широкие возможности в ней заложены.

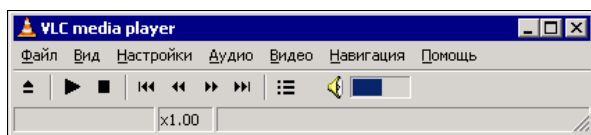


Рис. 18.2. Окно VLC media player

Для обычного воспроизведения аудио и видео достаточно, воспользовавшись главным меню программы, открыть нужный файл. После выбора команды **Файл | Открыть файл** вы увидите окно выбора источника информации (рис. 18.3).

Выбрав предложенными средствами файл для проигрывания, останется нажать кнопку **ОК**, и начнется воспроизведение. Но... нам этого не требуется.

Все, что вы сделали сейчас, нужно только для того, чтобы убедиться, что VLC Media Player работает. Для того чтобы запустить трансляцию нашего видео в сеть, немного модифицируем наши действия.

1. Выполните команду **Файл | Мастер**. Откроется окно мастера, который поможет оперативно настроить трансляцию (рис. 18.4).
2. Выберите в этом окне опцию **Вещание** в сеть и нажмите кнопку **Next**.
3. Отметьте опцию **Существующий список воспроизведения**.
4. Мы только что воспроизвели файл, список воспроизведения программа запомнила, и вы увидите строку с именем нашего файла. Нажмите кнопку **Next**.
5. Выберите поток вещания в следующем окне (рис. 18.5).

Метод вещания (в одноименной группе опций) можно выбрать любой, но вариант **RTP Unicast** позволяет вести трансляцию на конкретный IP-адрес, **RTP Multicast** ведет трансляцию на диапазон IP-адресов или подсеть, а **HTTP** позволяет любому компьютеру сети подключиться к передаче, используя ваш

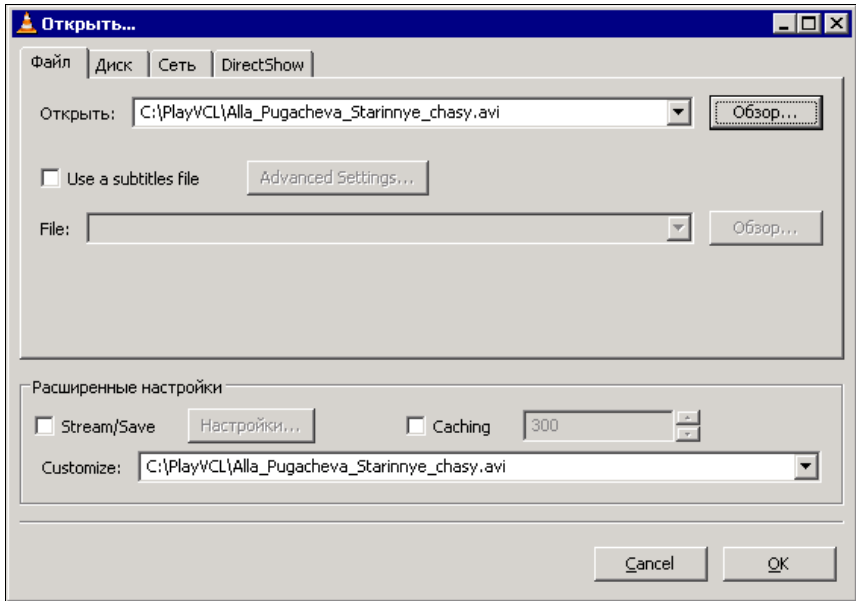


Рис. 18.3. Окно Открыть...

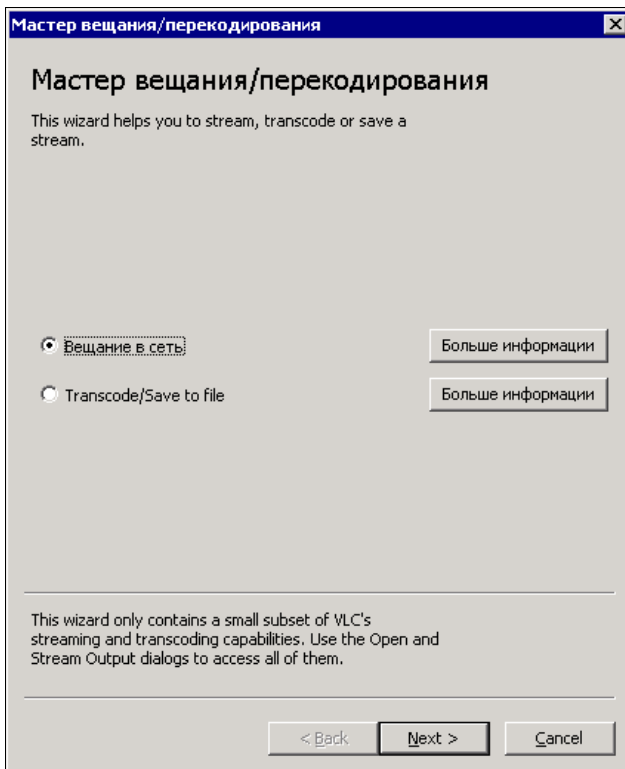


Рис. 18.4. Окно Мастер вещания/перекодирования

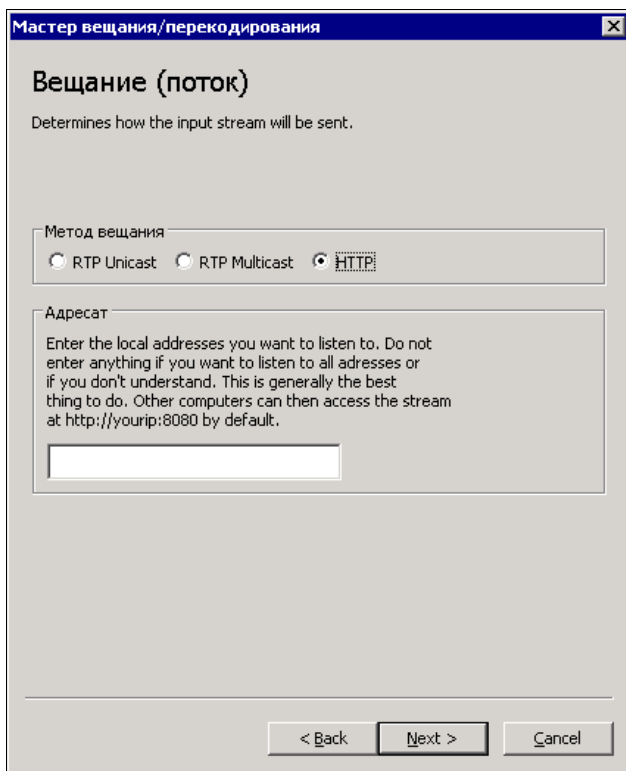


Рис. 18.5. Окно **Мастер вещания/перекодирования**, раздел **Вещание (поток)**

IP-адрес, если вы не укажете конкретный адрес передачи, оставив текстовое поле пустым. Так мы сейчас и поступим.

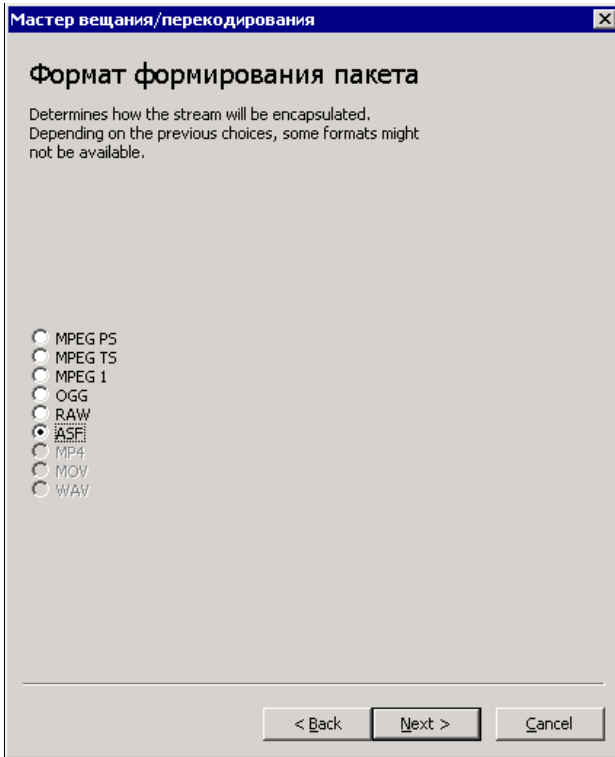
6. В следующем окне (рис. 18.6) выбираем формат передачи.

Выбор формата зависит от многих факторов: и от применяемого пользователями программного обеспечения, и от какой-либо договоренности с другими владельцами media-серверов... Давайте выберем **MPEG 1**.

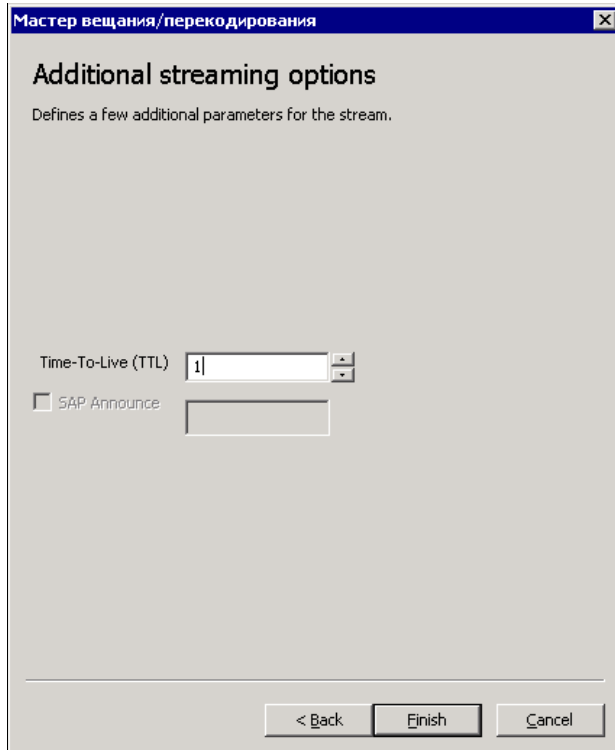
7. И в последнем окне (рис. 18.7) остается указать число маршрутизаторов, которые будут использоваться при трансляции. Если мы вещаем в локальную сеть — ставим единицу. Все! Нажимаем кнопку **Finish**.

Пошла передача! Но куда? Давайте пока остановим передачу, затем в меню **Вид** выберем команду **Список воспроизведения**, который мы тут же увидим перед собой (рис. 18.8).

В этом окне выберите команду **Управление | Сохранить список воспроизведения**. Укажите, под каким именем будет сохранен список, например List1, и сохраните его. Если вы делали все так, как описано, в вашем списке сохранятся два варианта работы программы — обычное воспроизведение файла и вещание в сеть. В любой момент через меню **Вид** вы сможете открыть сохраненный список воспроизведения.



**Рис. 18.6.** Окно **Мастер вещания/перекодирования**, раздел **Формат формирования пакета**



**Рис. 18.7.** Окно **Мастер вещания/перекодирования**, дополнительные опции передачи

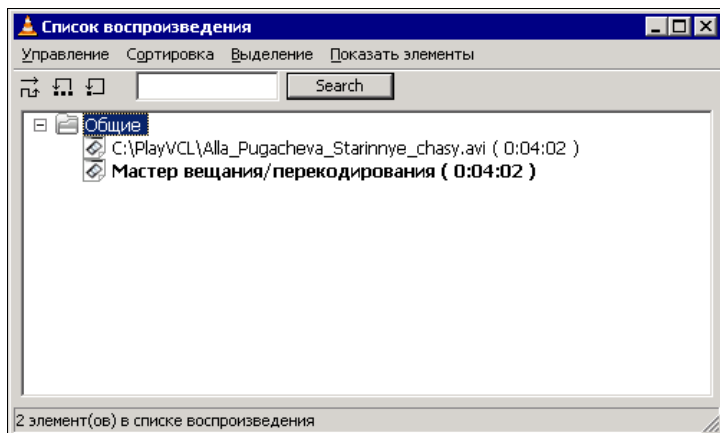


Рис. 18.8. Окно Список воспроизведения

## Прием

Теперь настроим программу на приемном конце.

### ПРИМЕЧАНИЕ

Чтобы упростить освоение, вы можете все операции выполнять на одном компьютере, запустив второй экземпляр программы!

1. Воспользуйтесь меню **Файл | Открыть**.

В открывшемся окне (рис. 18.9) на вкладке **Сеть** укажите протокол передачи и адрес источника и нажмите кнопку **ОК**. Не забудьте указать порт передачи.

В примере указан локальный адрес моего компьютера.

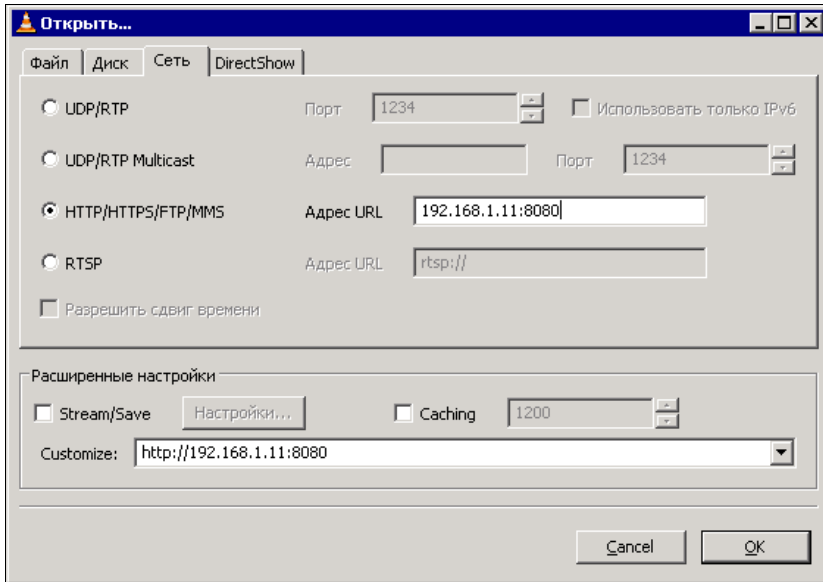
2. Теперь запускаем трансляцию в первом экземпляре программы и включаем воспроизведение во втором.

На передающем конце через меню **Вид | Список воспроизведения** можно указать циклическое воспроизведение элемента списка и включить его воспроизведение двойным щелчком по его строке.

Не пугайтесь, когда увидите на экране сообщение о какой-либо ошибке. Скорее всего, вы включили воспроизведение отсутствующего потока. Просто не успели включить передачу. Но на всякий случай проверьте еще разок настройки.

Программа достаточно проста в управлении, но имеет "свой характер". К нему надо немного приспособиться, и вы подружитесь с ней надолго. Пройдитесь по пунктам меню, посмотрите на возможности программы. Я уверен, что она очарует вас, как когда-то своим выступлением очаровала публику Алла Борисовна (рис. 18.10).

После освоения программы вы без труда сможете организовать не только вещание в своей сети, но и в Интернете, если у вас есть постоянное подключение к всемирной сети. Можно одновременно вести вещание по нескольким каналам, присвоив им отличающиеся друг от друга порты.

Рис. 18.9. Окно **Открыть...**, вкладка **Сеть**Рис. 18.10. Окно **VLC media player**: идет воспроизведение видеопотока



Интересно, что в Windows Server 2003 встроена возможность создания media-сервера. Можно просто добавить роль сервера **Сервер потоков мультимедиа**. Во время работы мастера создания **Пункта публикации** (собственно передающего сервера с определенной программой передач) автоматически может быть создана HTML-страница, в которую встроено окно медиаплеера. Эта роль сервера предполагает, что именно он содержит и Web-сервер. Вероятно, вам понравится эта возможность. Справка Windows довольно подробно освещает настройку сервера потоков мультимедиа и доступна на русском языке.

#### **ПРИМЕЧАНИЕ**

Если вы решили настраивать именно Windows Server 2003, да еще в терминальном режиме, то столкнетесь с тем, что не услышите звука при попытке отладить работу программ, несмотря на то, что в локальном режиме все работает. Чтобы включить звук, придется выполнить следующие действия: **Пуск | Выполнить | gpedit.msc | Computer configuration | Administrative templates | Windows components | Terminal services | Client/server data redirection | Allow audio redirection** и установить эту политику в состояние **Enabled**.

## **Ссылки**

Далее приведено несколько ссылок, по которым вы сможете найти дополнительную информацию об организации media-сервера. Вы не найдете в них рекомендаций по созданию такого сервера своими руками, но увидите серьезность подхода к этому вопросу различных фирм и цены на готовое оборудование, которое все чаще можно увидеть в продаже. Но, как сказано в известной рекламе: "Зачем платить больше?".

- [http://www.citforum.ru/hardware/articles/dig\\_home/;](http://www.citforum.ru/hardware/articles/dig_home/)
- [http://www.computerra.ru/think/ogorod/39258/;](http://www.computerra.ru/think/ogorod/39258/)
- <http://www.csu.ac.ru/osp/os/1996/04/source/71.html>.

## ГЛАВА 19



# Настраиваем почтовый сервер

Какая сеть без почтового сервера? Нет, конечно, возможно. Если вся сеть находится на одном столе, то почтовый сервер обычно не нужен. Но это обычно. Если вы системный администратор, пусть даже небольшой сети, то наверняка строите планы ее развития. А если даже один компьютер вашей сети оказался в другой комнате или, того хуже, на другом этаже, то следует задуматься о средствах коммуникации. Можно воспользоваться сервисами, имеющимися в Интернете, но для этого все клиенты сети должны иметь полноценный доступ в Интернет. А если это не так? Если по каким-либо причинам недопустимо предоставление доступа в Интернет многим пользователям сети (такое бывает!)? Тогда вам не обойтись без собственного почтового сервера.

## Почтовый сервер в Windows Server 2003

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. Чтобы иметь возможность получать почту на ваш почтовый сервер, необходимо зарегистрировать ваш домен в Интернете. 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.

Почтовый сервер начнем настраивать, воспользовавшись мастером настройки сервера, и на странице ролей выберем **Почтовый сервер**. На следующем шаге нам будет предложено выбрать метод проверки подлинности пользователей и имя домена электронной почты. Для проверки подлинности выберем **Локальные учет-**

**ные 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 применяться для внешней связи. Для примера настройки 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 необходима ручная настройка сервера. Для этого потребуется открывать отдельно SMTP- и POP3-серверы. SMTP открывается через **Администрирование | Диспетчер служб IIS** (рис. 19.1), а POP3 — через **Администрирование | Служба POP3** (рис. 19.2).

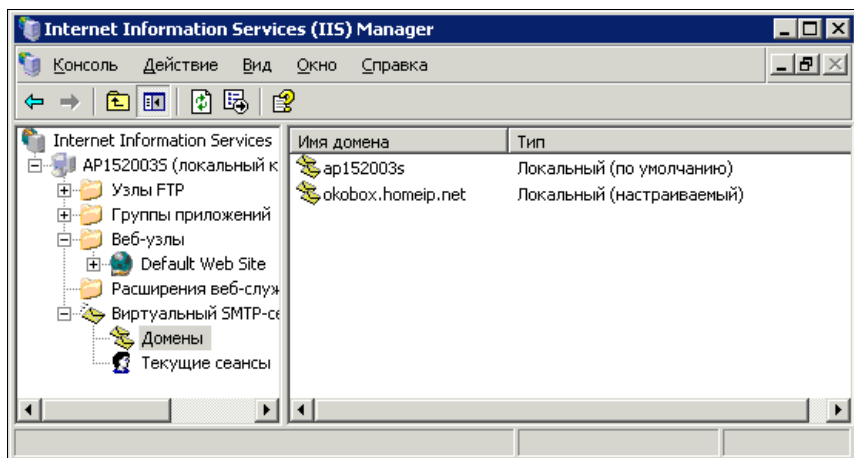


Рис. 19.1. Окно Internet Information Services (IIS) Manager (управление SMTP-сервером)

Для настройки порта SMTP-сервера откройте из окна **Internet Information Services (IIS) Manager** (см. рис. 19.1) окно свойств виртуального SMTP-сервера (из контекстного меню), а в этом окне выберите вкладку **Доставка**. В нижней части этой вкладки есть кнопки **Подключения** и **Дополнительно**. Нажав кнопку **Подключения**, вы откроете окно **Исходящие подключения** (рис. 19.3).

В этом окне при необходимости можно изменить значение порта для этого сервера. В примере стандартный порт 25 заменен значением 6525.

Если же на вкладке **Доставка** окна свойств виртуального SMTP-сервера нажать кнопку **Дополнительно**, то вы откроете окно **Дополнительная настройка доставки** (рис. 19.4), в котором можно указать **Имя подменяющего домена**, предназначенное для замены имени компьютера зарегистрированным именем почтового домена.

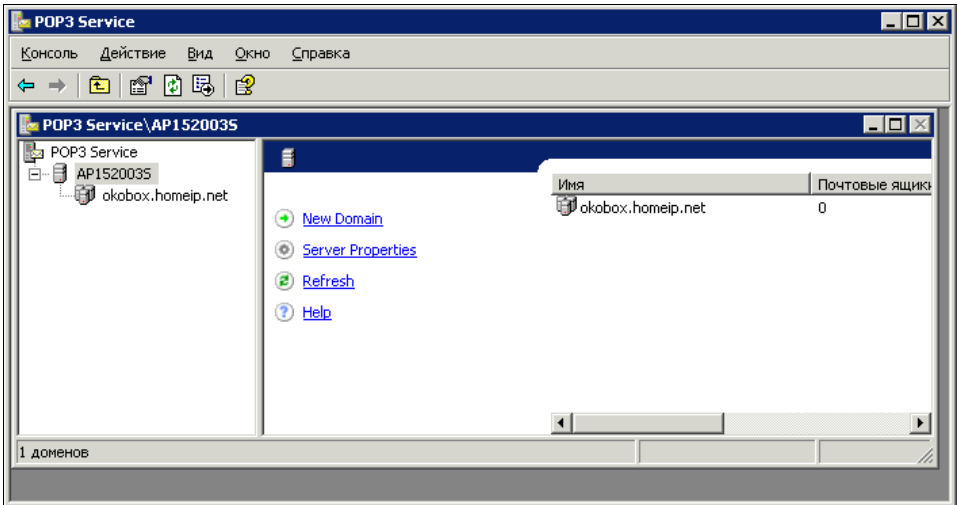


Рис. 19.2. Окно POP3 Service, раздел POP3 Service \ AP152003S

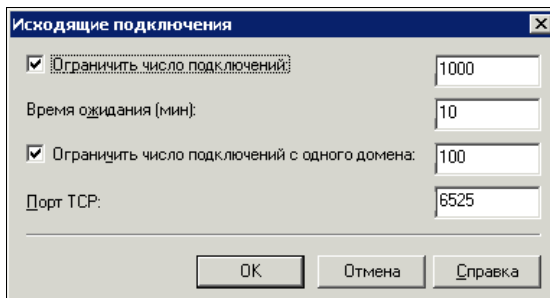


Рис. 19.3. Окно Исходящие подключения

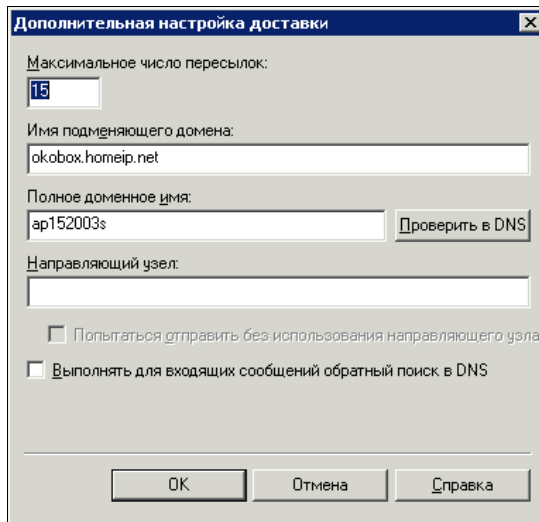


Рис. 19.4. Окно Дополнительная настройка доставки

Внеся изменения в настройки 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, этот процесс автоматизирован, и учетная запись может создаваться вместе с почтовым ящиком. Для создания почтового ящика достаточно в окне **POP3 Service** (раздел **POP3 Service \ AP152003S**) (см. рис. 19.2) выделить значок почтового домена в левой части окна, а в правой выбрать пункт меню **Add Mailbox** (Добавить почтовый ящик). При этом откроется окно **Добавление почтового ящика** (рис. 19.5). Внесите в соответствующие поля необходимые данные.

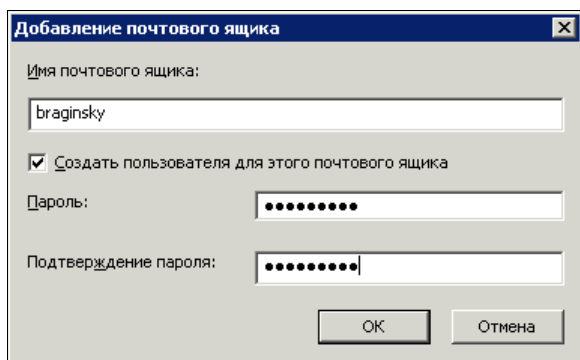


Рис. 19.5. Окно **Добавление почтового ящика**

Все. Почтовый ящик для учетной записи braginsky создан. Остается совсем немного. Следует открыть порт 110 для доступа к почтовому серверу из Интернета.

Если сервер находится внутри сети и не имеет прямого выхода в Интернет, он будет действовать только в пределах локальной сети, для которой он настроен. Для работы сервера в Интернете и обеспечения возможности обмена почтовыми сообщениями с пользователями Интернета необходимо, чтобы внешний интерфейс сервера был действительно внешним. Кроме того, подключение через интернет-провайдера "Стрим" (ADSL для физических лиц в Москве) затрудняет полноценно использовать почтовый сервер. Динамический IP-адрес невозможно прописать в маршрутизаторе Windows Server 2003.

## Управление почтовым сервером

SMTP-сервер обычно не требует специального управления. Все пользователи почтового сервера могут использовать SMTP-сервер для отправки сообщений. 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 ОС Windows Server 2003 есть и Web-интерфейс для управления почтовым сервером. Проверьте компоненты в окне **E-mail Services** (рис. 19.6), которые установлены в вашей системе. Если не установлен компонент **POP3 Service Web Administration**, то доустановите его.

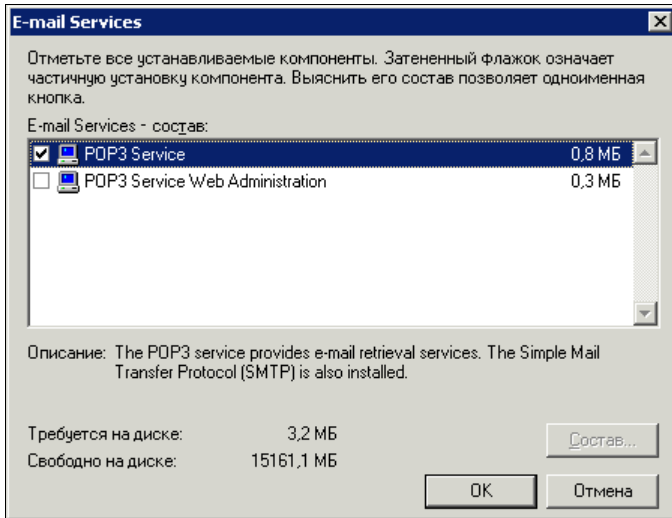


Рис. 19.6. Окно E-mail Services

После установки этого компонента вы получите возможность управлять почтовым сервером из Интернета или из своей сети через Web-интерфейс. Управление сервером через этот интерфейс несколько удобнее, чем через локальный интерфейс. Через этот интерфейс вы можете получить доступ к управлению не только программным почтовым сервером, но и по многим параметрам сервером 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 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 порту с номером 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 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. 19.7).

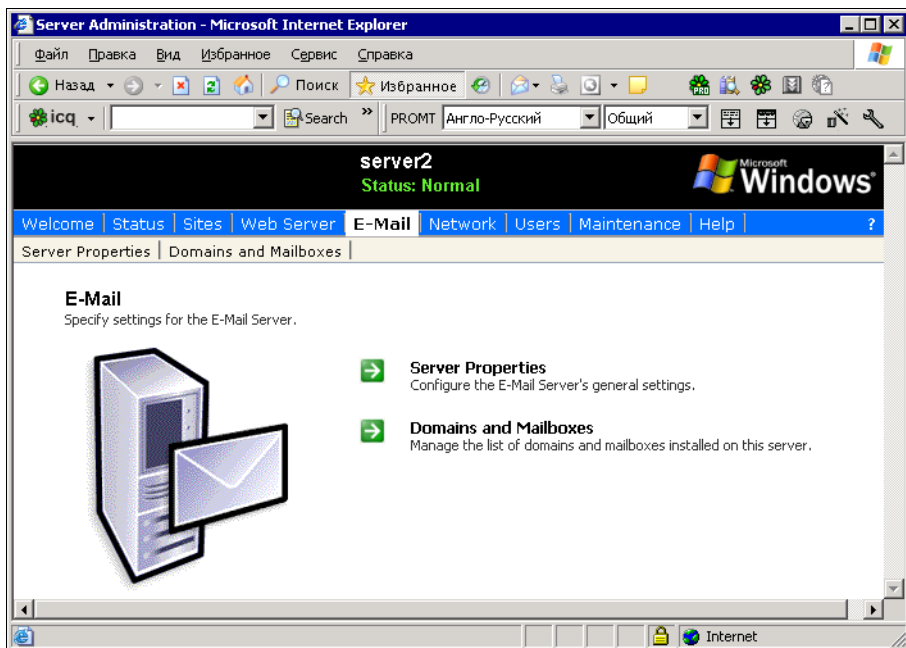


Рис. 19.7. Окно **Server Administration — Microsoft Internet Explorer**, вкладка **E-Mail**

На этой вкладке доступны два пункта меню: **Server Properties** (Свойства сервера) и **Domains and Mailboxes** (Домены и почтовые ящики). В большинстве случаев этих пунктов достаточно для повседневного администрирования почтового сервера. Выберем пункт **Server Properties** (рис. 19.8).

На открывшейся странице мы имеем возможность изменить каталог, содержащий почтовые ящики, поменять уровень протоколирования событий сервера и 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, такой сервер должен быть лучше защищен, чем обычный почтовый сервер. 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 появляется, 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.

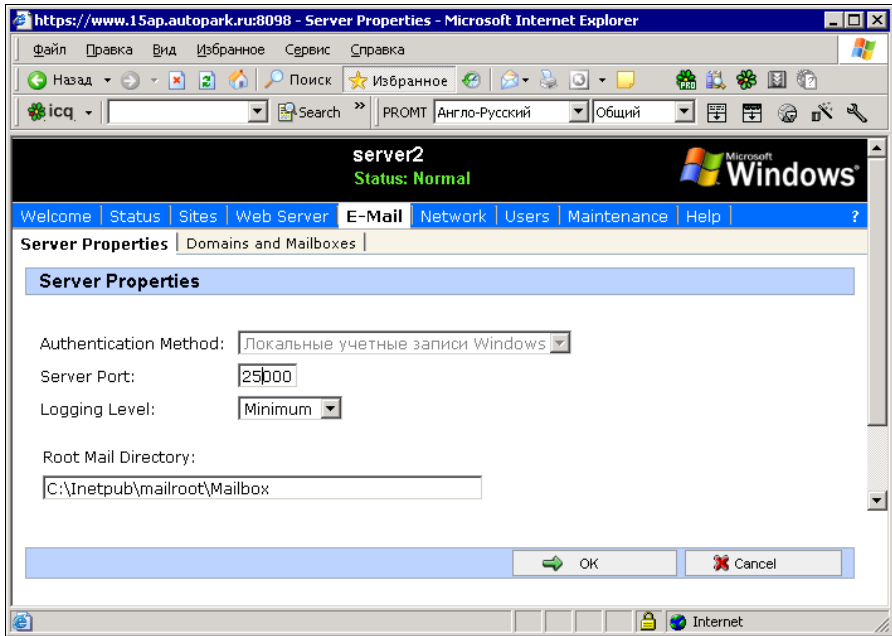


Рис. 19.8. Окно Internet Explorer, вкладка **Server Properties**

На странице **Domains and Mailboxes** (рис. 19.9) мы можем получить доступ к созданию/удалению и блокированию почтовых доменов, а также перейти на страницу управления самими почтовыми ящиками. Интерфейс этих страниц настолько понятен, что нет смысла подробно его рассматривать.

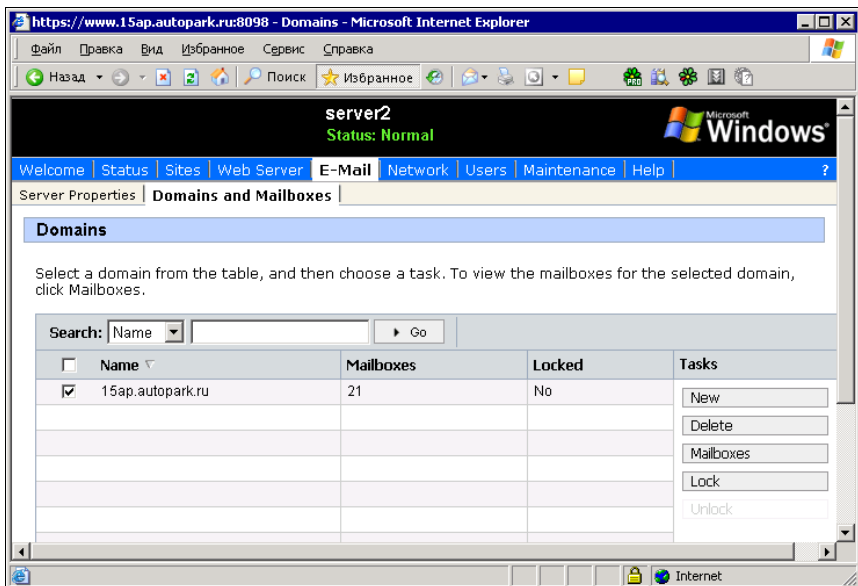


Рис. 19.9. Окно Internet Explorer, вкладка **Domains and Mailboxes**



Кроме управления доменами и почтовыми ящиками через Web-интерфейс мы можем получить доступ к управлению локальными учетными записями пользователей сервера, перейдя на вкладку **Users** (Пользователи) — рис. 19.10.

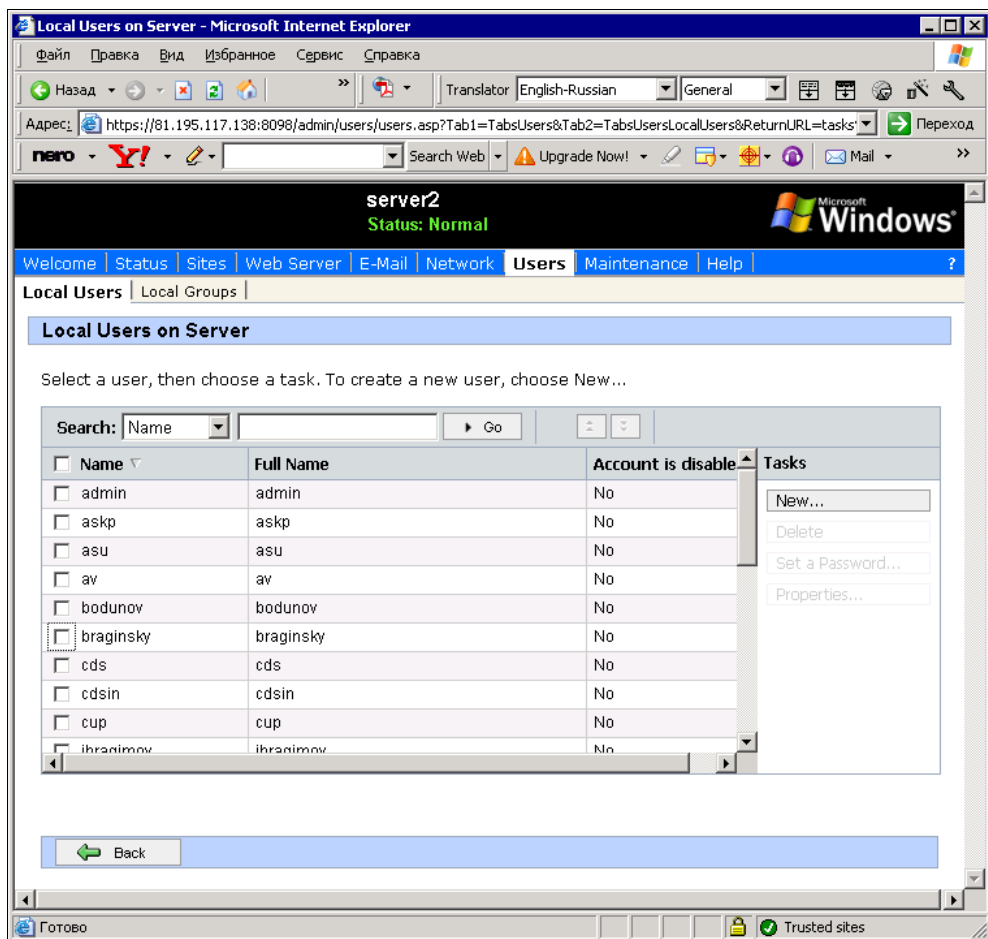


Рис. 19.10. Окно Internet Explorer, вкладка **Users**

Здесь можем создавать, удалять и модифицировать учетные записи. Если сервер работает только как почтовый, 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.

Рассмотрите самостоятельно остальные возможности этого интерфейса. Он позволяет управлять не только почтовым, но и всем вашим сервером. Возможно, что именно вас заинтересуют и другие его функции. Их достаточно, чтобы иметь возможность в удаленном режиме выполнять необходимые операции на вашем почтовом сервере. Если вы сталкивались ранее со средствами управления маршрутизатором,

рами и другими сетевыми устройствами по HTTP-протоколу, и вам понравился такой метод управления этими устройствами, то Web-интерфейс управления сервером вам обязательно понравится.

## Courier Mail Server

Сервер Courier Mail Server (CMS) обладает несколько более широкими возможностями, чем встроенный в Windows Server 2003. К тому же может управлять модным подключением к Интернету, если ваша сеть соединена с Интернетом через обычный модем. Этот же сервер может работать и внутри вашей сети.

Courier Mail Server (CMS) представляет собой сервер электронной почты, работающий под управлением операционной системы Windows 9x/ME/NT/2000/XP. Программа позволяет пользователям локальной сети обмениваться электронной почтой друг с другом, а так же получать и отправлять письма через Интернет.

Состав сервера CMS:

- SMTP-сервер;
- POP3-клиент;
- POP3-сервер;
- планировщик;
- IP-фильтр;
- сортировщик почты;
- SMTP-клиент;
- удаленный доступ.

Почтовый сервер CMS предназначен для организации обмена электронной почтой между компьютерами. Основными его функциями являются прием почтовых сообщений от клиентов и доставка их по адресам, указанным в сообщении. В качестве клиентов могут выступать как пользователи, так и другие почтовые серверы. Пользователи с помощью почтового клиента могут создавать сообщения, отправлять их на сервер и забирать почту из своих почтовых ящиков.

Для общения сервера и клиента используются почтовые протоколы:

- Simple Mail Transfer Protocol (*SMTP*) — для передачи сообщений на сервер;
- Post Office Protocol v.3 (*POP3*) — для приема сообщений из почтового ящика.

Используются стандартные порты: для SMTP — порт 25, для POP3 — порт 110.

Для блокирования нежелательных подключений в CMS имеется IP-фильтр.

Сообщения, полученные SMTP-сервером, помещаются в очередь входящих сообщений. Сообщения последовательно обрабатываются и направляются в почтовые ящики (для локальных получателей) и в очередь исходящих сообщений (для внешних получателей).

Получатель считается локальным, если домен в его адресе электронной почты (строка после @) совпадает с локальным доменом сервера.

Накопившиеся исходящие сообщения SMTP-клиент периодически отправляет в Интернет на другой почтовый сервер, который берет на себя ответственность за дальнейшую доставку сообщений.

Сеансы обмена почтой с Интернетом могут выполняться в автоматическом режиме по расписанию с помощью планировщика. При этом подключение к Интернету может осуществляться как по локальной сети, так и по модему (удаленный доступ).

POP3-клиент дает возможность забирать почту из почтовых ящиков, находящихся на других серверах, и доставлять локальным или внешним получателям.

Сортировщик почты позволяет на основе задаваемых правил перенаправлять определенным получателям сообщения, принятые из внешних ящиков.

## Системные требования

- Операционная система: Windows 9x/ME/NT/2000/XP.
- Свободное место на жестком диске: 1 Мбайт плюс несколько мегабайтов для хранения почты пользователей.
- Установленный сетевой протокол TCP/IP.
- Если предполагается обмен электронной почтой с Интернетом, то необходимо непосредственное соединение компьютера с глобальной сетью через сетевую плату, модем или аналогичное устройство.
- При подключении к Интернету с помощью модема необходим установленный компонент Windows — **Удаленный доступ к сети**.
- При наличии локальной сети на всех компьютерах для работы с электронной почтой через CMS должен быть установлен сетевой протокол TCP/IP и клиентские программы, способные работать с почтовыми серверами по протоколам SMTP и POP3 (Outlook Express, The Bat! или аналогичные).

## Установка и удаление

Почтовый сервер CMS поставляется в виде zip-архива, содержащего исполняемый файл и документацию. Для установки сервера создайте папку, в которой он будет функционировать, извлеките файлы из архива и поместите в эту папку, а затем запустите приложение CourierMS.exe. При первом запуске сервер внутри своей папки автоматически создаст необходимые для его работы подкаталоги и файлы. За пределами своей папки сервер не производит никаких изменений. Системный реестр Windows меняется только при регистрации в качестве службы.

Если запуск произошел нормально, то на экране появится главное окно сервера, а в системном лотке (system tray) рядом с часами — его значок.

Для того чтобы сервер запускался автоматически при запуске Windows, его можно зарегистрировать как службу.

Для удаления сервера остановите его, после чего удалите папку, в которой он находится, а также папки почтовых ящиков, очередей или журналов, если вы разместили их за пределами рабочей папки сервера. Если сервер запускался как служба, то перед его удалением надо отменить запуск в качестве службы.

## Работа в качестве службы

Помимо ручного запуска почтовый сервер CMS может автоматически запускаться как служба (сервис) Windows NT/2000/XP, а также Windows 9x/ME.

Для обеспечения запуска в качестве службы запустите CMS и в меню **Настройки** выберите команду **Запускаться службой**. При этом произойдет регистрация службы Courier Mail Server в системе.

Теперь при загрузке Windows почтовый сервер CMS будет автоматически запускаться как служба до входа пользователя в сеть. При завершении сеанса пользователя сервер будет продолжать работу.

Можно запустить службу и вручную. Для этого в Windows NT/2000/XP используйте диспетчер служб (Service Control Manager), а в Windows 9x/ME запустите CourierMS.exe с ключом /service из командной строки.

Для прекращения запуска в качестве службы в меню **Настройки** повторно выберите команду **Запускаться службой**.

## Главное окно

Главное окно сервера (рис. 19.11) Courier Mail Server содержит 4 панели:

- панель компонентов (вверху слева) содержит список компонентов сервера;
- панель подключений (вверху справа) содержит список текущих клиентских подключений к серверу, а также исходящих подключений к внешним SMTP- и POP3-серверам;
- панель статистики (внизу слева) отображает количество имеющихся учетных записей и состояние SMTP/POP3-серверов. Она также служит для запуска/останова серверов с помощью контекстного меню;
- панель журнала (внизу справа) отображает журнал работы сервера.

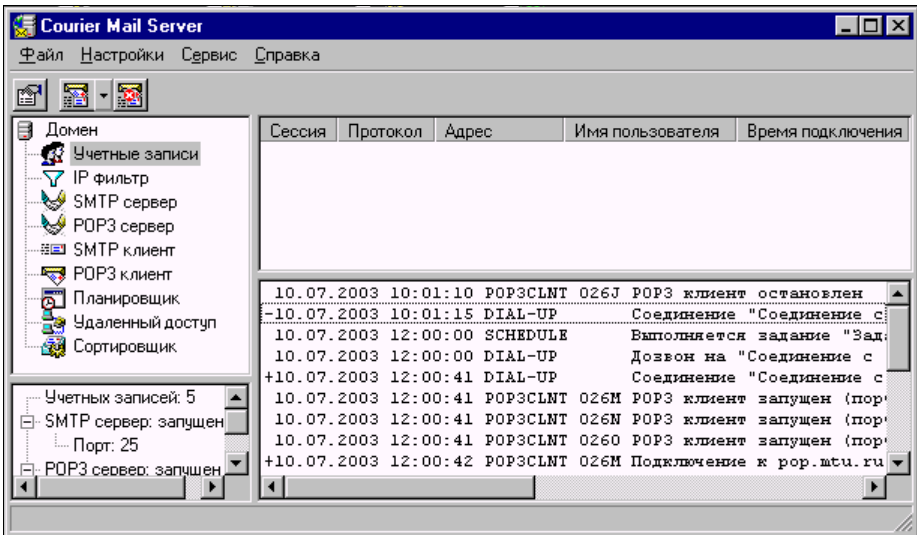


Рис. 19.11. Главное окно почтового сервера Courier Mail Server

Для настройки параметров главного окна в меню **Настройки** выберите команду **Интерфейс**.

Имеются следующие параметры:

- ❑ **Показывать главное окно при запуске** — если флажок установлен, то главное окно будет показываться при запуске сервера CMS;
- ❑ **Отображать значок в системном лотке** — назначение следует из названия;
- ❑ **Запоминать состояние главного окна** — если флажок установлен, то при выходе из сервера CMS будут запомнены размер и положение главного окна, а также размеры панелей;
- ❑ **Пароль главного окна** — пароль, запрашиваемый перед открытием главного окна. Если пароль пустой, запрашиваться он не будет;
- ❑ **Клавиша быстрого вызова** — комбинация клавиш для быстрого вызова главного окна;
- ❑ **Количество строк экранного журнала** — максимальное количество строк, отображаемых одновременно в экранном журнале.

## Настройка сервера

Настройка сервера заключается в последовательной настройке всех его компонентов. Для настройки свойств компонента выберите его в дереве компонентов, после чего в меню **Файл** или в контекстном меню выберите команду **Свойства**. Для настройки свойств журнала в меню **Настройки** выберите команду **Журнал**. В каждом окне настройки можно вызвать контекстную справку после нажатия клавиши <F1>.

### Домен

Вкладка **Общие** (рис. 19.12) содержит следующие опции.

- ❑ **Имя** — имя локального домена, например, mycompany.ru.

Теперь, если SMTP-сервер CMS получит сообщение, адресованное, например, **user@mycompany.ru**, он поместит его в почтовый ящик user, т. к. получатель принадлежит локальному домену. Если адрес получателя будет **user@yourcompany.ru**, то письмо будет отправлено в Интернет, т. к. домен **yourcompany.ru** не является локальным для этого сервера.

Получатель, у которого не указан домен, считается локальным, т. е. если SMTP-сервер примет сообщение с адресом получателя user, он поместит его в локальный почтовый ящик user, как и в случае полного адреса **user@mycompany.ru**.

- ❑ **Администратор** — почтовый ящик администратора.

Согласно стандарту Интернета любой почтовый сервер должен иметь почтовый ящик postmaster, служащий для приема сообщений о проблемах, связанных с работой сервера. Если сервер получит сообщение, адресованное **postmaster@mycompany.ru** или просто postmaster, оно будет доставлено администратору.

- ❑ **Автоматически разрывать соединения при останове** — если этот флажок установлен, то при останове сервера клиентские соединения будут разорваны автоматически, без подтверждения администратора. Если почтовый сервер CMS

запущен как служба, то соединения разрываются автоматически, независимо от состояния данного флажка.

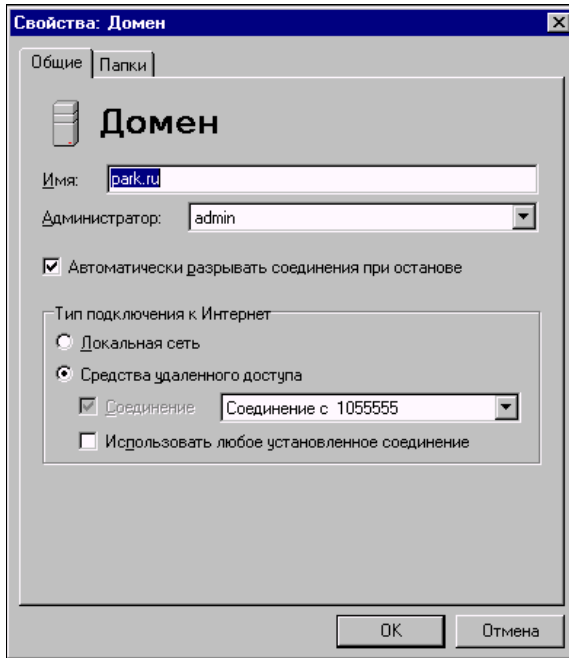


Рис. 19.12. Окно **Свойства: Домен**, вкладка **Общие**

#### □ Группа **Тип подключения к Интернет**:

- **Локальная сеть** — для подключения будет использоваться локальная сеть;
- **Средства удаленного доступа** — для подключения будут использоваться средства удаленного доступа;
- **Соединение** — установите флажок для подключения через указанное соединение;
- **Использовать любое установленное соединение** — установите этот флажок для подключения через любое уже установленное соединение.

На вкладке **Папки** можно настроить папки почтовых ящиков, очередей входящих и исходящих сообщений, файлов журнала.

## Учетные записи

Редактор учетных записей (рис. 19.13) предназначен для ведения списка учетных записей пользователей сервера. При создании учетной записи создается также соответствующая папка почтового ящика. При удалении учетной записи папка почтового ящика удаляется автоматически со всем содержимым.

При первом запуске сервера автоматически создается учетная запись postmaster (пароль — 1).

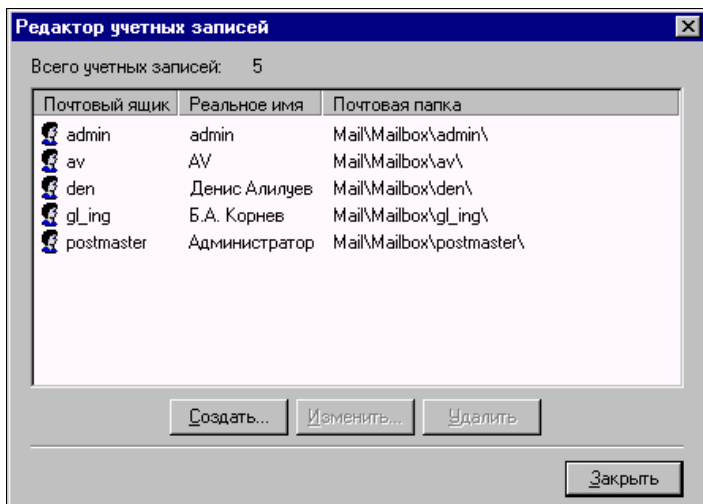


Рис. 19.13. Редактор учетных записей

Каждая учетная запись (рис. 19.14) имеет следующие параметры:

- ❑ **Реальное имя** — имя владельца почтового ящика;
- ❑ **Имя почтового ящика** — наименование почтового ящика. Оно же является и именем пользователя при подключении к серверу. В имени ящика не используйте русские буквы и специальные символы, т. к. некоторые почтовые программы работают с ними некорректно. Если имя ящика user, локальный домен mydomain.ru, то адрес электронной почты данного пользователя **user@mydomain.ru**;
- ❑ **Пароль** — пароль для подключения к серверу;
- ❑ **Доступ POP3 клиентам разрешен** — если этот флажок установлен, то доступ к почтовому ящику разрешен;
- ❑ **Почтовая папка** — папка, в которой будут храниться сообщения данного ящика;
- ❑ **Внешний адрес e-mail** — адрес электронной почты, которым будет заменяться локальный адрес отправителя при отправке сообщений в Интернет. Если поле пусто, то замена производиться не будет. Функция замены необходима, например, в том случае, если локальный домен официально не зарегистрирован. Предположим, что локальный домен называется **mycompany.ru** и не зарегистрирован. Локальный пользователь с адресом **user@mycompany.ru** отправил сообщение в Интернет. Возможны два варианта:
  - SMTP-сервер, через который производится отправка, откажется принимать такое сообщение, т. к. домен **mycompany.ru** ему неизвестен;
  - сообщение будет принято и доставлено получателю, но ответ на него не дойдет до адресата, т. к. адрес получателя будет **user@mycompany.ru**. Поскольку этот домен не зарегистрирован, то, соответственно, неизвестен почтовым серверам Интернета.

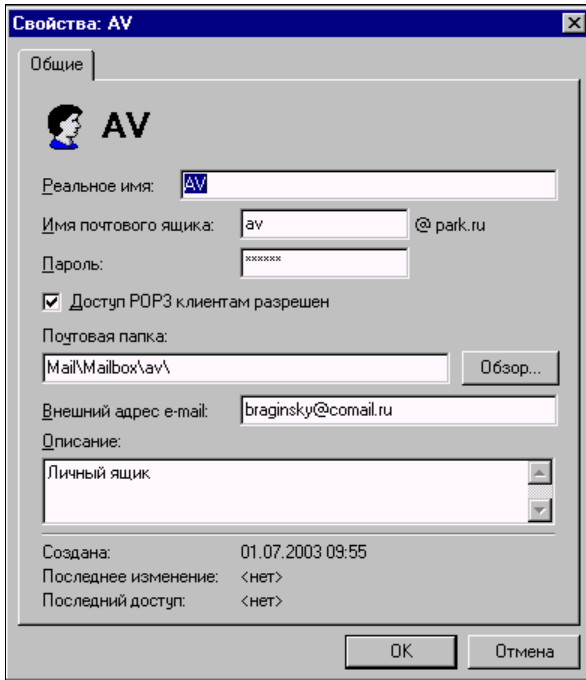


Рис. 19.14. Редактор учетных записей: свойства записи

Таким образом, в данной ситуации необходимо использовать замену адреса. Если в поле ввести реально существующий адрес электронной почты (например, почтовый ящик, размещенный у провайдера), то сервер, принимающий сообщение, будет считать, что оно отправлено с этого адреса. Ответ на сообщение будет также доставлен на данный адрес;

- ❑ **Описание** — любой текстовый комментарий;
- ❑ **Создана** — дата и время создания учетной записи;
- ❑ **Последнее изменение** — дата и время последней модификации;
- ❑ **Последний доступ** — дата и время последнего подключения к почтовому ящику.

## IP-фильтр

Окно свойств IP-фильтра с правилами фильтрации приведено на рис. 19.15. Доступны следующие настройки:

- ❑ **Разрешить все подключения** — при выборе этого параметра фильтрация подключений производиться не будет;
- ❑ **Фильтровать на основе списка правил** — для фильтрации будет использоваться список правил фильтра. В каждом правиле можно указывать либо конкретный IP-адрес, либо диапазон, при этом фильтрации подвергаются все адреса, входящие в диапазон. Правило распространяется на протоколы, отмеченные флажками. Подключения, не соответствующие ни одному правилу, блокируют-



ся. Правила при фильтрации просматриваются сверху вниз, поэтому более общие правила должны находиться ниже более конкретных;

- группа **Для адресов, не указанных в списке** используется для задания прав подключения с адресов, не попавших в список.

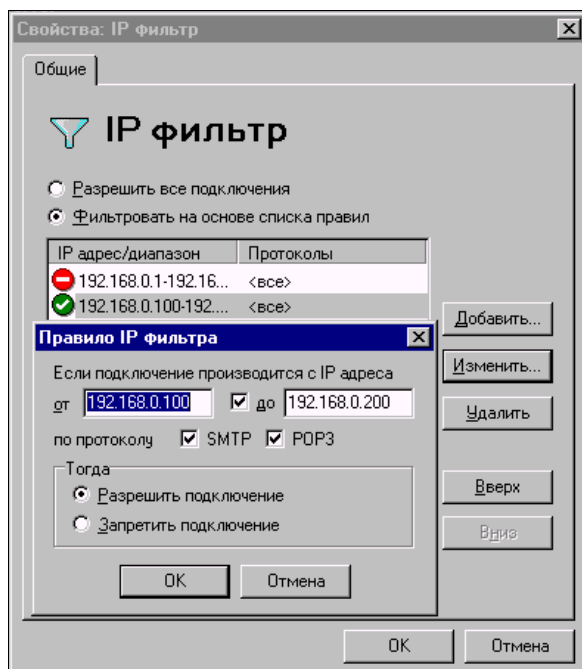


Рис. 19.15. Окна **Свойства: IP фильтр** и **Правило IP фильтра**

Рассмотрим пример. Требуется разрешить подключение к серверу с локального компьютера (127.0.0.1) и из локальной сети (192.168.10.xxx). С адреса 192.168.10.12 запретить подключение к SMTP-серверу. С остальных адресов запретить любые подключения.

Выбираем переключатель **Фильтровать на основе списка правил** и создаем по порядку три правила:

1. 127.0.0.1, SMTP и POP3, разрешить.
2. 192.168.10.12, SMTP, запретить.
3. 192.168.10.1—192.168.10.255, SMTP и POP3, разрешить.

## SMTP/POP3-серверы

Окна свойств SMTP- и POP3-серверов показаны на рис. 19.16 и 19.17.

- **Порт** — номер порта, на котором будет работать сервер. Стандартные значения: для SMTP — 25, для POP3 — 110. При изменении порта сервер начнет работать на нем только после перезапуска (выполняется на панели статистики через контекстное меню).

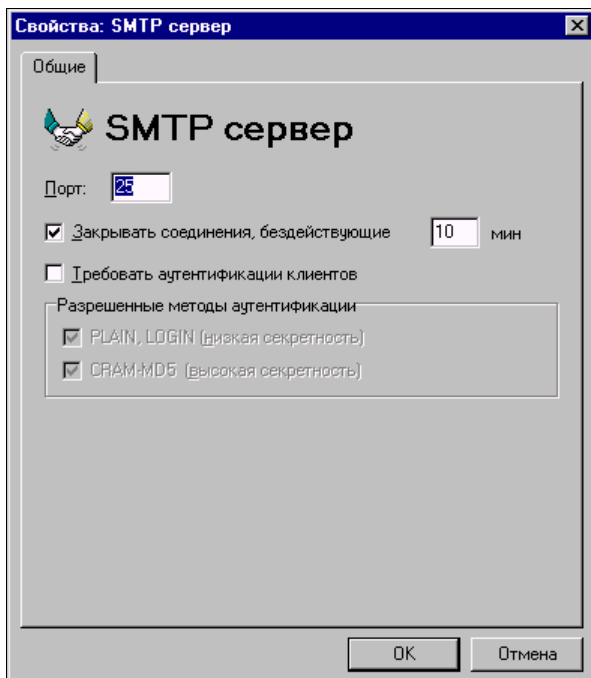


Рис. 19.16. Окно Свойства: SMTP сервер

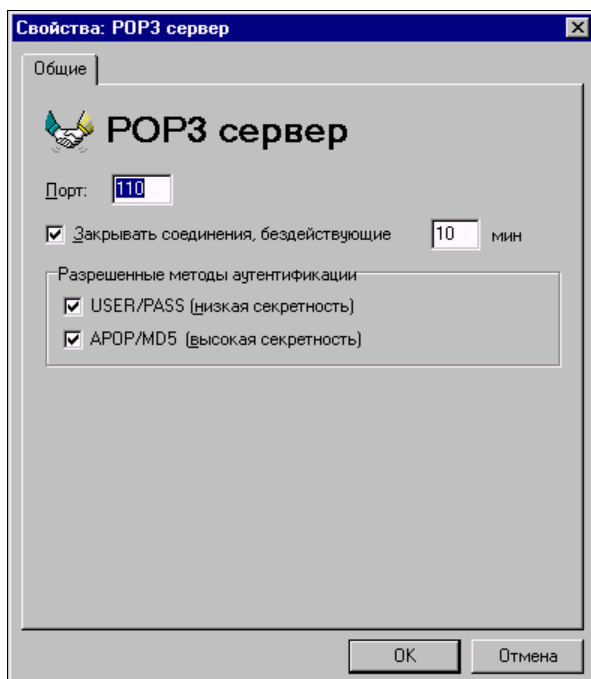


Рис. 19.17. Окно Свойства: POP3 сервер

- ❑ **Закрывать соединения, бездействующие NN мин** — если в течение указанного времени (*NN* мин) клиент не отправил на сервер никаких данных, соединение принудительно разрывается. Стандартное значение — 10 минут, но для локальной сети можно указать меньшее значение, т. к. поддержка бездействующих соединений отнимает ресурсы сервера.
- ❑ В группе **Разрешенные методы аутентификации** перечислены методы аутентификации, поддерживаемые сервером. Методы, отмеченные флажками, разрешены к использованию. В SMTP-сервере обязательная аутентификация клиентов может быть отключена с помощью флажка **Требовать аутентификации клиентов**.

## SMTP-клиент

Для связи с SMTP-сервером провайдера существует SMTP-клиент (рис. 19.18).

- ❑ **SMTP сервер** — имя или IP-адрес SMTP-сервера, через который будет отправляться почта в Интернет. Обычно указывается почтовый сервер провайдера.
- ❑ **Порт** — номер порта подключения к серверу. Стандартное значение — 25.
- ❑ **Тайм-аут (минут)** — если в течение указанного в этом поле времени сервер не вернул никаких данных, соединение принудительно разрывается. Стандартное значение — 5 минут.
- ❑ **В EHLO вместо имени локального домена использовать** — если этот флажок установлен, то при подключении к серверу в команде EHLO будет указана заданная строка, иначе — имя локального домена.

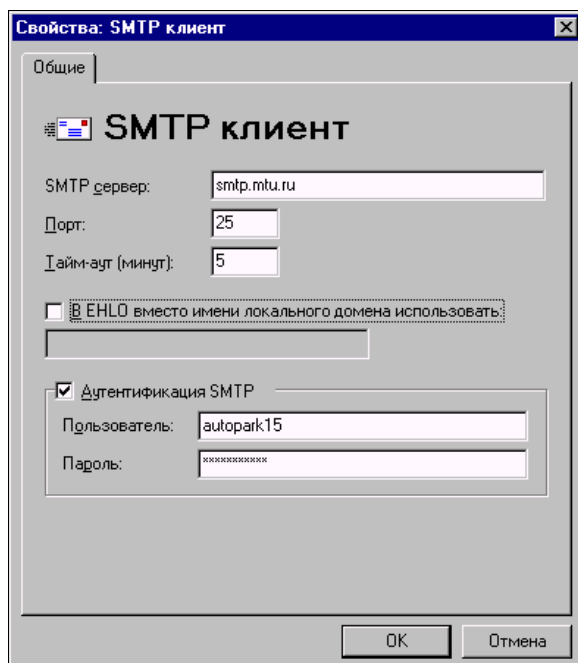


Рис. 19.18. Окно Свойства: SMTP клиент

- ❑ Группа **Аутентификация SMTP** используется при необходимости аутентификации на SMTP-сервере.

## POP3-клиент

Для связи с POP3-сервером провайдера служит POP3-клиент (рис. 19.19). POP3-клиент содержит список внешних почтовых ящиков (учетных записей), из которых необходимо забирать почту.

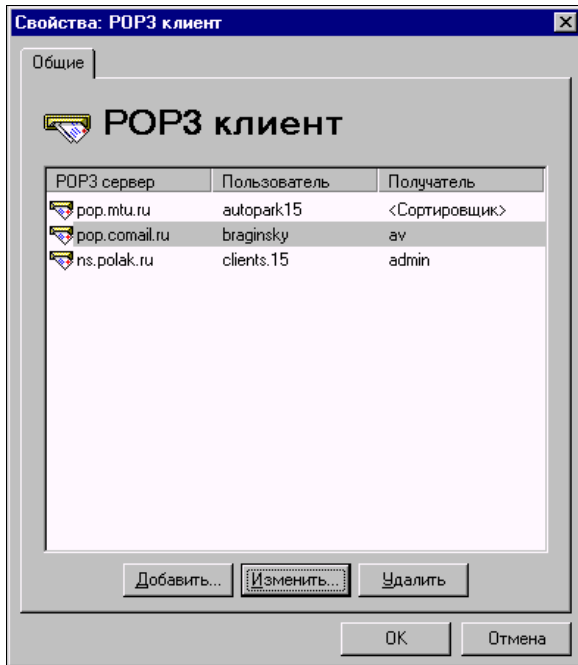


Рис. 19.19. Окно **Свойства: POP3 клиент**

### Параметры внешней учетной записи

На рис. 19.20 показано окно для ввода параметров внешней учетной записи.

- ❑ **Получать сообщения этой учетной записи** — если этот флажок установлен, почта из данного ящика будет забираться.
- ❑ **POP3 сервер** — имя (или IP-адрес) POP3-сервера, на котором расположен внешний почтовый ящик.
- ❑ **Порт** — номер порта подключения к серверу. Стандартное значение — 110.
- ❑ **Пользователь** — имя пользователя почтового ящика. Обычно совпадает с именем почтового ящика (слева от @ в адресе электронной почты).
- ❑ **Пароль** — пароль почтового ящика.
- ❑ **Получатель** — адрес, на который будут доставляться принятые письма. Из списка можно выбрать любой локальный почтовый ящик, <Домен> или <Сортировщик>.

### ПРИМЕЧАНИЕ

Можно не выбирать значение из списка, а ввести в список нужные адреса (в том числе и внешние), перечисленные через запятую. Сообщения будут перенаправлены на эти адреса. При указании в качестве получателя <Домен> адрес получателя для локального домена ищется сначала в полях **Received**, а в случае неудачи — в полях **To** и **Cc**.

- ❑ **Использовать аутентификацию APOP/MD5** — если этот флажок установлен, то при подключении к серверу вместо стандартной аутентификации USER/PASS будет использоваться безопасный метод APOP/MD5. Некоторые POP3-серверы могут не поддерживать этот метод аутентификации.

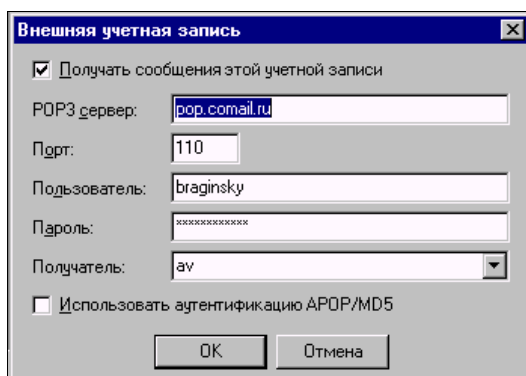


Рис. 19.20. Окно Внешняя учетная запись

## Планировщик

Планировщик (рис. 19.21) управляет получением и отправкой сообщений в соответствии с расписанием.

Если установлен флажок **Выполнять задания планировщика**, задания планировщика будут выполняться. Список содержит задания планировщика.

### Параметры задания

Параметры для каждого задания (рис. 19.22) устанавливаются индивидуально и очень гибко.

Вкладка **Общие** содержит следующие настройки.

- ❑ **Имя** — наименование задания.
- ❑ **Задание** — действие, которое будет выполнено.
- ❑ **Группа Время выполнения:**
  - **однократно** — задание выполнится один раз, время выполнения указывается в поле **в** (в формате ЧЧ:ММ);
  - **периодически** — задание будет выполняться периодически, период указывается в поле **каждые** (в формате ЧЧ:ММ). Если установлен флажок **круглосуточно**, то задание будет выполняться с 00:00 до 23:59, иначе будут использоваться поля **с** и **до**;

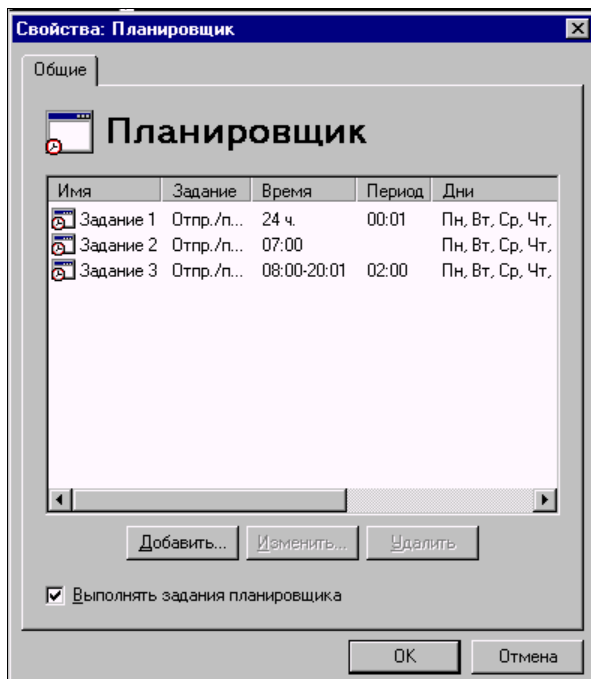


Рис. 19.21. Окно Свойства: Планировщик

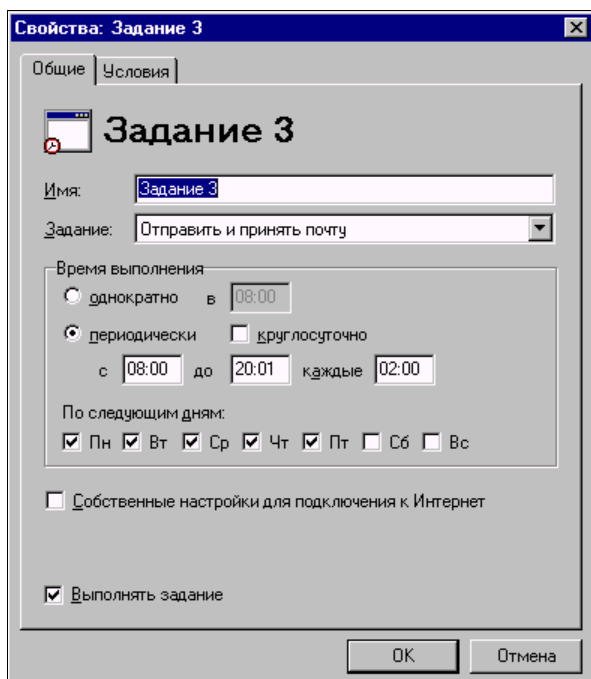


Рис. 19.22. Окно Свойства: Задание N

- **По следующим дням** — эти флажки устанавливают у тех дней недели, в которые задание должно выполняться.
- Собственные настройки для подключения к Интернет** — если этот флажок установлен, то на дополнительной вкладке **Подключение** можно задать параметры подключения для данного задания. Если флажок сброшен, то для подключения используются настройки домена.
- Выполнять задание** — если этот флажок установлен, то задание будет выполняться.

Вкладка **Условия** содержит группу **Условия выполнения**. Если условия с установленными флажками — активные, то условия проверяются в тот момент, когда по времени задание должно выполниться. Если хотя бы одно из активных условий выполнено, то задание выполняется:

- если число исходящих сообщений** — условие выполнено, если количество сообщений в очереди исходящих не меньше указанного значения;
- если объем исходящих сообщений** — условие выполнено, если совокупный объем всех сообщений в очереди исходящих не меньше указанного значения;
- если сообщения ожидают отправки** — условие выполнено, если самое старое сообщение в очереди исходящих находится там не меньше указанного времени;
- если существует файл** — условие выполнено, если существует указанный файл. В имени файла можно использовать символы маски "?" и "\*" (например, Mail\Mailbox\scheduler\\*.msg);
- удалить файл после запуска задания** — если этот флажок установлен, то после выполнения задания файл удаляется.

Вкладка **Подключение** содержит параметры подключения к Интернету для данного задания.

## Удаленный доступ

В окне **Свойства: Удаленный доступ** (рис. 19.23) выводится список соединений удаленного доступа Windows.

Для каждого соединения можно установить независимые от настроек Windows параметры (рис. 19.24).

- Группа **Телефоны**:
  - **Основной** — основной номер телефона соединения;
  - **Дополнительные** — список дополнительных номеров телефонов;
  - **Префикс выхода на линию** — назначение следует из названия;
  - **Набор с вариантами тоновый, импульсный** — тип набора номера.
- Число попыток соединения** — число попыток установить соединение.
- Пауза между попытками, сек** — задержка в секундах перед следующей попыткой.

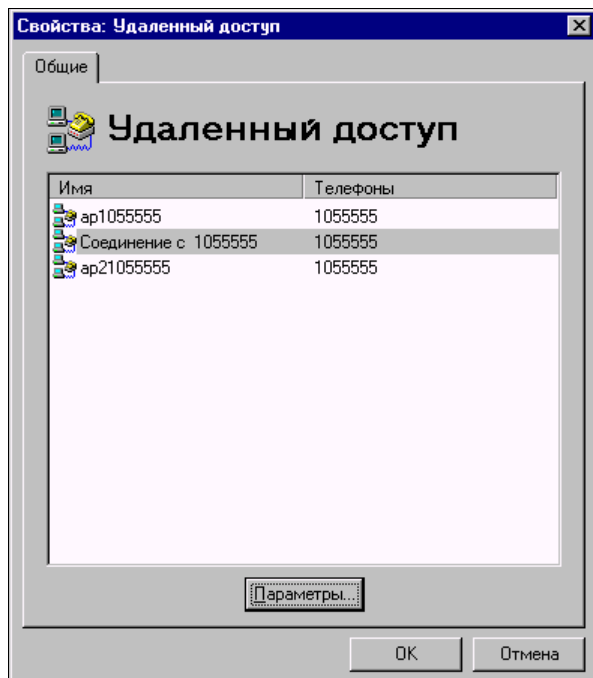


Рис. 19.23. Окно Свойства: Удаленный доступ

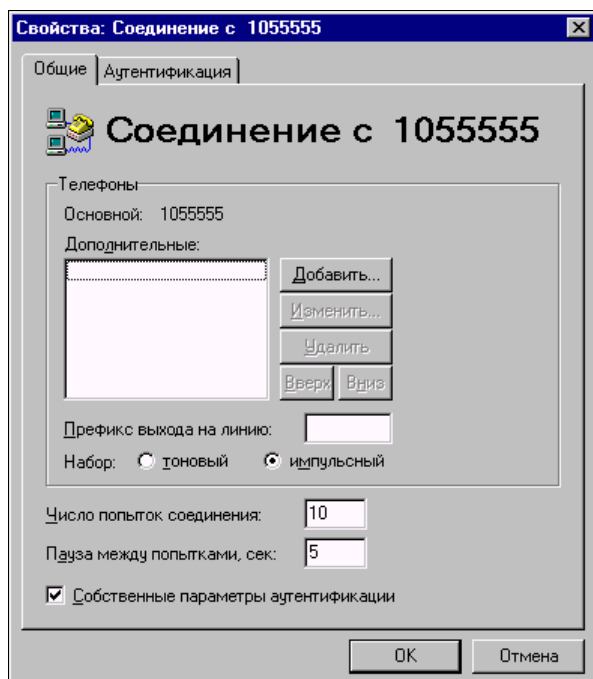


Рис. 19.24. Окно Свойства: Соединение с 1055555



При соединении с провайдером сначала используется основной номер, а затем дополнительные номера по порядку. Если попытка соединения не удалась, выдерживается пауза и производится попытка соединения последующему номеру. При достижении конца списка номеров дозвон продолжается с основного номера и т. д. до исчерпания попыток.

- ❑ **Собственные параметры аутентификации** — если этот флажок установлен, то на дополнительной вкладке **Аутентификация** можно задать параметры аутентификации для данного соединения. Если флажок сброшен, то для аутентификации используются данные Windows.

Вкладка **Аутентификация** содержит параметры аутентификации на удаленном компьютере после установления связи. Если провайдер не требует указания домена при подключении, то поле **Домен** можно оставить пустым.

## Сортировщик

Сортировщик почты (рис. 19.25) на основе задаваемых правил перенаправляет сообщения, полученные из внешних почтовых ящиков определенным получателям. Сортировщик содержит список правил, на основе которых и происходит сортировка сообщений.

- ❑ **Доставлять неотсортированную почту по адресам** — список адресов, перечисленных через запятую, по которым будут доставляться сообщения, не удовлетворившие ни одному правилу. Если не указан ни один адрес, сообщения будут доставляться администратору.

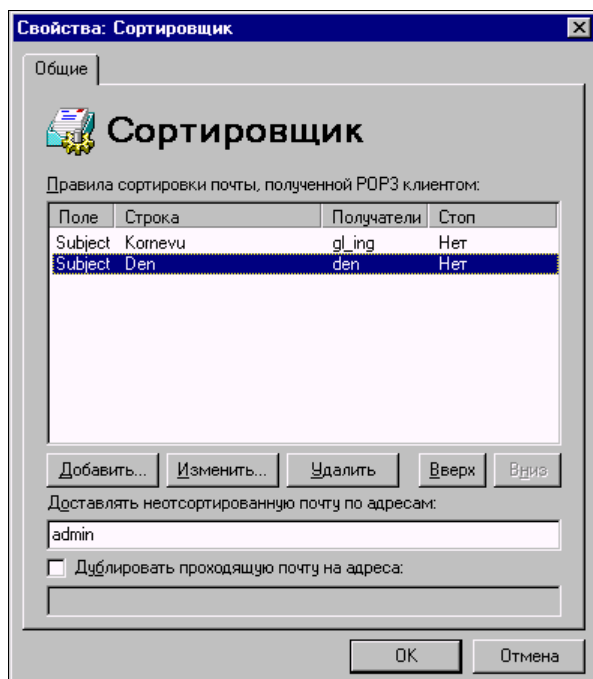


Рис. 19.25. Окно **Свойства: Сортировщик**

- Дублировать проходящую почту на адреса** — список адресов, перечисленных через запятую, на которые будут направляться копии всех сообщений, получаемых SMTP-сервером.

### Параметры правил сортировки

Правила сортировки задаются в отдельном окне (рис. 19.26).

- Если поле заголовка** — анализируемое поле заголовка сообщения. Можно выбрать значение из списка или ввести вручную, если оно отсутствует в списке.
- Содержит текст** — текст для поиска в значении поля.
- Тогда доставить сообщение по следующим адресам** — список получателей, которым будет доставлено данное сообщение, если правило выполняется. Можно указывать как локальных, так и внешних получателей.
- И прекратить дальнейшую обработку правил** — если данное правило выполнилось, остальные правила не будут проверяться для данного сообщения.

Для каждого сообщения последовательно проверяются все правила до тех пор, пока не будет достигнут конец списка или не выполнится правило, у которого установлен флажок прекращения дальнейшей обработки. Правило выполняется, если в заголовке сообщения имеется указанное поле, и оно содержит введенный текст. В этом случае происходит доставка сообщения указанным получателям.

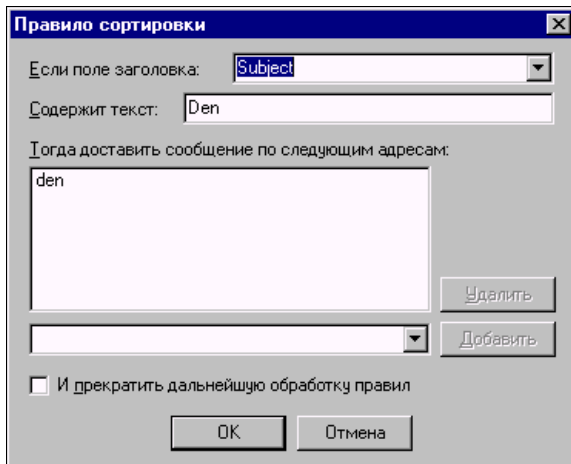


Рис. 19.26. Окно Правило сортировки

## Журнал

Группа **Режим сохранения в файл:**

- Не сохранять** — журнал не будет сохраняться в файл (только отображение на экране);
- Отдельный файл для каждой даты** — журнал за каждую дату сохраняется в файл с именем вида ГГГГДДММ.log;

- ❑ **Отдельный файл для каждого дня недели** — журнал за каждый день недели сохраняется в файл с названием дня недели (Monday.log, Tuesday.log и т. д.);
- ❑ **Один общий файл** — журнал записывается в один файл с именем, указанным в поле **Имя файла**. В поле нужно указывать только имя файла, без папки. Папка журнала настраивается в свойствах домена;
- ❑ **Ограничить размер файла NN Кб** — если флажок установлен, то при достижении файлом журнала указанного размера он закрывается, и его расширение меняется на old. Если файл с расширением old существует, он удаляется. Журнал продолжает сохраняться во вновь созданный файл с расширением log.

Группа **Уровень подробности**:

- ❑ **Низкий** — записываются сообщения об ошибках и наиболее важные системные сообщения;
- ❑ **Средний** — кроме сообщений низкого уровня записываются сообщения о запуске/остановке компонентов, подключении/отключении клиентов, работе сортировщика;
- ❑ **Высокий** — записываются сообщения обо всех событиях сервера.

## Настройка почтовых клиентов

Эти настройки необходимо произвести на компьютерах пользователей, которым нужен доступ к электронной почте посредством почтового сервера CMS. Для того чтобы почтовый клиент мог отправлять и принимать почту, в его настройках нужно указать адреса серверов входящей и исходящей почты, а также параметры учетной записи для подключения к почтовому ящику. Настройки в разных почтовых клиентах могут иметь различные названия, но обычно имеются следующие настройки: **SMTP сервер**, **POP3 сервер**, **Пользователь (Учетная запись)**, **Пароль**.

В поля **SMTP сервер** и **POP3 сервер** введите адрес компьютера, на котором запущен сервер CMS. Рекомендуется вводить IP-адрес, а не сетевое имя, т. к. при этом сервер не будет тратить дополнительное время на определение IP-адреса по сетевому имени (что, кстати сказать, не всегда возможно). IP-адрес компьютера вы можете узнать, запустив на нем программу ipconfig.exe или winipcfg.exe.

Если клиент запущен на том же компьютере, что и сервер, то для этого клиента в качестве IP-адреса серверов можно указать 127.0.0.1 (соответствующее сетевое имя — localhost). В поля **Пользователь (Учетная запись)** и **Пароль** введите имя и пароль почтового ящика, которые указаны в свойствах этого ящика на сервере. Если сервер использует нестандартные номера портов, то в клиентской программе укажите соответствующие значения (для этого, обычно, имеется поле **Порт**). **Тип подключения к серверу** — укажите с помощью локальной сети.

## Эксплуатация

Правильно установленный и настроенный сервер не требует постоянного внимания администратора и работает в автоматическом режиме. Текущие подключения клиентов к серверу, а также исходящие подключения к внешним SMTP- и POP3-серверам отображаются на панели подключений.

Для каждого подключения отображаются следующие параметры:

- значок, соответствующий типу подключения;
- Сессия** — идентификатор почтовой сессии;
- Протокол** — протокол, по которому выполнено подключение;
- Адрес** — имя или IP-адрес клиента/сервера, с которым идет обмен;
- Имя пользователя** — для SMTP-подключений отображается аргумент команды ENLO и имя пользователя, для POP3-подключений отображается имя пользователя (для клиентских подключений имя пользователя отображается только после аутентификации);
- Время подключения** — дата и время подключения. Для принудительного отключения клиента выделите соответствующий элемент в списке и в контекстном меню выберите команду **Удалить**.

Для остановки сервера CMS в меню **Файл** выберите команду **Остановить**.

События, происходящие в сервере, записываются в журнал. Журнал ведется одновременно в файле и на экране. Строки экранного журнала можно копировать, вырезать в буфер обмена и удалять с помощью команд контекстного меню.

Формат строки журнала следующий:

- тип события: " " (пробел) — информация, ! — ошибка, \* — предупреждение, + — подключение, "- — отключение, x — подключение клиента заблокировано IP-фильтром, > — отправка строки, < — прием строки, @ — действие с почтовым сообщением;
- дата и время события;
- имя компонента, к которому относится событие;
- идентификатор почтовой сессии;
- описание события.

Сеансы обмена почтой с Интернетом можно инициировать вручную. Для отправки почты в меню **Сервис** выберите команду **Отправить почту**, а для приема — команду **Принять почту**.

Имеется возможность удаленного запуска заданий планировщика. Для этого создайте отдельную учетную запись, например, scheduler. В планировщике создайте задание на отправку/прием почты круглосуточно каждую минуту, с условием **если существует файл**. В качестве имени файла укажите путь к почтовой папке созданной учетной записи — Mail\Mailbox\scheduler\\*.msg. Установите флажок **удалить файл после запуска задания**. Теперь отправьте любое сообщение на адрес созданной учетной записи (**scheduler@локальный\_домен**). После того как оно попадет в почтовый ящик scheduler, в течение минуты запустится задание планировщика.

Если необходимо управлять отдельно отправкой/приемом почты, создайте, соответственно, две учетные записи (например, scheduler\_send и scheduler\_recv) и настройте два задания планировщика.

Если при попытке отправки сообщения в Интернет удаленный SMTP-сервер не принял ни одного получателя или вернул код постоянной ошибки (5xx), файл со-

общения получает расширение `bad`, и попыток его отправить больше не производится. Постоянная ошибка сервера означает, что данное сообщение не может быть отправлено без корректировки. Причину отказа сервера и код ошибки можно найти в журнале (искать лучше всего по имени файла сообщения — `*.msg`).

Для повторной попытки отправить такое сообщение дайте файлу расширение `msg`. Вероятнее всего, повторная попытка будет также неудачной.

Если в свойствах домена не указан администратор или его почтовая папка недоступна, то сообщения, направленные ему, будут удаляться.

## Безопасность

Имеются две ступени защиты сервера от несанкционированного доступа:

- фильтрация клиентских подключений;
- аутентификация подключившихся пользователей.

При подключении клиента его IP-адрес анализируется IP-фильтром, и, если подключение запрещено, соединение принудительно разрывается. Данный факт отражается в журнале.

Если круг компьютеров, которым разрешен доступ к серверу CMS, ограничен, настройте IP-фильтр таким образом, чтобы он разрешал подключение только с этих компьютеров и блокировал прочие подключения. Тем самым пресекаются попытки подключения к серверу с несанкционированного компьютера.

Однако возможны ситуации, когда с разрешенного компьютера осуществляется попытка несанкционированного доступа к серверу. Это могут быть, например, действия вируса. Для защиты от подобных действий используется аутентификация (проверка имени пользователя и пароля). Если она выполнена успешно, клиент получает доступ к серверу.

Методы аутентификации SMTP- и POP3-серверов можно условно разделить на две группы: с низкой секретностью и высокой.

При использовании методов с низкой секретностью (для SMTP это PLAIN и LOGIN, для POP3 — USER/PASS) пароль на сервер передается в открытом виде.

При использовании методов с высокой секретностью (для SMTP это CRAM-MD5, для POP3 — APOP/MD5) на сервер передается результат преобразования пароля, объединенного с другими данными, специальной хэш-функцией. При этом восстановить исходный пароль, зная результат преобразования, невозможно, т. е. даже в случае перехвата злоумышленником аутентификационных данных, передаваемых по сети, пароль защищен от компрометации.

Таким образом, рекомендуется использовать только методы с высокой секретностью, если их поддерживают почтовые клиенты, которые будут подключаться к серверу (это можно определить экспериментальным путем).

## Проверка работоспособности

После установки и настройки сервера и клиентов необходимо проверить их взаимодействие.

Предположим, что локальным доменом является **mydomain.ru**, порты SMTP/POP3-серверов стандартные (25 и 110 соответственно) и на сервере имеются два почтовых ящика: user1 и user2. Запустите почтовый клиент на компьютере пользователя user1 и создайте новое сообщение. В поле **Кому** (To) введите адрес **user2@mydomain.ru**. Введите любую тему и содержание письма. Отправьте письмо. Оно должно без ошибок отправиться на сервер.

Запустите почтовый клиент на компьютере пользователя user2 и примите почту. Должно прийти сообщение от user1. (Если сообщение не принято, подождите несколько секунд, пока сообщение попадет в почтовый ящик, и примите почту снова.) Создайте и отправьте ответ на сообщение.

Примите почту для user1.

Если оба письма нормально отправлены и приняты, можно считать почтовую систему работоспособной в локальной сети.

## Устранение неполадок

В случае возникновения проблем с отправкой или получением почты придерживайтесь следующего порядка действий:

1. Убедитесь, что при запуске сервера CMS запускаются SMTP/POP3-серверы (это отражается в журнале). Если они не запускаются, это означает, что какое-то другое запущенное приложение использует данные порты. Либо остановите это приложение, либо настройте серверы CMS на другие порты и запустите их.
2. Если SMTP/POP3-серверы запускаются нормально, тогда нужно попробовать подключиться к ним с компьютера пользователя при помощи служебной программы telnet. Для этого в меню кнопки **Пуск** выберите команду **Выполнить** и введите: telnet <адрес> <порт>, где *адрес* — это IP-адрес или сетевое имя компьютера, на котором запущен почтовый сервер CMS; *порт* — это порт SMTP-или POP3-сервера CMS (стандартные значения 25 и 110).

После выполнения команды в окне программы telnet должна появиться строка, начинающаяся с символов "220" для SMTP-сервера, и "+OK" для POP3-сервера. В данной строке должно также содержаться имя локального домена, назначенное в почтовом сервере CMS. Если это произошло, то соответствующий сервер доступен с данного компьютера.

Если серверы доступны, а почта не принимается или не отправляется, скорее всего, неправильно настроен почтовый клиент. Проверьте его настройки, возможно, указано неправильное имя пользователя или пароль.

Если сервер недоступен из программы telnet, то причина либо в настройке сервера (или он не запущен), либо проблема в сети. Проверьте настройки сервера, посмотрите файл журнала — там должны отражаться факты подключений/отключений и обмен данными по почтовым протоколам. Возможно, потребуется повысить уровень подробности журнала, чтобы детально разобраться в проблеме.

Для более комфортной работы с журналом разработчики предлагают дополнительную утилиту CMS Log Viewer (рис. 19.27), которую можно скачать с сайта программы.

Программа постоянно совершенствуется. После выхода бесплатной версии 1.57, которая доступна по ссылке <http://courierms.narod.ru/>, появились и не бесплатные новые версии, обладающие значительно более широкими возможностями.

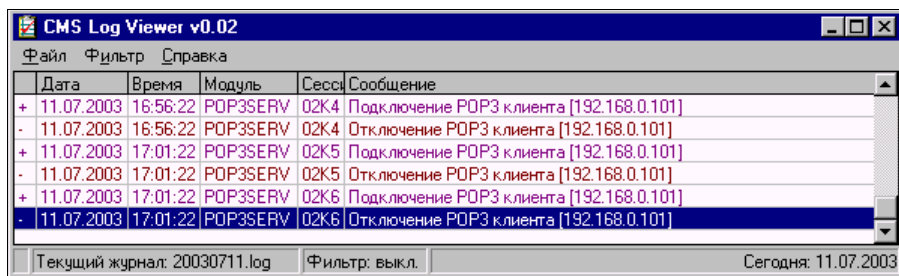


Рис. 19.27. Дополнительная утилита

## Ссылки

В Интернете можно найти и другие программы, которые могут работать в качестве почтового сервера, а также рекомендации по их настройке. Далее приведены ссылки на источники полезной информации:

- почтовый сервер в Linux

<http://www.sitysoft.com/modules/articles/item.php?itemid=11>,

<http://www.mailinfo.ru/stories.php?story=02/01/09/3747367>;

- Office Mail Server

<http://classcom.by/oms/>,

<http://darkdragon.dynalias.org/wiki/OMSHelp>;

- Kerio MailServer

<http://www.izcity.com/data/soft/article999.htm>;

- MDaemon

<http://www.redcom.ru/isp/netFiles/iServers/MDaemon>,

<http://www.ru-board.com/new/article.php?sid=142>.







## ЧАСТЬ V

# Преобразование одноранговой сети в иерархическую

Для сети под управлением ОС Windows в настоящее время есть только один путь перехода от однорангового варианта к иерархическому — это создание доменной сети. Даже если у вас много рабочих станций в одноранговой сети, то переход не будет слишком трудоемким и хлопотным. Рабочая станция, не включенная в домен, но работающая в сети, будет пользоваться DHCP-сервером, шлюзами в другие сети и Интернет, доступными ресурсами на других рабочих станциях. Иногда только потребуется указать имя и пароль учетной записи доменного пользователя, которую создать не долго и не трудно. Начинайте переход, не откладывая это полезное мероприятие в долгий ящик. Для небольшой сети, несмотря на существование более новых ОС, наиболее подходит Windows 2000 Server, на примере которой мы и рассмотрим создание иерархической сети.



## ГЛАВА 20



# Организация доменной сети

Что ни говори, а следить за прогрессом в области IT совсем не вредно. Уже несколько лет Active Directory (AD) активно эксплуатируется в локальных сетях, но некоторые администраторы до сих пор считают, что AD это излишество. Может быть и излишество, если у вас всего две машины с Windows XP Home или сеть из компьютеров под Windows 98. Но если в вашей сети больше двух компьютеров, предполагается, что будут подключаться и другие, причем под управлением разных ОС, то Active Directory вам совсем не повредит.

## 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 это целый комплекс средств Windows Server 2003. Это и сетевой каталог, содержащий сведения обо всех объектах сети, публикуемых в этом каталоге, это 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, которые для него предусмотрены 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, содержа-

щей 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 несанкционированных 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 19*, требует авторизации клиентов, как локальных пользователей компьютера.

Придется решить — по какому пути дальше идти. 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 не много, 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.

Традиционное для большинства системных администраторов начало установки новых ролей сервера — это **Администрирование | Мастер настройки сервера**. Роль, которую в данный момент следует выбрать для сервера, — это Контроллер домена (Active Directory). Контроллер домена — это 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.

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. 20.1).

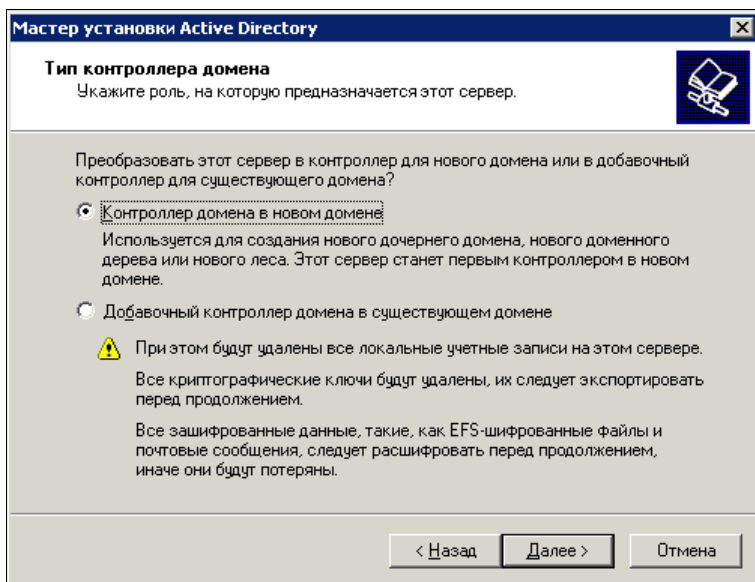


Рис. 20.1. Окно Мастер установки Active Directory (выбор роли сервера)

Далее необходимо определить тип создаваемого домена (рис. 20.2). В нашем случае это совершенно новый домен, независимый ни от каких других доменов.

#### ПРИМЕЧАНИЕ

Для выбора других вариантов требуется наличие уже работающей доменной сети.

На следующем этапе требуется указать имя домена (рис. 20.3). В главе 8 мы уже рассматривали вопрос об имени домена в связи с установкой DNS-сервера. Тогда было решено, что имя будущего домена будет **myhome.dom**. Это имя домена и применим при установке AD. Конечно, если вы имеете другой вариант имени, который необходимо использовать, применяйте его.

Введя имя и нажав кнопку **Далее**, подтверждаем или изменяем NetBIOS-имя домена (рис. 20.4).

Далее указываем место хранения данных AD (рис. 20.5). Имея эту информацию, вы можете делать резервные копии базы данных.

Указывая место размещения копии общих файлов домена (рис. 20.6), обратите внимание на то, что эта копия должна быть помещена в том NTFS. Для резервных копий файлов часто применяют отдельные диски FAT32, что позволяет обратиться

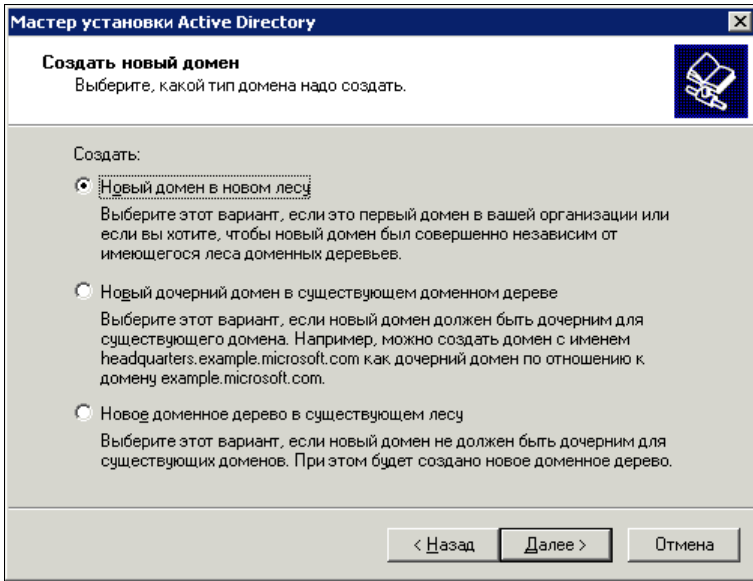


Рис. 20.2. Окно Мастер установки Active Directory (выбор типа домена)

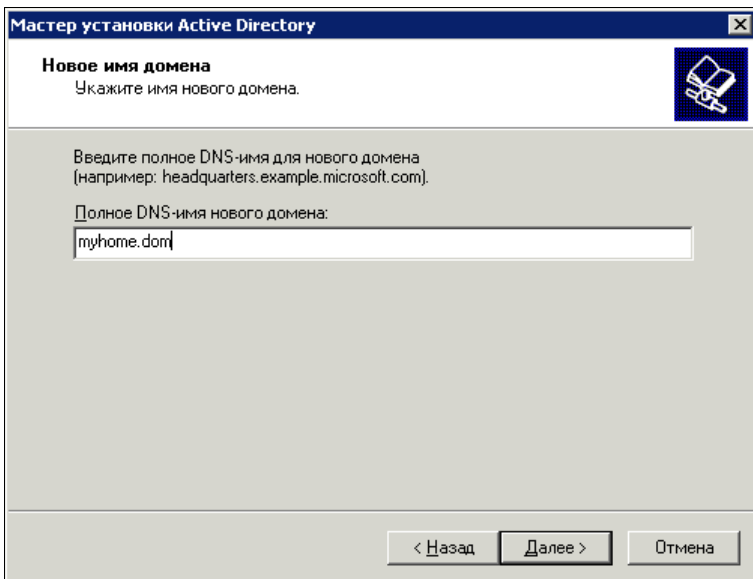


Рис. 20.3. Окно Мастер установки Active Directory (указание имени домена)

к этим дискам даже из под DOS в аварийной ситуации. Но в данном случае это 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 не правильно 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".

Далее мастер предложит выбрать вариант разрешений по умолчанию (рис. 20.7), применяемых в нашем домене. 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.

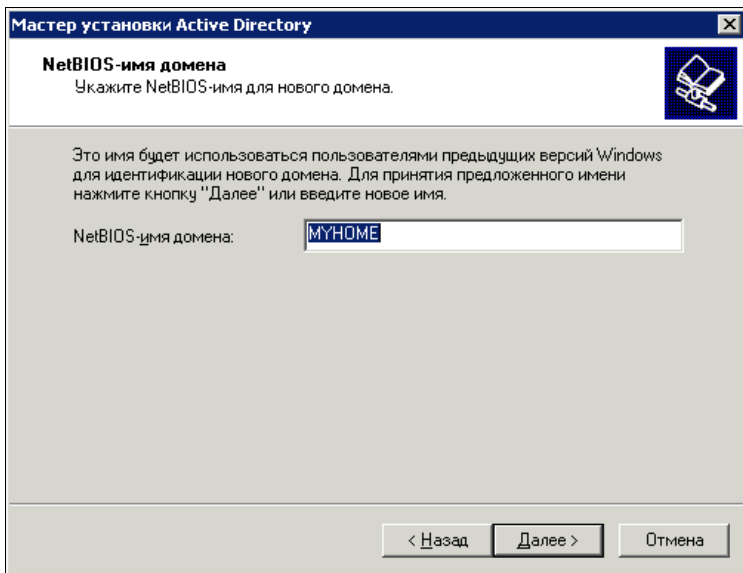


Рис. 20.4. Окно Мастер установки Active Directory — NetBIOS-имя домена

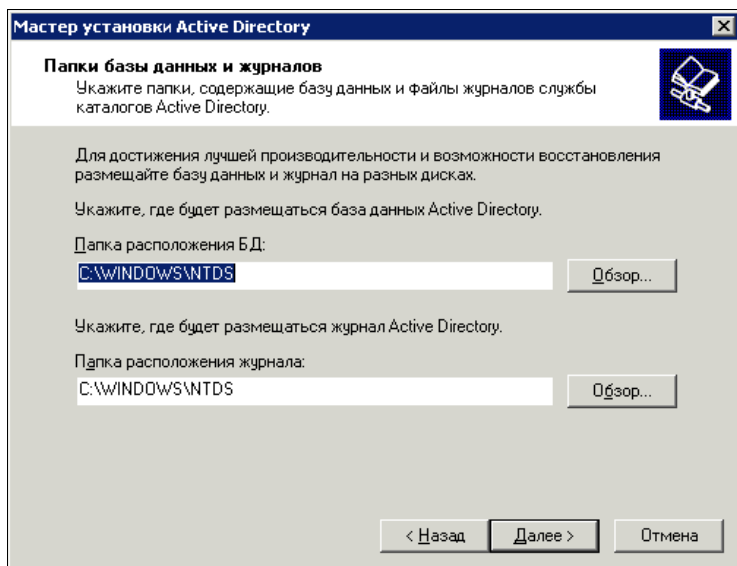


Рис. 20.5. Окно Мастер установки Active Directory (размещение базы данных AD и журнала службы каталогов)

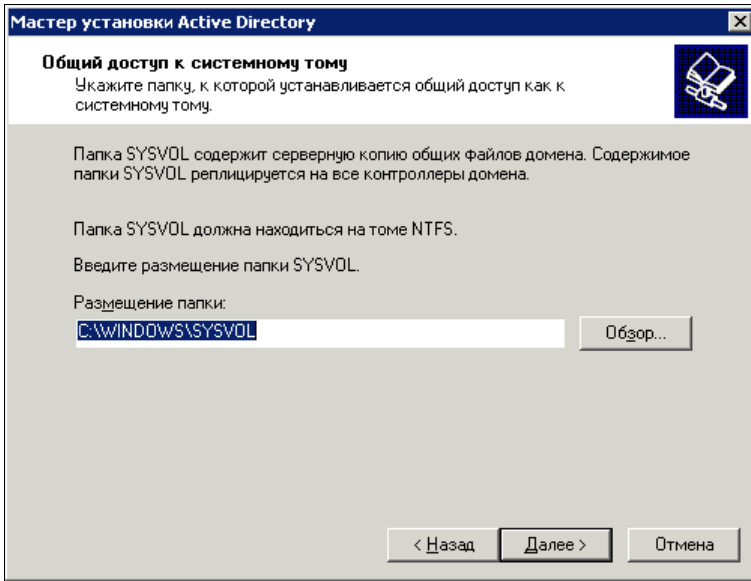


Рис. 20.6. Окно Мастер установки Active Directory (размещение копии общих файлов домена)

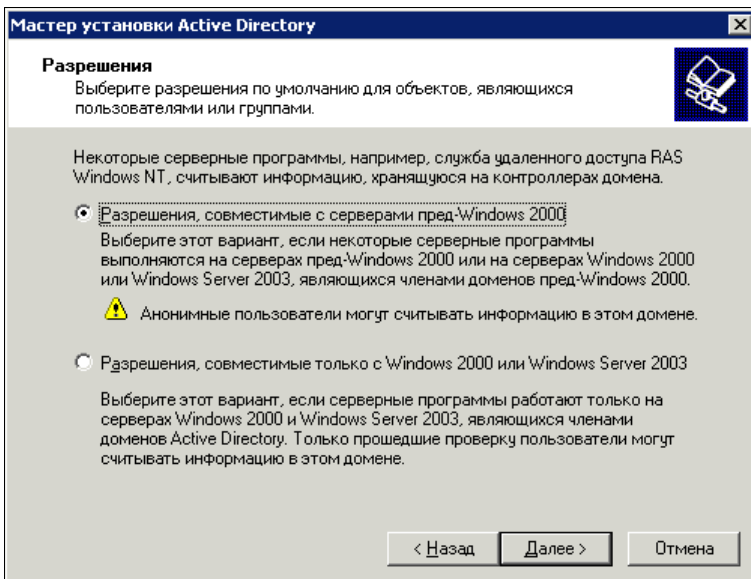


Рис. 20.7. Окно Мастер установки Active Directory (разрешения по умолчанию)

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 пояснений не требует (рис. 20.8).



После ознакомления вас со всеми выбранными вами опциями мастер начинает процедуру создания AD. На это может потребоваться несколько минут.

После завершения установки необходима перезагрузка сервера.

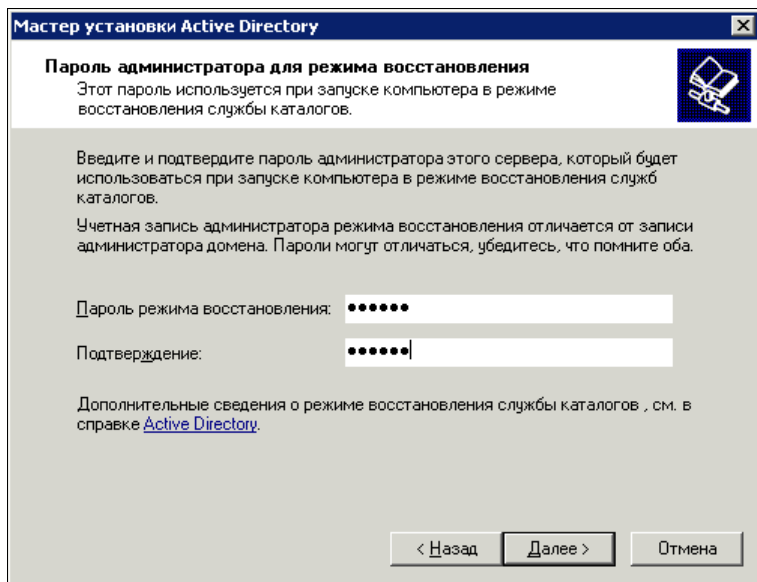


Рис. 20.8. Окно **Мастер установки Active Directory** (пароль режима восстановления)

## После перезагрузки

После перезагрузки все ранее установленные серверы и службы должны продолжать нормально работать, кроме почтового сервера. 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 в обычном режиме не возможна.

Теперь доступ к управлению учетными записями находится по адресу **Администрирование | Active Directory Пользователи и Компьютеры** (рис. 20.9). Здесь теперь все, — сами учетные записи, группы пользователей, которые заранее наделены определенными правами или создаваемые вами. На этом этапе настройки 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.

К сожалению, я не нашел способа, чтобы реанимировать службу POP3 после установки AD. Отправка писем по-прежнему работает, поскольку мы выбрали воз-

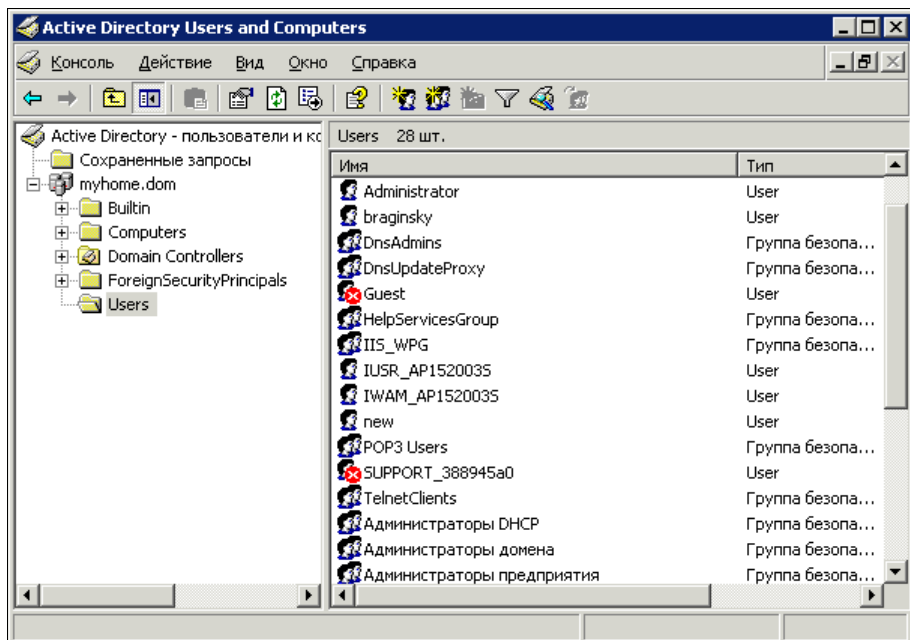


Рис. 20.9. Окно Active Directory Users and Computers — Active Directory — пользователи и компьютеры

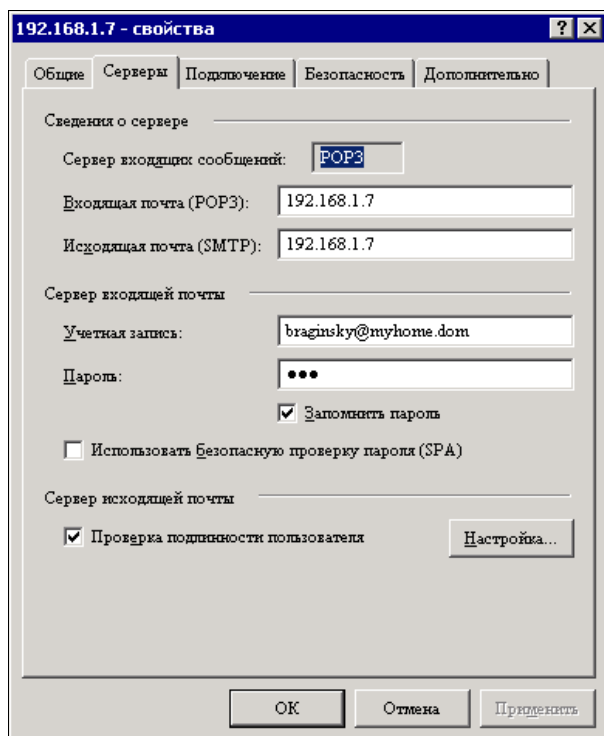


Рис. 20.10. Свойства учетной записи в Outlook Express

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. 20.10).

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 соответствующее окно: **Администрирование | Политики безопасности домена**. В открывшемся окне развернем **Параметры безопасности** и выделим **Политика паролей** (рис. 20.11).

Обратите внимание на правую сторону окна. Здесь можно указать свойства паролей, которые допустимо применять в домене. На рисунке показан самый мягкий

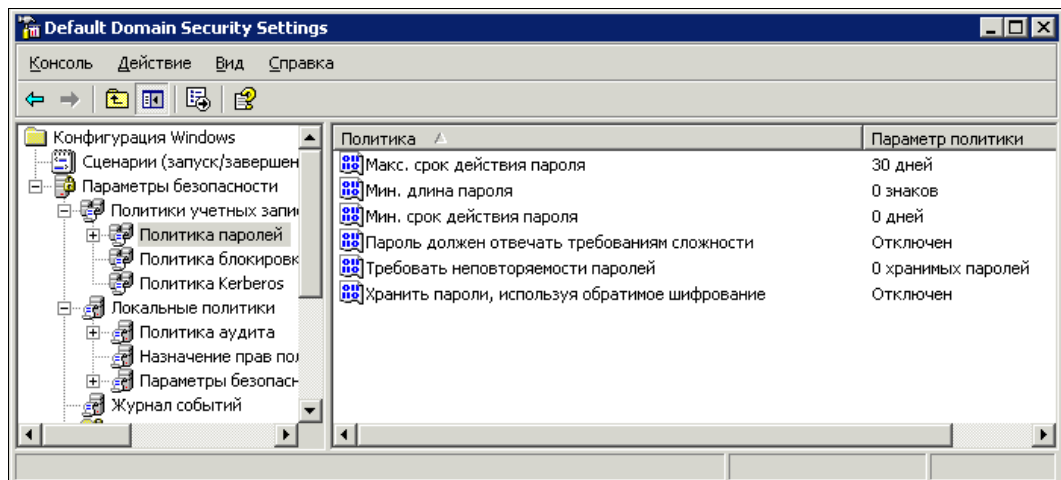


Рис. 20.11. Окно **Default Domain Security Settings** (параметры безопасности домена)

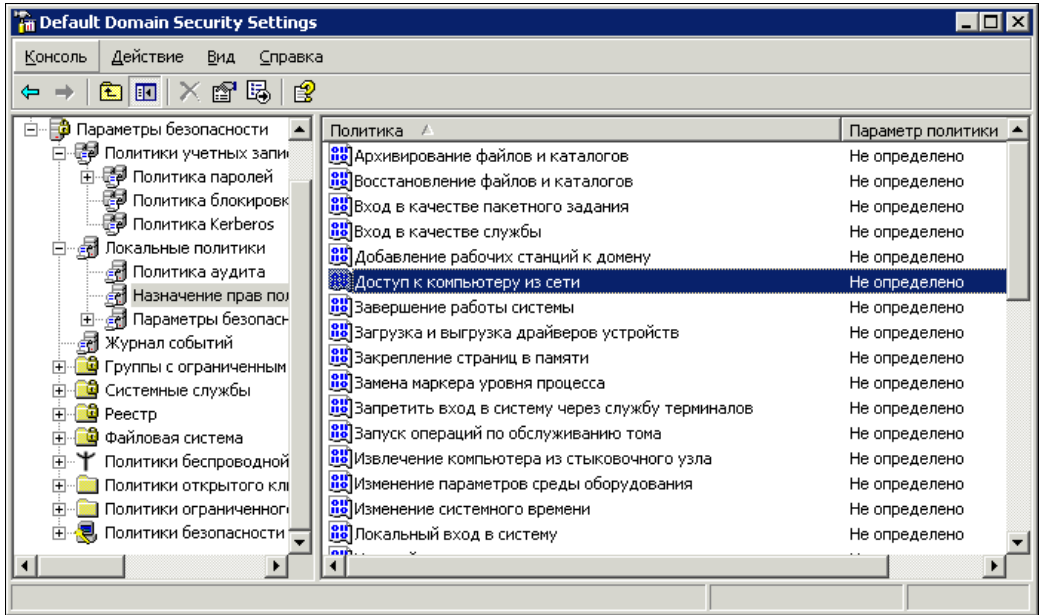


Рис. 20.12. Окно Default Domain Security Settings (параметры безопасности домена — Назначение прав пользователей)

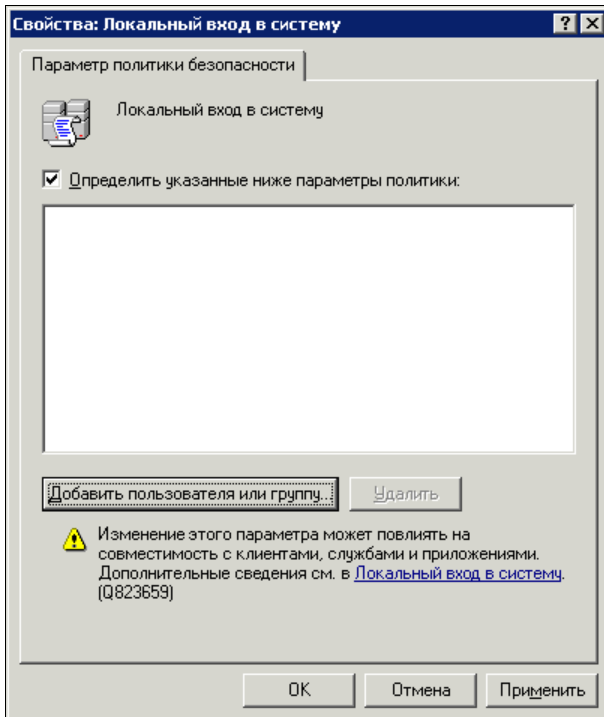


Рис. 20.13. Окно Свойства: Локальный вход в систему

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** и затем **Назначение прав пользователя** (рис. 20.12).

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. 20.13).

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. 20.9).

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), **ForeignSecurity-Principal** (Объекты из других доменов), **Users** (Пользователи).

В дереве объектов AD есть еще одна интересная папка — **Сохраненные запросы**, которая может быть полезной при поиске учетных записей, когда их становится много (рис. 20.14). Администратору домена нередко приходится в AD искать 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 поль-

зователей 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.

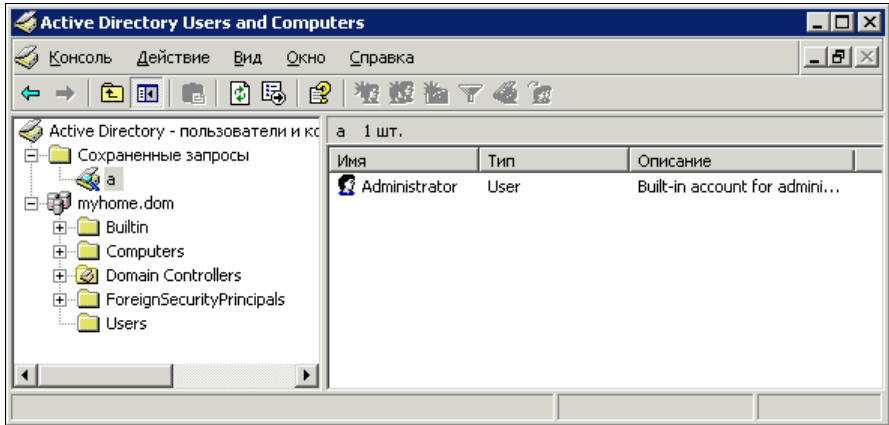


Рис. 20.14. Окно **Active Directory Users and Computers** — **Active Directory пользователи и компьютеры** (сохраненный запрос)

Создадим учетную запись пользователя, который имеет постоянную обязанность — контролировать работу DHCP-сервера, корректировать настройки этого сервера, при необходимости.

Открываем **Администрирование | Active Directory Пользователи и Компьютеры** (рис. 20.15). Для размещения всех созданных нами пользователей и групп создадим *организационные единицы* — OU (*Organizational Unit*). Создаются они точно так же, как обычные папки. В данном примере создана OU — Family (семья) с вложенными OU — Groups (группы) и Users (пользователи).

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.

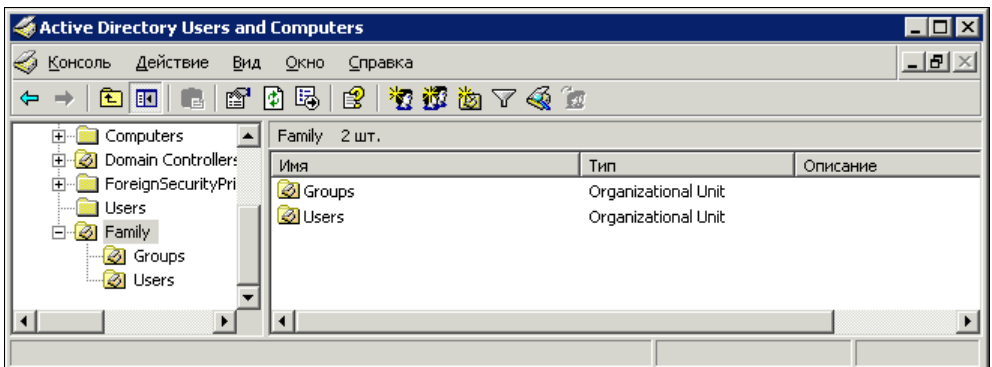
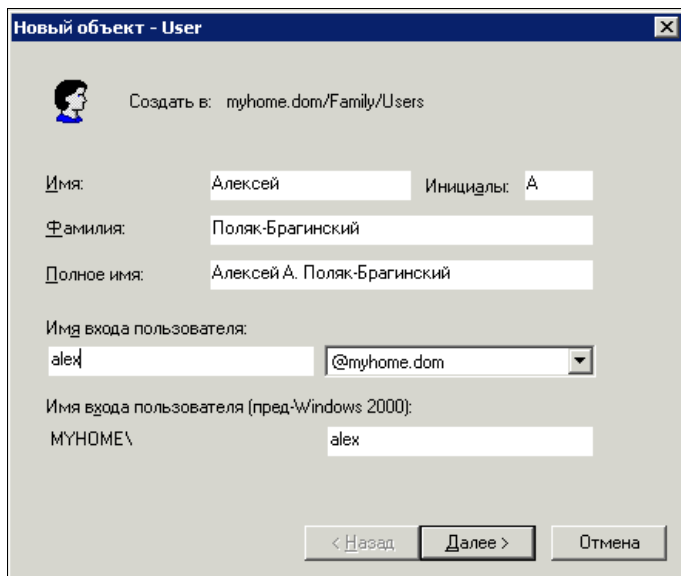


Рис. 20.15. Окно **Active Directory Users and Computers** (организационные единицы)

Перейдя в OU Users, вложенную в OU Family, создаем нового пользователя (User). При этом откроется окно, показанное на рис. 20.16.



Новый объект - User

Создать в: myhome.dom/Family/Users

Имя: Алексей      Инициалы: А

Фамилия: Поляк-Брагинский

Полное имя: Алексей А. Поляк-Брагинский

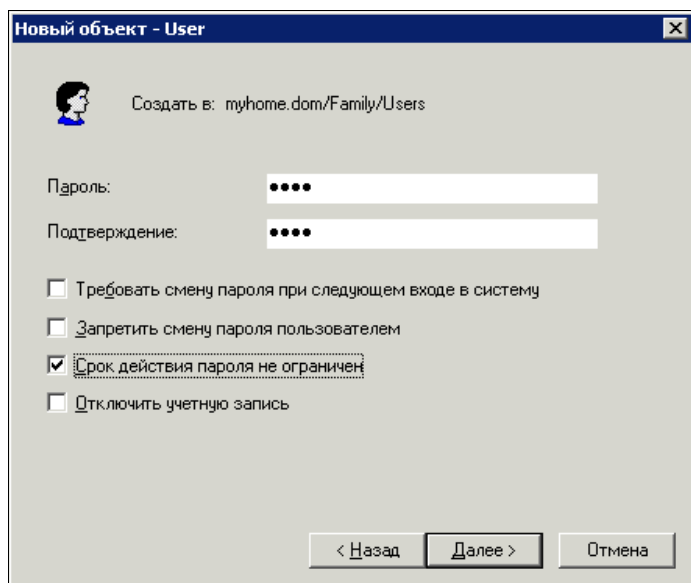
Имя входа пользователя:  
alex      @myhome.dom

Имя входа пользователя (пред-Windows 2000):  
МУНОМЕ\alex

< Назад      Далее >      Отмена

Рис. 20.16. Окно Новый объект — User

Заполняем все поля формы. Некоторые поля заполняются автоматически, но вы можете изменить созданные автоматически записи. Нажав кнопку **Далее**, перейдем в следующее окно (рис. 20.17).



Новый объект - User

Создать в: myhome.dom/Family/Users

Пароль: ●●●●

Подтверждение: ●●●●

Требуется смену пароля при следующем входе в систему

Запретить смену пароля пользователем

Срок действия пароля не ограничен

Отключить учетную запись

< Назад      Далее >      Отмена

Рис. 20.17. Окно Новый объект — User (создание пароля)

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.

Окно свойств учетной записи (рис. 20.18) 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.

The image shows a Windows-style dialog box titled "Свойства: Алексей А. Поляк-Брагинский". It has a tabbed interface with the following tabs: "Член групп", "Входящие звонки", "Среда", "Сеансы", "Удаленное управление", "Профиль служб терминалов", "СOM+", "Общие", "Адрес", "Учетная запись", "Профиль", "Телефоны", and "Организация". The "Общие" tab is selected. Below the tabs, there is a small profile picture icon and the name "Алексей А. Поляк-Брагинский". The main area contains several text input fields: "Имя:" (containing "Алексей"), "Инициалы:" (containing "А"), "Фамилия:" (containing "Поляк-Брагинский"), "Выводимое имя:" (containing "Алексей А. Поляк-Брагинский"), "Описание:", "Комната:", "Номер телефона:" (with a "Другой..." button), "Эл. почта:", and "Веб-страница:" (with a "Другой..." button). At the bottom, there are three buttons: "ОК", "Отмена", and "Применить".

Рис. 20.18. Окно Свойства: <Имя учетной записи>

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. 20.19). Нажмите кнопку **Добавить**. В открывшемся окне **Выбор: "Группы"** нажмите кнопку **Дополнительно**. В развернутом окне **Выбор: "Группы"** нажмите кнопку **Поиск** (рис. 20.20).



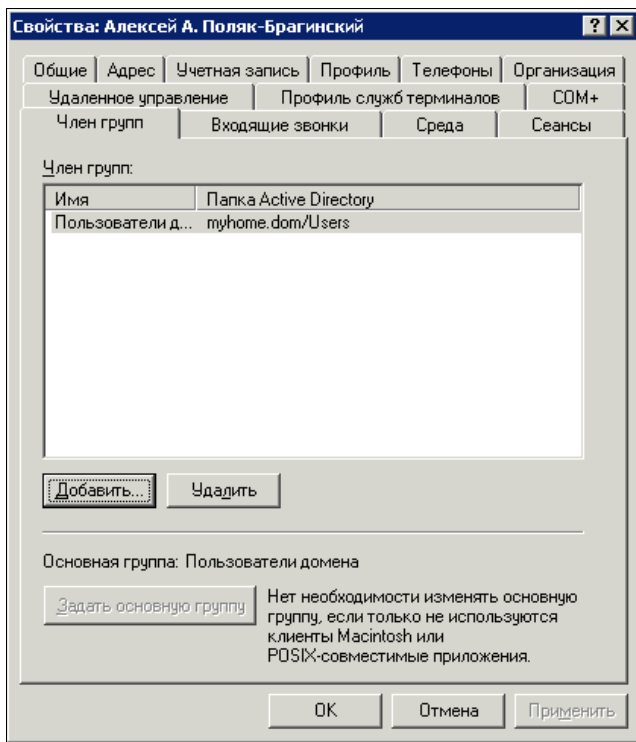


Рис. 20.19. Окно **Свойства: <Имя учетной записи>** (добавление в группу)

В появившемся списке уже существующих групп найдите **Администраторы ДНСР**. Выделите ее мышью и нажмите кнопку **ОК**.

В свернутом варианте этого окна (рис. 20.21) появится имя выбранной группы в поле для ввода имен объектов. Нажав еще раз **ОК**, 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 (см. рис. 20.19). Они позволяют 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**. 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.

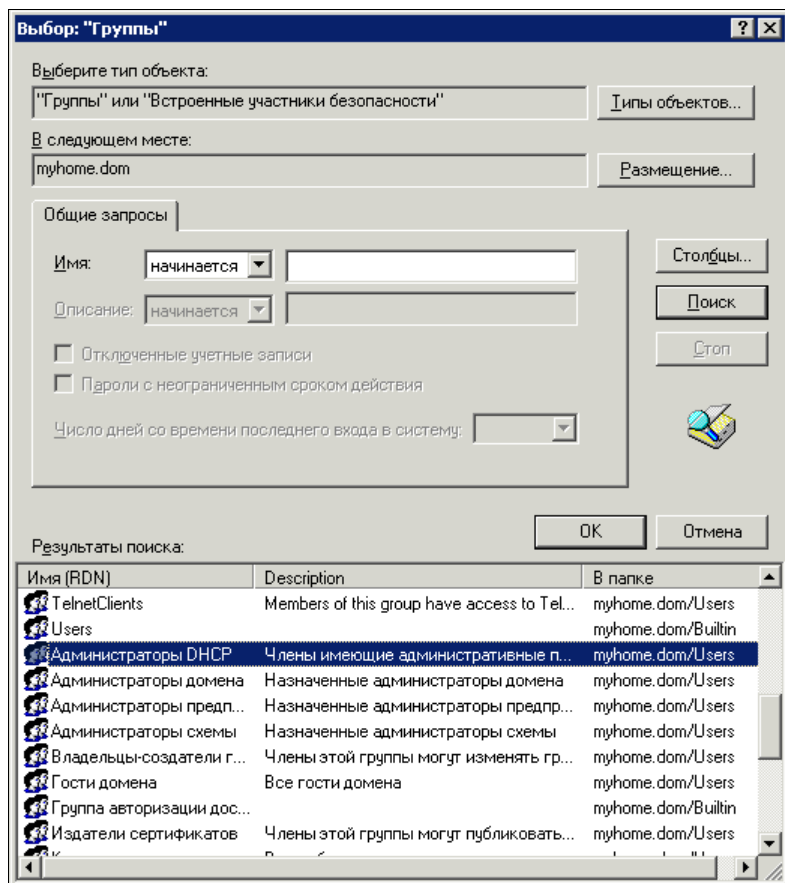


Рис. 20.20. Окно Выбор: "Группы"

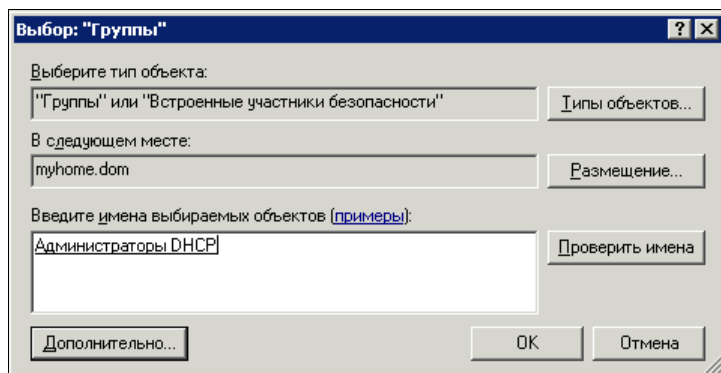


Рис. 20.21. Окно Выбор: "Группы" (свернутый вариант)

## Сетевой профиль

Редко, кто из сетевых администраторов применяет это свойство учетной записи. Но если вы хотите максимально унифицировать рабочие станции и их настройки, то 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 получают дополнительное преимущество — независимо от того, с какой рабочей станции они входят в сеть, вид рабочего стола и ярлыки к программам будут неизменны. Пользователи в любой момент могут закрыть лишние элементы рабочего стола, но при следующей загрузке компьютера эти элементы появятся вновь.

Профиль служб терминалов аналогичен сетевому профилю пользователя, но настраивается только на сервере. На рабочей станции для настройки профиля сервера терминалов не потребуются выполнять дополнительных действий.

## Регистрация компьютеров

В папке Computers окна **Active Directory Users and Computers** (рис. 20.22) можно поместить учетные записи компьютеров. Правда, реально действующими могут быть только учетные записи компьютеров с ОС не ниже Windows 2000.

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 (см. рис. 20.19). Примечательно это свойство тем, что мы можем не пользователя, а саму рабочую станцию наделить определенными правами.

Ни в какой одноранговой сети такое невозможно 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.

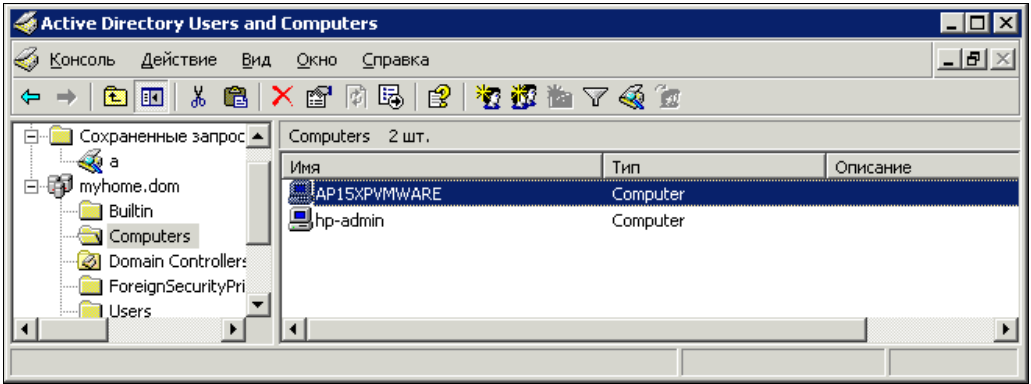


Рис. 20.22. Окно **Active Directory Users and Computers** (папка **Computers**)

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 доступ к ним. В отдельных случаях надо 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. 20.23).

Опубликовав принтер в Active Directory, вы сможете назначать права для управления данным принтером отдельным пользователям. Для этого достаточно открыть окно свойств объекта (принтера) и назначить управляющего (рис. 20.24).

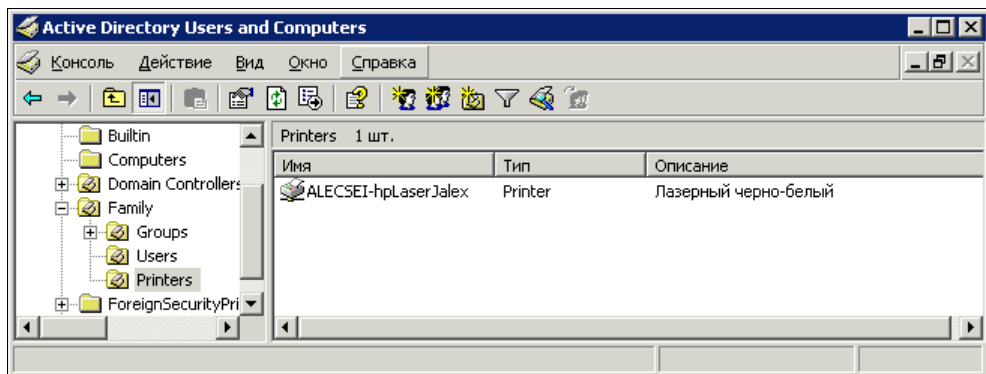
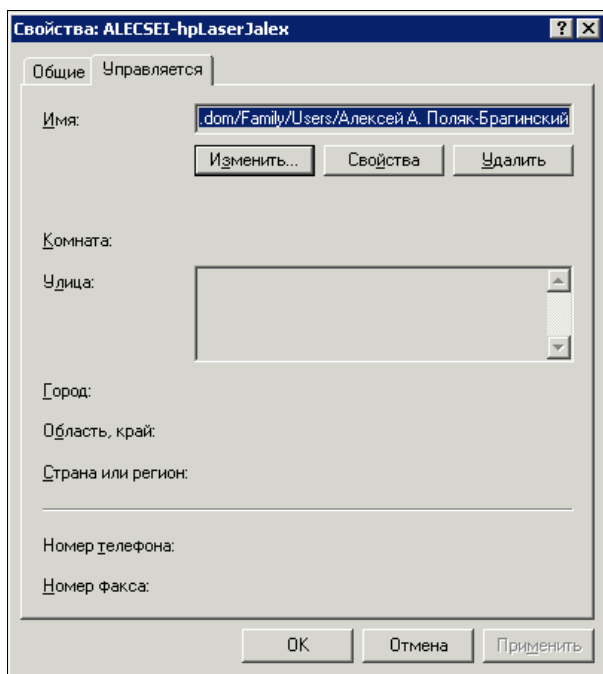


Рис. 20.23. Окно Active Directory Users and Computers (Printers)

Рис. 20.24. Окно **Свойства: <Имя принтера>**, вкладка **Управляется**

## Изменение свойств объектов

Я ранее уже упоминал о том, что можно изменять свойства сразу нескольких объектов, входящих в Active Directory. Это можно делать с помощью сохраненных запросов. На рис. 20.25 показан сохраненный запрос **Пользователи**, в котором определяющим поиском 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.

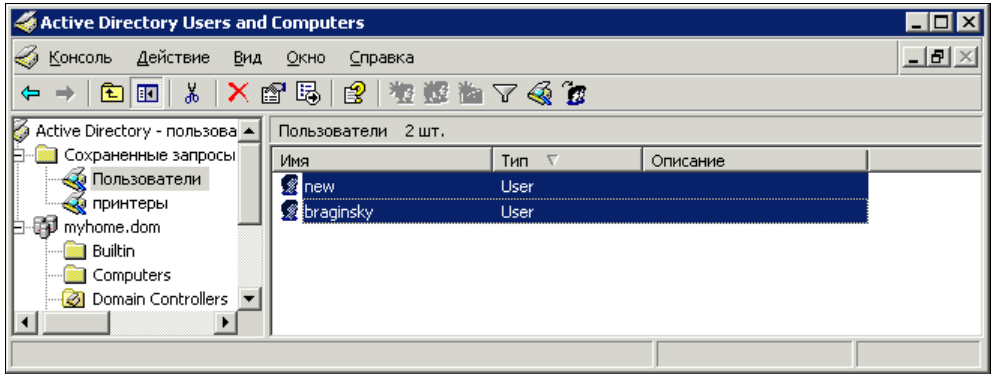


Рис. 20.25. Окно **Active Directory Users and Computers** — **Active Directory** — пользователи и компьютеры (сохраненный запрос Пользователи)

Теперь, удерживая клавишу <Shift>, выделяем все найденные записи.

Выбрав в контекстном меню всего выделенного блока записей пункт **Свойства**, мы можем изменять свойства сразу для всех выбранных объектов (рис. 20.26). Выбрав, например, опцию **Время входа**, мы попадем в окно **Время входа** (рис. 20.27).

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.

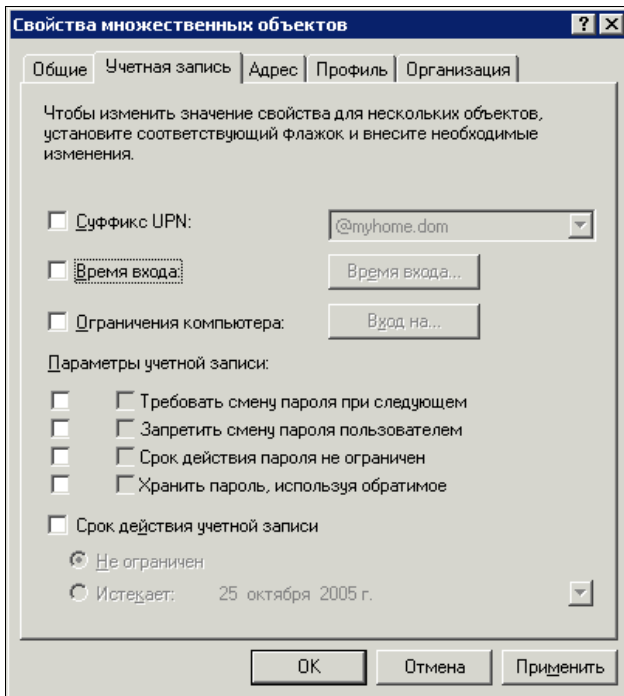


Рис. 20.26. Окно **Свойства множественных объектов**

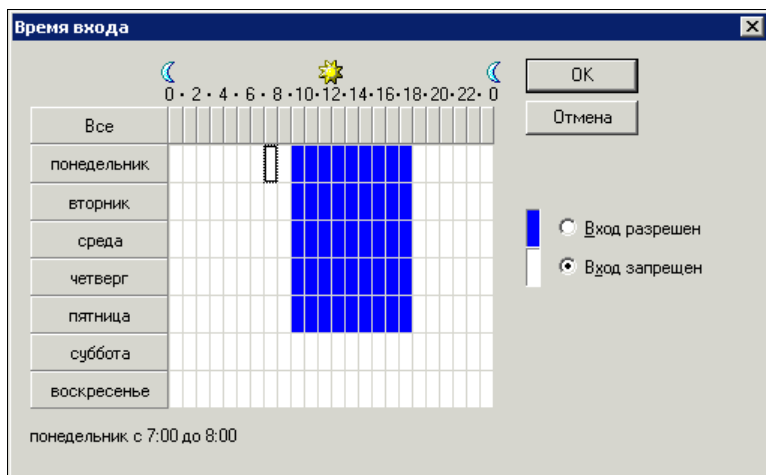


Рис. 20.27. Окно Время входа

## О безопасности

Раньше, когда компьютеры вашей сети были в рабочих группах, желательно было выполнять одно правило: "Не проводить повседневную работу на рабочих станциях от имени администратора компьютера".

Это правило связано с обеспечением информационной безопасности в сети. К сожалению, операционная система Windows уже всегда позволяет его выполнять. Есть приложения, которые отказываются работать, если пользователь не администратор компьютера. Но на сервере доменной сети это правило должно выполняться в любом случае. Старайтесь не использовать на сервере приложения, которые требуют сеанса администратора домена или компьютера. Многие серверные приложения могут работать в режиме службы (сервиса). Таким приложениям не нужен активный сеанс пользователя, открытый на компьютере. Соответственно, в обычном режиме может вообще не быть пользователей, которые вошли в систему на сервере. Особенно важно, чтобы администратор домена не имел постоянно открытого сеанса. Вы можете спросить: что же теперь необходимо для выполнения любого действия — входить, а потом снова выходить из сеанса? Нет. На сервере для удобства работы может быть запущен сеанс почти бесправного пользователя. А для выполнения программ и процедур от имени администратора домена существует команда `runas`. В графическом режиме работы она может быть выполнена выбором в контекстном меню ярлыка программы пункта **Запуск от имени** или в англоязычном варианте **Run as**. Но можно использовать команду из окна командной строки. Учитывая, что большинство администраторов применяют файловый менеджер FAR, можно именно его запускать таким образом. Теперь из его окна будут доступны и другие программы или консоли администратора. Все, что будет запущено или открыто из файлового менеджера, запущенного от имени администратора домена, так же будет открываться от его имени.

Вот как выглядит команда запуска файлового менеджера FAR от имени администратора домена МУНОМЕ в командной строке (все пишется в одну строку) из сессии простого пользователя SimpleUser (листинг 20.1).

#### Листинг 20.1

```
C:\Documents and Settings\SimpleUser>runas /user:myhome\administrator
c:\far\far
Введите пароль для myhome\administrator:
```

После ввода команды система затребует пароль администратора домена, а после его ввода откроется FAR. При вводе пароля никакие символы не отображаются. При первом открытии файлового менеджера от имени администратора домена его следует немного подстроить под текущего пользователя.

Я надеюсь, что описанных возможностей Active Directory вполне достаточно, чтобы вы могли представить возможности управления объектами в нем и осознать удобства администрирования сети, когда установлен этот компонент сервера.

Приведу несколько ссылок на источники полезной информации о переходе на работу с Active Directory (AD).

Перевод сети на Windows 2000:

- <http://www.osp.ru/text/302/175285/>;
- [http://rtfm.rechitsa.by/modules.php?name=News&file=view&news\\_id=237](http://rtfm.rechitsa.by/modules.php?name=News&file=view&news_id=237).

Переход на Windows 2003:

- <http://www.osp.ru/text/302/177399/>.

Большая коллекция материалов о Windows 2003:

- <http://www.networkdoc.ru/insop/win2003.html>.

Большая коллекция материалов по AD:

- <http://www.networkdoc.ru/insop/activ-dir.html>.

Полезности для администратора:

- <http://www.jroshin.pp.ru/cgi-bin/sqcgi/area/RU.WINDOWS.XP/codewin/msg/141>

Интересно, что для Linux тоже существует сервер каталогов— аналог AD. Например, на странице <http://mds.mandriva.org/wiki/Download> доступна версия Mandriva Directory Service для Mandriva Linux 2008. Но пока этот сервис не для начинающих администраторов, тем более что отсутствует его описание на русском языке. Впрочем, может быть вам будет интересно установить MDS и попытаться применить его в своей сети. В качестве клиентов сервиса могут быть и рабочие станции Windows.





## ЧАСТЬ VI

# Особые приемы администрирования

В этой части рассмотрим приемы администрирования сети, позволяющие упростить эту работу и сократить затраты времени администратора. Даже несложная работа может быть утомительной, если ее выполнять часто, или она требует многократного повторения одних и тех же действий. Не очень приятно, когда для выполнения простого действия на удаленном компьютере сети приходится куда-то идти, а хуже того ехать. В арсенале опытных администраторов всегда есть средства, которые позволяют снизить непроизводительные затраты времени и освободить его для более интересных дел.



# ГЛАВА 21



## Средства автоматизации

Целый класс средств, упрощающих работу администратора, это сценарии и написанные на их основе несложные программы, которые содержат в себе рутинные команды и выполняют их в заданном порядке. В Интернете на форумах, где общаются администраторы, можно найти много полезных сценариев, но еще больше можно написать самостоятельно. Рассмотрим несколько примеров сценариев и программ, которые вполне могут пригодиться и вам, поскольку были созданы для решения конкретных задач администрирования сети.

### Применяем сценарии

#### Общие сведения

*Сценарии*, или, как их часто называют, *скрипты*, — пожалуй, особая область практики администратора сети. Можно администрировать сеть и не иметь дела со сценариями. Во всяком случае, не применять их самостоятельно. Ведь сама операционная система использует разнообразные сценарии, которые настраиваются через интерфейсы, доступные пользователям. Разработчики скрыли от пользователя эти "премудрые" файлы, избавив его от необходимости изучения языков сценариев и чтения собственно сценариев, созданных кем-то.

Есть пользователи, которые даже обычный пакетный файл не в состоянии написать, не то что серьезный сценарий. Если вы решили администрировать сеть, пусть даже самую миниатюрную, есть смысл использовать эти простые, не требующие особых систем программирования, но все же программы.

Вот совсем простой пример применения пакетного файла в повседневной практике. У меня дома работает обычный компьютер, на котором работать удобнее, чем на ноутбуке, который приходится носить с собой. Но написанные на стационарном компьютере страницы необходимо каждый раз копировать на ноутбук. Есть, конечно, различные средства, разработанные Microsoft, для синхронизации данных на компьютерах. В очередной раз разработчики Windows избавляют пользователя от лишних раздумий. Но меня больше устраивают методы и средства, которые я могу

применять на любом компьютере и досконально понимаю, которые не надо долго настраивать и которые не могут привести к побочным эффектам в системе... Вот и на этот раз для меня было проще написать небольшой пакетный файл (листинг 21.1).

#### Листинг 21.1. Файл XcopyBook.bat

```
@ echo off
xcopy /c /y /z /i /e /d <Путь к каталогу с файлами> ↵
\\<Имя_компьютера>\<Сетевой путь к каталогу> >C:\Arch.txt
if errorlevel 4 goto lowmemory
if errorlevel 2 goto abort
Edit c:\arch.txt
goto exit
:lowmemory
echo Недостаточно памяти
echo или неверный путь.
goto exit
:abort
echo Нажата комбинация клавиш <Ctrl>+<C>.
goto exit
:exit
```

Для копирования измененных и новых файлов и вложенных каталогов применяется команда `xcopy`. Возможностей команды достаточно, чтобы выполнять копирование файлов на другой компьютер. Предусмотрены и сообщения о возможных при копировании проблемах. Все действия, выполняемые командой `xcopy`, протоколируются в файл `Arch.txt`, содержание которого после завершения процедуры копирования выводится на экран с помощью встроенного в Windows редактора `Edit`. Посмотрев на экран, можно убедиться, что все необходимые файлы скопированы.

Старые, проверенные средства, безотказно работающие на протяжении многих лет. Предварительно требовалось только дать доступ к каталогам на ноутбуке для пользователя стационарного компьютера.

Интересно, что из командной строки копирование, удаление и другие действия с файлами выполняются надежнее, чем через Проводник Windows. Однажды неудачно выполненная процедура восстановления системы и ее откат привели к образованию шести с половиной тысяч копий различных файлов. Попытка удалить все эти копии через Проводник регулярно приводила к зависанию системы. Команда `del` из командной строки с указанием маски для удаляемых файлов справилась с задачей без малейшей заминки.

Не стоит забывать средства, которые были разработаны еще во времена, предшествующие появлению Windows.

## Редактор PrimalScript

Конечно, в современных сетях старых средств явно не достаточно. Есть смысл применять языки сценариев, такие как VBScript, JScript. Это наиболее применяемые языки в практике администраторов сетей под Windows.

Для написания этих сценариев не требуется ничего, кроме текстового редактора, но удобней все же применять специализированные редакторы, в которых предусмотрена подсветка синтаксиса языков сценариев, есть возможность сохранять наиболее употребительные конструкции кода и даже выполнять сценарии в режиме отладки.

Один из таких редакторов — PrimalScript, который можно найти по адресу <http://www.primalscript.com/>. Конечно, это не единственное средство, но я им пользуюсь достаточно давно, и мне этот редактор кажется очень удобным. Как и во многих средствах разработки программ, в среде PrimalScript 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. Он расположен по адресу <http://www.microsoft.com/downloads>. При загрузке отладчика обратите внимание на его версию, должна быть версия Script Debugger for Windows NT 4.0, 2000, and XP.

На рис. 21.1 показано окно редактора PrimalScript с открытым файлом сценария.

Во время отладки сценариев в этой программе может вызываться окно отладчика сценариев Windows (рис. 21.2).

Достаточно полное описание программы представлено в документе <http://www.sapien.com/tutorials/ps20minutes.pdf>. Описание на английском языке, но хорошо иллюстрировано, и при понимании решаемой задачи может стать хорошим подспорьем на первых порах. Программа будет очень полезным дополнением арсенала администратора сети, если вы предполагаете писать сценарии регулярно.

Есть задачи, которые не могут быть решены иначе, чем через применение сценариев. Например, в Windows нет средства, отображающего группы, в которые входит учетная запись пользователя на сервере. Но достаточно запустить на выполнение сценарий, представленный в листинге 21.2, и перечень групп будет собран в текстовый файл.

### Листинг 21.2. Сценарий Groups.vbs. Список групп пользователей

```
'*****Список групп пользователей*****  
'Имя — Groups.vbs  
'DomainName — введите имя домена или сервера  
'Требуется 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*****

```

С помощью сценариев можно выполнять множество административных задач в сети. Например, назначить или отменить общий доступ к файлам на сетевом компьютере (листинги 21.3 и 21.4).

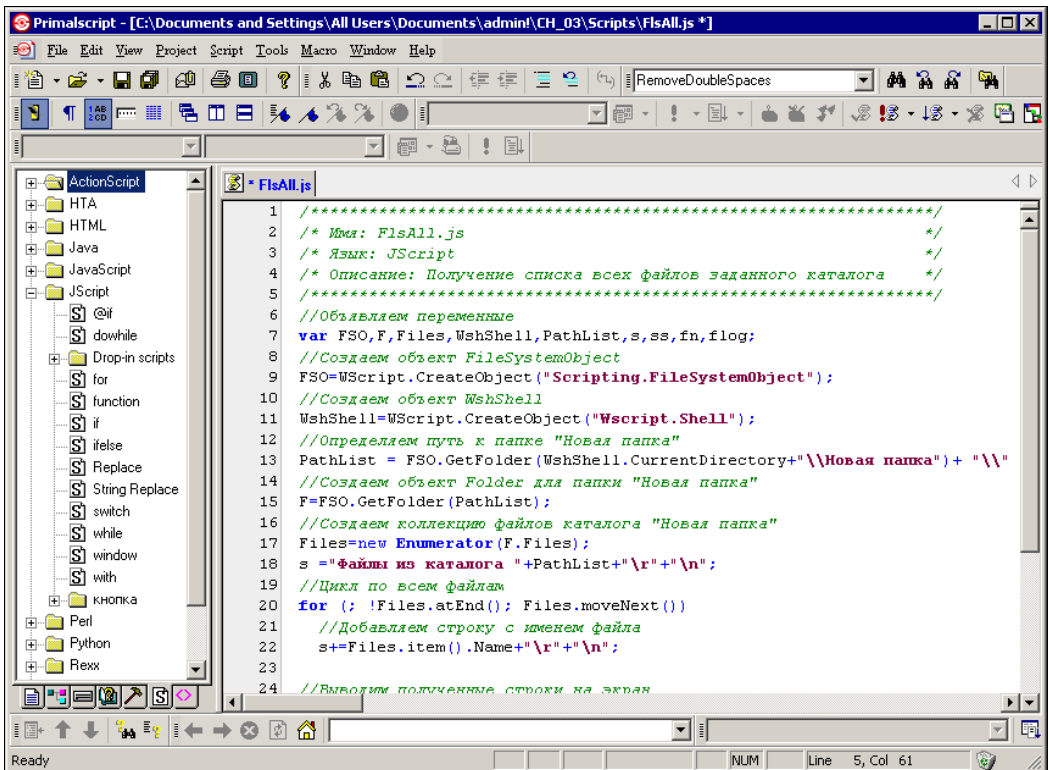


Рис. 21.1. Окно редактора PrimalScript с открытым файлом сценария

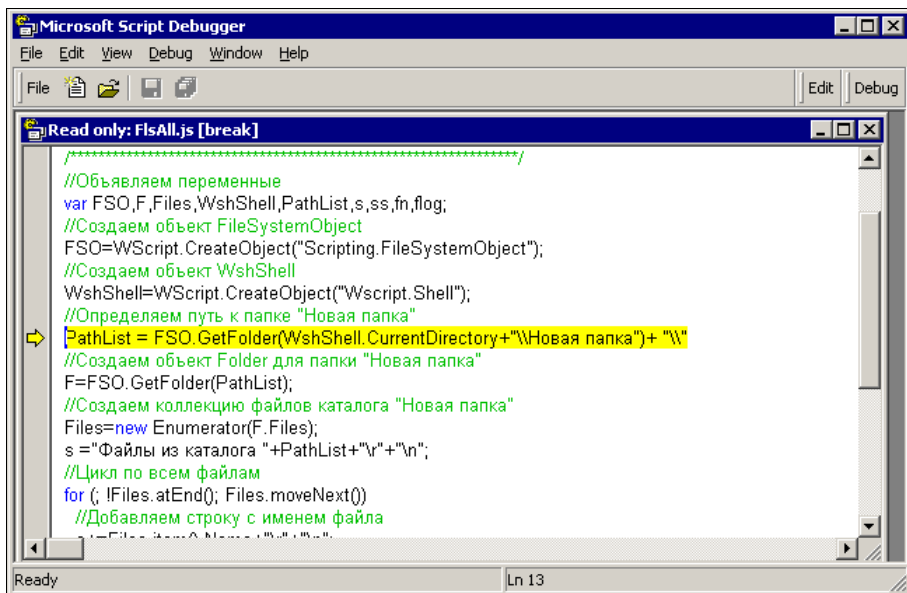


Рис. 21.2. Окно отладчика Microsoft Script Debugger с выделенной строкой кода, содержащей ошибку

### Листинг 21.3. 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*****

```

### Листинг 21.4. 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*****

```

### ПРИМЕЧАНИЕ

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

Конечно, обычно назначение общего доступа к папкам делается в спокойной обстановке, продуманно, с соблюдением режима информационной безопасности. Но иногда бывает необходимо поместить на удаленный компьютер какой-либо файл или наоборот скопировать его оттуда, но доступа к каталогу, содержащему файл, нет. Более того, наличие такого доступа недопустимо, а файл должен перемещаться или копироваться в автоматическом режиме. Что ж, можно открыть доступ к каталогу лишь на время работы с файлом. А по завершении этой работы закрыть доступ к каталогу.

Без применения сценария в такой ситуации не обойтись.

Есть еще одно интересное применение сценариям.

## Программы в формате HTA

Формат файлов *HTA* (HTML Application) получил распространение в качестве инструмента для индивидуального применения. Внутри файла могут ужиться сценарии, написанные на различных *script*-языках. При запуске такой файл выглядит как обычное окно программы. Эти свойства позволяют применить данный 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*-языках. 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. 21.3 и листинг 21.5).

### Листинг 21.5. 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="оНТА" CAPTION="yes" MAXIMIZEBUTTON=NO
      MINIMIZEBUTTON=NO>
<!--
  После объявления основных свойств страницы – скрипт, выводящий
  список пользователей в файл users.txt (размещен в заголовке)
  *****Начало*****'-->
<SCRIPT LANGUAGE="VBScript">
<!--
  DomainName = InputBox ("Введите имя сервера вместо
      заполнителей", "Пользователи на:", "XXXXX")
  Set Container = GetObject("WinNT://" & DomainName)
  Container.Filter = Array("User")
  i = 0
  StrTxt = ""
  Messg = ""
  For Each User In Container
    i = i + 1
    On Error Resume Next
    Messg = i
    Messg = Messg & ";" & User.Name
    Err.Clear
    Messg = Messg & ";" & User.FullName
    Err.Clear
    Messg = Messg & ";" & User.LastLogin
    If Err.Description <> "" Then Messg = Messg & ";" & _
        "01.01.1930 00:00:00"
    Err.Clear
    Messg = Messg & VbCrLf
    StrTxt = StrTxt & Messg
    Err.Clear
  Next

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

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

```

```

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

<!--Скрипт для вывода сообщения от часов'-->
<script language="VBScript">
<!--
  Sub mousmove()
    Alert "...И время ни на миг не остановишь!"
  End Sub
'-->
</script>

```

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

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

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

```
// -->
</script>

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

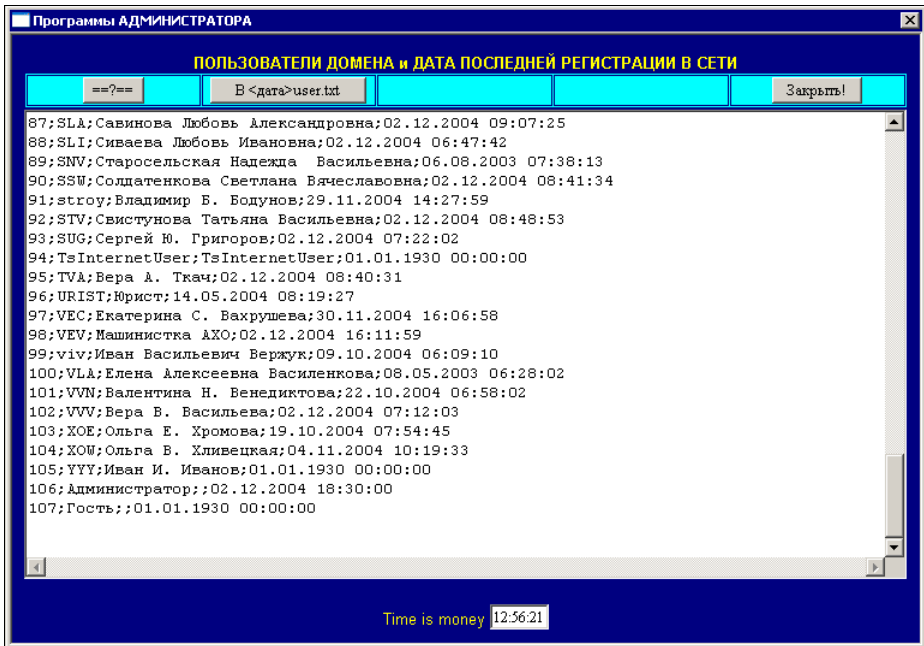


Рис. 21.3. Окно Программы АДМИНИСТРАТОРА

Для того чтобы эта программа заработала, достаточно весь ее код поместить в текстовый файл, а затем изменить расширение на hta. В процессе работы программа создает файл users.txt в том же каталоге, где она находится. Содержание текстового окна программы может быть отредактировано. После нажатия кнопки **В <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 НТА-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 редактор PrimalScript, пробный запуск программы из этой среды выполнять не стоит. НТА-файлы в этой среде работают некорректно, и запускать их следует отдельно

от среды разработки после сохранения изменений. Для уменьшения объема программы в ней не обработана одна ошибка. Если при запуске программы вы откажитесь от сбора сведений о пользователях, на экран будет выведено сообщение об ошибке, после чего будет показан список учетных записей, полученный при последнем нормальном запуске программы. Вы можете самостоятельно создавать подобные вспомогательные средства. Через непродолжительное время можно создать целый арсенал средств, который в наибольшей степени подойдет именно вам и для вашей сети.

## Ссылки

Если у вас появилось желание глубже познакомиться с языками сценариев и их возможностями, вы можете сделать это, посетив страницы в Интернете, которые посвящены этим вопросам.

На странице <http://www.okobox.narod.ru/scripts.htm> приведено несколько полезных для администратора сети сценариев, и в том числе, описанные в этой главе.

Следующие ссылки содержат как информацию о создании сценариев, так и их примеры:

- <http://www.citforum.ru/internet/html/hta/index.shtml>;
- <http://forum.script-coding.info/>;
- <http://www.script-coding.info/HTA.html>;
- [http://www.board74.ru/gui\\_for\\_script/articles/basis4.html](http://www.board74.ru/gui_for_script/articles/basis4.html);
- <http://www.citforum.ru/internet/vbscript/vbscript.shtml>;
- <http://www.rsdn.ru/article/files/dotnet/jsr.xml>;
- <http://forum.ru-board.com/topic.cgi?forum=24&topic=1539>.

## Сценарии в Linux

Операционная система Linux построена на основе множества сценариев, которые пользователями и разработчиками Linux обычно называются скриптами.

Поэтому для того, чтобы познакомиться с текстами сценариев в Linux, достаточно открыть в текстовом редакторе любой из них. Системные скрипты достаточно сложны для понимания начинающими, но при желании вы сможете разобраться в них.

Мы рассмотрим возможности повышения удобства работы в системе с помощью совсем коротких скриптов. Команды Linux могут выполняться последовательно, т. е. в одной строке может быть введена последовательность команд, которые будут передавать результат выполнения друг другу до получения желаемого результата.

Создание скрипта заключается в том, чтобы последовательность команд записать в исполняемый файл, который затем можно использовать многократно. Иногда эти команды не так уж и сложны, но удобнее выполнить команду с коротким и по-

нятым именем, чем вводить длинную цепочку составляющих команды. Исполняемым в Linux может быть любой текстовый файл, как с расширением, так и без него. Достаточно в качестве первой строки в файле указать `#!/bin/bash`, и сделать его исполняемым.

Приведем два примера скриптов, на основе которых вы сможете создавать свои собственные скрипты, изучив команды Linux. Все файлы по умолчанию создаются в каталоге текущего пользователя.

### Пример 1

Создадим скрипт добавляющий сетевому интерфейсу дополнительный IP-адрес.

Создадим исполняемый файл `myscr.txt`, вводя команды в окне терминала:

Введите:

```
cat > myscr.txt
```

Введите:

```
#!/bin/bash
```

Нажмите комбинацию клавиш `<Ctrl>+<D>`.

Введите:

```
chmod ugo+rw myscr.txt
```

Так будет выглядеть наша процедура в окне терминала:

```
beard@beard-laptop ~ $ cat > myscr.txt
#!/bin/bash
beard@beard-laptop ~ $ chmod ugo+rw myscr.txt
beard@beard-laptop ~ $
```

Заготовка файла есть. Теперь заполним содержательную часть файла:

```
beard@beard-laptop ~ $ cat >> myscr.txt
sudo ifconfig eth0:1 214.79.100.52 netmask 255.255.255.192
<Ctrl> + <D>
beard@beard-laptop ~ $
```

Проверим содержимое файла:

```
beard@beard-laptop ~ $ cat myscr.txt
#!/bin/bash
sudo ifconfig eth0:1 214.79.100.52 netmask 255.255.255.192
beard@beard-laptop ~ $
```

Все верно. Теперь для добавления дополнительного адреса интерфейсу `eth0` достаточно выполнить команду и проверить ее результат:

```
beard@beard-laptop ~ $ /home/beard/myscr.txt
[sudo] password for beard:
beard@beard-laptop ~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:d3:f9:30:6e
          inet6 addr: fe80::216:d3ff:fe9:306e/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:34919 errors:0 dropped:0 overruns:0 frame:0
```

```
TX packets:36738 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:27236428 (27.2 MB) TX bytes:4991537 (4.9 MB)
Interrupt:17
```

```
eth0:1 Link encap:Ethernet HWaddr 00:16:d3:f9:30:6e
inet addr:214.79.100.52 Bcast:214.79.100.63 Mask:255.255.255.192
UP BROADCAST MULTICAST MTU:1500 Metric:1
Interrupt:17
```

```
lo Link encap:Локальная петля (Loopback)
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:2896 errors:0 dropped:0 overruns:0 frame:0
TX packets:2896 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:266901 (266.9 KB) TX bytes:266901 (266.9 KB)
```

```
beard@beard-laptop ~ $
```

Команда сработала. Интерфейс eth0-1 получил дополнительный адрес.

Теперь создадим более сложный скрипт, который позволит оперативно узнавать владельцев IP-адресов, с которыми на данный момент установил связь наш компьютер.

Процедура создания файла аналогична рассмотренной в первом примере. Только содержание файла должно быть таким:

```
#!/bin/bash
sudo netstat -anp |grep 'tcp\|udp' | awk '{print $5}' | cut -d: -f1 | \
sort | uniq > data.txt
```

```
for ip in $(cat data.txt); do
whois $ip | echo "$ip $(grep 'netname')";
whois $ip | echo "$ip $(grep 'NetName')";
whois $ip | echo "$ip $(grep 'OrgName')";
done
```

При выполнении этот скрипт сохранит в файл data.txt перечень IP-адресов, с которыми установлено соединение, а затем с помощью команды whois проанализирует сохраненные адреса на предмет наличия в сведениях, полученных от регистраторов этих адресов полей "netname", "NetName" и "OrgName". Результат анализа будет выведен на экран. В момент создания примера на экран была выведена следующая информация:

```
beard@beard-laptop ~ $ '/home/beard/scr.txt'
0.0.0.0
0.0.0.0
0.0.0.0
```

```
192.168.10.1
192.168.10.1 NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
192.168.10.1 OrgName: Internet Assigned Numbers Authority
213.180.204.110 netname: YANDEX-213-180-204
213.180.204.110
213.180.204.110
213.208.165.26 netname: NaukaNet
213.208.165.26
213.208.165.26
69.46.36.6
69.46.36.6 NetName: NETRIVER02
69.46.36.6 OrgName: NetRiver INT LLC
74.125.79.100
74.125.79.100 NetName: GOOGLE
74.125.79.100 OrgName: Google Inc.
74.125.87.103
74.125.87.103 NetName: GOOGLE
74.125.87.103 OrgName: Google Inc.
74.125.87.155
74.125.87.155 NetName: GOOGLE
74.125.87.155 OrgName: Google Inc.
77.239.239.74 netname: RU-SATEL-20070312
77.239.239.74
77.239.239.74
87.248.207.254 netname: LLNW-EU-2
87.248.207.254
87.248.207.254
90.156.178.18 netname: vega-net
90.156.178.18
90.156.178.18
beard@beard-laptop ~ $
```

Расширения к имени файла скрипта можно не добавлять. Linux на расширения редко обращает внимание. В примерах расширение txt использовано для наглядности того, что исполняемым становится текстовый файл.



## ГЛАВА 22



# Средства удаленного управления и администрирования

О некоторых средствах управления сервером вы узнали, читая предыдущие главы. Например, для управления почтовым сервером мы применяли Web-интерфейс. Нетрудно самостоятельно разобраться и в других возможностях этого интерфейса. Но в этой главе мы рассмотрим два средства управления сервером и сетью, одно из которых стандартно, а другое — совершенно нестандартное средство, которое редко применяется, но в определенных условиях может быть очень полезно.

## Управляем локально

В данном случае "локально" обозначает только то, что мы находимся рядом с сервером и не ходим от компьютера к компьютеру для выполнения определенных административных функций.

Для действительно локального управления сервером существует средство Управление компьютером. Его можно найти в меню **Администрирование**, как в серверных операционных системах, так и в Windows XP и Windows Vista. Но это средство может быть использовано и для управления другими компьютерами, как серверами, так и рабочими станциями, находящимися в вашей сети. Это очень удобно, даже если сеть совсем не большая, а ее компьютеры находятся практически рядом.

На рис. 22.1 показано окно **Computer Management** (Управление компьютером).

При запуске этой консоли автоматически мы подключены к локальному компьютеру. Если это сервер, то к серверу. Уже это хорошо. Через данную оснастку мы можем управлять практически всеми параметрами нашего компьютера. Но, рассмотрев меню этого окна, мы обнаружим, что в меню **Действие** есть пункт **Подключиться к другому компьютеру**. Выбрав этот пункт, мы получим приглашение указать имя компьютера, который хотим администрировать (рис. 22.2).

Но, введя имя компьютера и нажав кнопку **ОК**, мы получим результат, который нас совершенно не устраивает (рис. 22.3). Это может произойти и не сразу, а при попытке выполнить какое-либо действие в окне.

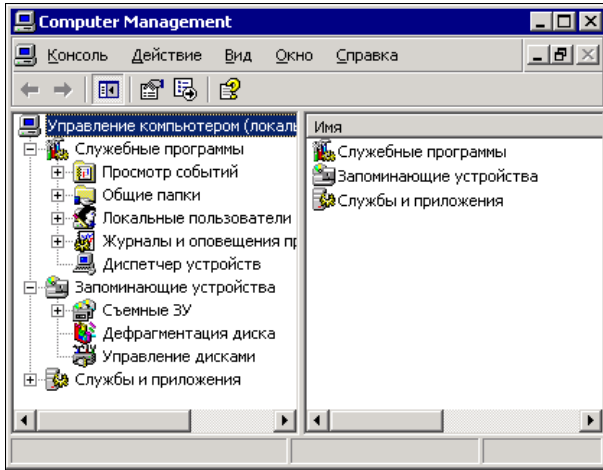


Рис. 22.1. Окно Computer Management

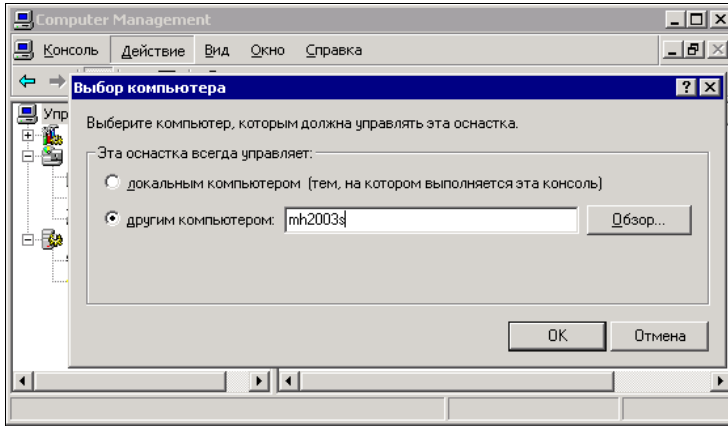


Рис. 22.2. Окно Computer Management — выбор компьютера

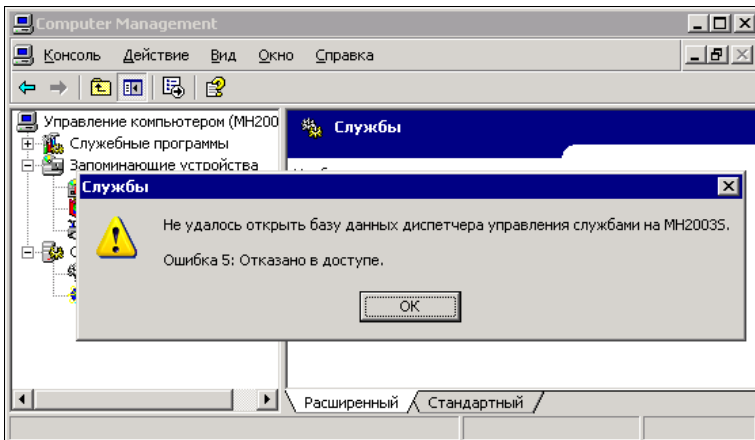


Рис. 22.3. Окно Computer Management — отказ в доступе к компьютеру

Нам отказано в доступе к управлению другим компьютером. В чем же дело? Все очень просто. Работая на любом компьютере, не принято работать в качестве администратора домена, но нам требуются именно его права для управления любым компьютером сети! Как быть? Все очень просто. Закрываем консоль и снова идем в меню **Администрирование**. Выбираем пункт **Управление компьютером**, но правой кнопкой мыши. В контекстном меню выбираем **Запуск от имени** и вводим имя и пароль администратора домена, не забыв перед именем указать имя домена. Теперь мы можем (рис. 22.4) выбрать службу на другом компьютере для того, чтобы ее включить или выключить.

На рабочих станциях и серверах, не являющихся контроллерами домена, можно управлять учетными записями пользователей (рис. 22.5).

Выбрав один из служебных Web-узлов (tsweb) на сервере, можно подключиться к сеансу удаленного рабочего стола (рис. 22.6).

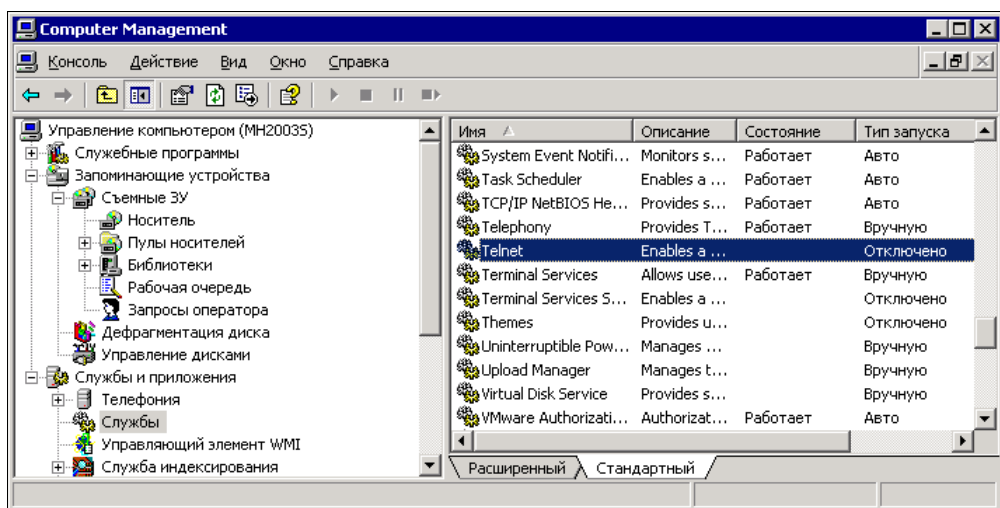


Рис. 22.4. Окно **Computer Management** — выбор службы для управления

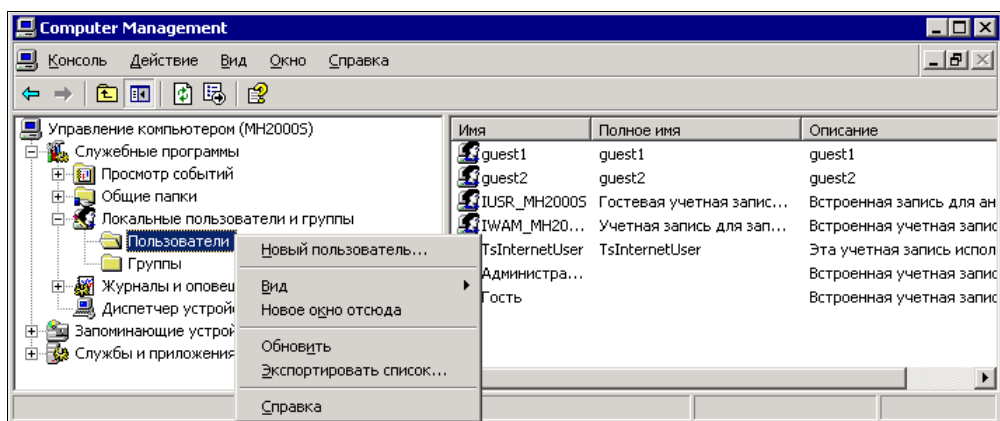


Рис. 22.5. Окно **Computer Management** — контекстное меню

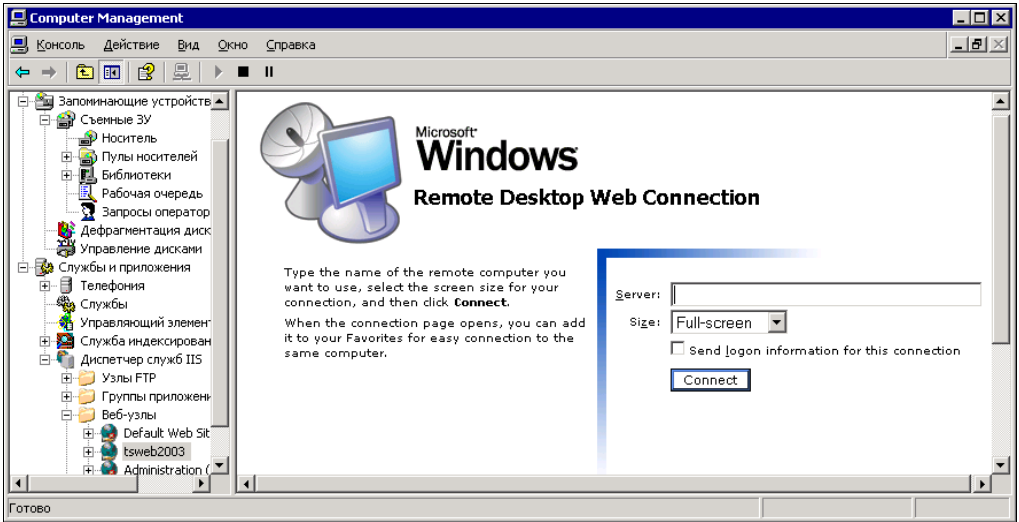


Рис. 22.6. Окно Computer Management — tsweb

Если с данного компьютера попытка подключения к удаленной машине происходит впервые, то вам будет предложено установить дополнительный компонент системы, а система безопасности Windows предупредит о возможных рисках (рис. 22.7). Конечно, в данном случае вы ничем не рискуете и можете согласиться с установкой компонента.

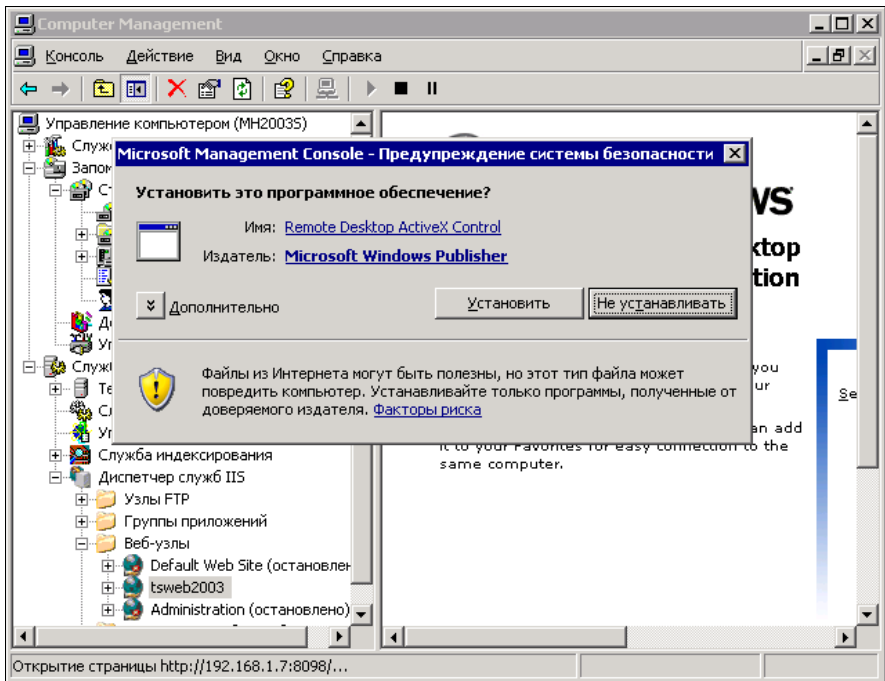


Рис. 22.7. Окно Computer Management — tsweb и предупреждение системы безопасности

Не удастся удаленно управлять дисками компьютера, но это и в самом деле, лучше делать, находясь рядом с машиной.

Таким образом, используя одно локальное средство управления компьютером, вы можете управлять компьютерами всей сети!

## Осуществляем удаленное администрирование

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

Тем не менее есть способ, позволяющий администратору выполнять некоторые процедуры, находясь вне своей сети, но имея доступ к электронной почте. Ведь почта может работать даже при очень медленном соединении с Интернетом. Для реализации этого способа необходимо обеспечить возможность автоматического приема и отправки почты со стороны удаленной сети. Для этих целей можно применить CourierMS — почтовый сервер, о котором мы говорили ранее, или настроить почтовый сервер, встроенный в Windows Server 2003. Кроме почтового сервера нам потребуется консольный почтовый клиент. На сайте <http://ironfist.at.tut.by/> можно найти очень компактный (менее 50 Кбайт) и, как показала практика, надежный консольный почтовый клиент ZeRAT. Применять его для работы с обычной электронной почтой, если на вашем компьютере Windows, большого смысла нет, если только вы не почитатель командной строки. Существующие распространенные почтовые клиенты вполне удовлетворяют запросам пользователей. Но это —

консольный почтовый клиент, в котором интерфейс для работы с ним — командная строка.

Те, кому требуется графическая оболочка, смогут ее найти на том же сайте. Ее применение даст возможность оперативно просматривать тексты сообщений, сохранившихся на сервере.

Роль командной строки с распространением Windows постепенно отодвигалась на второй план. Тем не менее новые операционные системы позволяют выполнять множество операций, в том числе и связанных с администрированием сети и сервера, из командной строки. Для сохранения заготовок команд можно применить обычные командные файлы с расширением `bat`.

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

## Решаем задачи администрирования по e-mail

Для рассмотрения работы программы ZeRAT и возможностей администрирования по e-mail решим простую задачу. Предположим, вы находитесь вне администрируемой сети, и вам с сервера необходимо проверить связь с одной из рабочих станций, IP-адрес которой известен. Для контроля наличия такой связи используется обычная команда `ping`, но ее применение возможно, когда есть доступ к серверу непосредственно или через удаленный рабочий стол, или через Telnet, или... — в любом случае требуется хорошая устойчивая связь с сервером. В наших условиях это невозможно, но нам требуется послать на сервер сообщение, содержащее необходимую команду. Сервер, выполнив команду, должен отправить вам результат ее выполнения.

Прежде всего, необходимо на почтовом сервере завести служебную учетную запись, куда будут приходить сообщения с командами, пусть это будет **admins@popdomayn**.

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

Для настройки ZeRAT используются несколько конфигурационных файлов. Рассмотрим настройки применительно к нашему случаю. Будем считать, что вы установили ZeRAT в папку C:\zerat\. В листинге 22.1 приведено содержание файла Zerat.ini

**Листинг 22.1. Файл Zerat.ini**

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

В листинге 22.2 представлено содержание файла admins.txt, в котором присутствуют все необходимые сведения для создания и отправки автоматического сообщения.

**ПРИМЕЧАНИЕ**

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

**Листинг 22.2. Файл admins.txt**

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

Для того чтобы сервер мог обработать ваше сообщение к нему, потребуется описание его действий в bat-файле. Листинг 22.3 описывает файл IN.bat, который должен запускаться с определенными вами интервалами планировщиком Windows. Сервер проверит наличие сообщения в почтовом ящике и даст команду на прием почты программой ZeRAT.

**Листинг 22.3. Файл IN.bat**

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

Для того чтобы сервер знал, откуда принять почту, создадим файл pop.ini (листинг 22.4).

**Листинг 22.4. Файл pop.ini**

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

В файле IN.bat содержится ссылка на unzip.bat (листинг 22.5). Этот файл необходим для распаковки вложения и выполнения дополнительных команд.

**Листинг 22.5. Файл unzip.bat**

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

Приняв, распаковав вложение, удалив файл архива, сервер выполнит командный файл admins.bat, содержание которого может быть следующим (листинг 22.6).

**Листинг 22.6. Файл admins.bat**

```
ping <IP-адрес> > mess.txt
out.bat
```

Результат выполнения команды ping будет записан в файл mess.txt, который сервер и отправит вам. Команды для отправки сообщения должны быть записаны в файле out.bat, содержание которого приведено в листинге 22.7.

**Листинг 22.7. Файл out.bat**

```
if not exist mess.txt goto d ; если нет mess.txt, прекращаем выполнение
pkzip -add c:\zerat\admins.zip mess.txt ; архивируем файл
```



```
zerat.exe admins.txt           ; отправляем архив на ваш адрес
del c:\zerat\mess.txt         ; удаляем более не нужные файлы
del c:\zerat\admins.zip
:d
```

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

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

Среди команд командной строки в новых операционных системах, начиная с Windows XP, появилось много новых. Возможности некоторых из них сравнимы с возможностями отдельных программ. Например, появился целый комплекс команд netsh diag. Эти команды подробно описаны в справочной системе, а здесь рассмотрим одну из них — netsh diag connect iphost.

В командной строке можно написать следующее:

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

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

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

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

Если заранее подготовить несколько вспомогательных bat-файлов, то можно упростить написание команд для сервера. Допустим, вам часто требуется проверять связь сервера с какими-либо компьютерами сети или с другими серверами. Вы можете в качестве заготовки для команд написать следующий файл ipscan.bat (листинг 22.8) и отправить его на сервер (процедуру отправки опишем позднее).

#### Листинг 22.8. Файл ipscan.bat

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

```
netsh diag connect iphost %4% 25
netsh diag connect iphost %4% 110
netsh diag connect iphost %4% 53
```

В этом файле несколько раз перечислена одна и та же команда, но с различными параметрами. Если вы поместите этот файл в папку C:\zerat\, то для выполнения сканирования по нескольким адресам вам понадобится файл admins.bat следующего содержания (листинг 22.9).

#### Листинг 22.9. Файл admins.bat с перечнем из четырех адресов

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

Как видно, написание командного файла существенно упростилось. В ответ на свое послание вы получите файл mess.txt с результатом работы вашей команды (листинг 22.10).

#### Листинг 22.10. Файл mess.txt с результатом выполнения команды

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

```

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

```

Просмотрев внимательно содержание файла, можно сделать выводы о работе просканированных узлов, представленные в табл. 22.1.

**Таблица 22.1. Обработанный ответ сервера**

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

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

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

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

А теперь процедура отправки заготовленных для выполнения команд. Для пересылки дополнительного файла его следует упаковать вместе с `admins.bat` в `admins.zip`. После получения этой посылки сервер распакует все файлы в папке `C:\zerat\`. Если вам необходимо сразу выполнить подготовленные команды, то содержание `admins.bat` соответствует листингу 22.9. Если требуется только переслать файлы и получить об этом уведомление, то файл `admins.bat` может быть таким, как в листинге 22.11.

#### Листинг 22.11. Файл `admins.bat` с заданием добавления заготовленных команд

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

Получив ответ (листинг 22.12), вы сможете убедиться, что все файлы находятся на своих местах.

#### Листинг 22.12. Файл `mess.txt` с перечнем `bat`-файлов

Том в устройстве C не имеет метки.

Серийный номер тома: 0936-D08A

Содержимое папки `c:\zerat\txt`

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

Содержимое папки `c:\zerat`

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

Вариант применения команды `dir` в данном случае позволяет вывести только имена командных файлов, находящихся в папках `C:\zerat\txt\` и `C:\zerat\`. Надеюсь, что приведенных примеров достаточно, чтобы представить себе возможности администрирования сети по электронной почте, но еще на одну следует указать сейчас. Почтовые сообщения от сервера могут быть достаточно краткими, чтобы использовать для чтения... сотовый телефон! Теперь настроив свой мобильник на прием электронной почты, вы сможете всегда получать сведения о состоянии сервера независимо от своего места нахождения. А еще можно воспользоваться услугами Smsmail (<http://www.smsmail.ru/>) и получать сообщения от сервера в виде SMS.

Вы можете заготовить множество команд удаленного управления, которые позволят вам из любой точки мира, где работает электронная почта, вести постоянный контроль за состоянием своих серверов и сетей, даже если их достаточно много.

## Удаленный доступ к рабочему столу рабочей станции через Интернет

Начнем с самого простого, хотя и не самого распространенного случая. У вас есть:

- рабочая станция с Windows XP Professional, к которой необходимо получить доступ;
- рабочая станция с операционной системой не ниже Windows 95, с которой надо получить доступ;
- хорошее подключение к Интернету;
- выделенный IP-адрес.

Последнее допущение на практике встречается не так уж и часто, но позднее, на основе уже рассмотренного варианта подключения, мы сможем решить эту задачу, когда постоянного IP-адреса у вас нет.

## Настраиваем рабочую станцию с выделенным IP-адресом

Итак, настраиваем рабочую станцию, к которой хотим получить доступ.

Для выполнения описываемых настроек нужен обычный доступ к компьютеру в локальном режиме с его консоли (монитор, клавиатура, мышь), необходимо быть администратором компьютера.

1. В Панели управления откройте компонент **Установка и удаление программ**.
2. Нажмите кнопку **Установка компонентов Windows**.
3. Выберите компонент **Internet Information Services (IIS)** и нажмите кнопку **Состав**.

4. В списке **Internet Information Services** — **состав** выберите элемент **World Wide Web Service** (Служба WWW) и нажмите кнопку **Состав**.
5. В списке **Служба WWW** — **состав** установите флажок **Remote Desktop Web Connection** (Интернет-подключение к удаленному рабочему столу) и нажмите кнопку **ОК**.
6. В окне мастера компонентов Windows нажмите кнопку **Далее**.
7. Откройте диспетчер служб Интернета. Для этого в Панели управления дважды щелкните значок **Администрирование** и выберите **Internet Information Services** (Диспетчер служб Интернета).
8. Разверните структуру папок до папки *имя\_локального\_компьютера*\Веб-узлы\Веб-узел по умолчанию\tsweb.
9. Щелкните папку tsweb правой кнопкой мыши и выберите команду **Свойства**.
10. В диалоговом окне **Свойства** выберите вкладку **Безопасность каталога**.
11. В группе **Анонимный доступ и проверка подлинности** нажмите кнопку **Изменить**.
12. В диалоговом окне **Методы проверки подлинности** установите флажок **Анонимный доступ** и дважды нажмите кнопку **ОК**.
13. Щелкните значок **Система** в Панели управления.
14. На вкладке **Удаленное использование** установите флажок **Разрешить удаленное подключение к этому компьютеру** и нажмите кнопку **ОК**.
15. В области **Дистанционное управление рабочим столом** нажмите кнопку **Выбрать удаленных пользователей**.
16. В диалоговом окне **Пользователи удаленного рабочего стола** нажмите кнопку **Добавить**.

#### **ПРИМЕЧАНИЕ**

Если единственным пользователем этого компьютера будет его администратор, то добавление пользователей не требуется.

17. В диалоговом окне **Выбор: пользователи** нажмите кнопку **Размещение**, чтобы указать область поиска.
18. Нажмите кнопку **Размещение**, чтобы указать размещение (если нет сетевых пользователей, то только локальные учетные записи).
19. Нажмите кнопку **Типы объектов**, чтобы указать типы объектов, поиск которых нужно выполнить.
20. В поле **Введите имена выбираемых объектов (примеры)** введите имена искомым объектов.
21. Нажмите кнопку **Проверить имена**.
22. Найдя имя, нажмите кнопку **ОК**. Теперь имя появится в списке пользователей в диалоговом окне **Пользователи удаленного рабочего стола**.
23. Убедитесь в наличии необходимых разрешений на удаленное подключение к данному компьютеру и нажмите кнопку **ОК**.

Теперь настроим компьютер, с которого хотим получить доступ.

Выполнение описанных далее процедур требуется не всегда. На одной из машин с Windows 98 оказалось достаточно ввести в строку адреса в браузере адрес машины для подключения, и необходимые компоненты установились автоматически с подключаемой машины. Но в справочной системе Windows такая процедура не описана, поэтому будем придерживаться рекомендуемой методики.

1. На компьютере, где установлена операционная система Windows 95, Windows 98, Windows NT 4.0 или Windows 2000, вставьте в дисковод установочный компакт-диск Windows XP Professional.
2. При появлении на экране страницы приветствия выберите ссылку **Выполнение иных задач**, а затем — вариант **Установка удаленного управления рабочим столом**.
3. Далее следуйте инструкциям на экране.

## Устанавливаем подключение к рабочему столу

### Вариант 1

Выполните следующие действия:

1. Удостоверьтесь, что выполнены все необходимые настройки компьютеров.
2. Убедитесь, что вы можете получить доступ к удаленному компьютеру. Для этого достаточно выполнить из окна командной строки команду

```
ping <IP-адрес удаленного компьютера>
```

#### **ПРИМЕЧАНИЕ**

Справочная система Windows XP говорит о необходимости применения в сети какого-либо метода определения имен, но это не обязательно, а иногда даже невозможно. Единственным неудобством в этом случае будет необходимость использования числового IP-адреса компьютеров вместо символического.

3. На компьютере, с которого получаете доступ, запустите программу Microsoft Internet Explorer.
4. В поле **Адрес** введите IP-адрес каталога tsweb удаленного компьютера (адрес задается в виде строки `http://<ip-адрес удаленного компьютера>/tsweb`) и нажмите клавишу <Enter>. На экран будет выведена страница "Интернет-подключение к удаленному рабочему столу".

#### **ПРИМЕЧАНИЕ**

Разумеется, что конкретное значение IP-адреса должно соответствовать адресу вашего компьютера. Адрес страницы можно сохранить в меню **Избранное** для ускорения доступа к ней в следующий раз.

5. В поле **Сервер** опять введите IP-адрес удаленного компьютера.  
При необходимости укажите размер экрана и сведения входа для подключения.
6. Нажмите кнопку **Подключить**.

### ПРИМЕЧАНИЕ

Для работы с программой **Интернет-подключение к удаленному рабочему столу** необходима программа Internet Explorer 4.0 или более поздней версии. Сама программа **Интернет-подключение к удаленному рабочему столу** может быть установлена на одном из доступных в сети компьютеров, например, на сервере, с которым обеспечена связь "удаленных рабочих столов".

## Вариант 2

Для подключения можно применять и программу **Подключение к удаленному рабочему столу**, которая является усовершенствованным аналогом "клиента служб терминалов" для Windows 2000 Server и может применяться вместо него.

1. Чтобы запустить программу **Подключение к удаленному рабочему столу**, нажмите кнопку **Пуск**, перейдите к пункту **Программы** или **Все программы | Стандартные | Связь** и выберите программу **Подключение к удаленному рабочему столу**. Для изменения параметров подключения (таких как размер экрана, сведения для автоматического входа и параметры производительности) перед подключением нажмите кнопку **Параметры**. Пролистав вкладки, можно настроить параметры отображения и управления удаленным рабочим столом. Для ускорения доступа в следующий раз на вкладке **Общие** нажмите кнопку **Сохранить как**, введите имя файла параметров подключения и нажмите кнопку **Сохранить**. В поле **Компьютер** задайте имя удаленного компьютера (если есть служба определения имен) или его IP-адрес.
2. Нажмите кнопку **Подключить**.
3. Откроется диалоговое окно **Вход в Windows**.

В диалоговом окне **Вход в Windows** введите имя пользователя, пароль и домен (если требуется), а затем нажмите кнопку **ОК**.

### ПРИМЕЧАНИЕ

Подключения сохраняются в файлы удаленного рабочего стола (с расширением gdr). Файл с расширением gdr содержит все сведения о подключении к серверу терминалов, включая параметры, введенные на вкладке **Параметры** при сохранении файла. Пользователь имеет возможность создать любое количество gdr-файлов, включая файлы подключения к одному и тому же серверу с разными настройками. Например, имеется возможность сохранить файл подключения в полноэкранном режиме и файл подключения с размером экрана 800×600. Файлы gdr по умолчанию сохраняются как скрытые в папке Мои документы. Для редактирования gdr-файла и изменения содержащихся в нем параметров подключения щелкните файл правой кнопкой мыши и выберите команду **Изменить**.

## Рекомендации

Таким образом, вы имеете два способа подключения к рабочему столу удаленного компьютера, для систем с Windows 9x предпочтительней вариант с браузером, для Windows XP — вариант с программой **Подключение к удаленному рабочему столу**. Но это мое субъективное мнение.



При подключении к удаленному рабочему столу машины, включенной в доменную сеть (зарегистрированную на сервере и настроенную для работы в сети), текущий сеанс пользователя блокируется. Если компьютер имеет локальный режим работы, но физически включен в сеть (аналог работы в Интернете), то текущий сеанс становится неактивным, а все запущенные программы продолжают работать. Пользуясь этим свойством, вы можете подключаться к рабочему столу удаленного компьютера под разными именами и запускать не связанные друг с другом программы, причем без риска случайного закрытия одной из них.

По завершении работы с удаленным рабочим столом у вас есть выбор. Можно закрыть сеанс работы с рабочим столом, а можно просто отключиться от него. При этом все программы будут продолжать работать.

Настраивая параметры доступа, можно минимизировать трафик и успешно работать при не слишком быстрой связи (модем). Некоторая медлительность связи будет скомпенсирована самой возможностью подключаться к своему компьютеру, находящемуся в десятках километров от вас.

Придется, правда, настроить сервер удаленного доступа. В справочной системе операционной системы Windows XP рассматривается подключение удаленного доступа к рабочему месту по телефонной линии. Чтобы создать подключение удаленного доступа к рабочему месту по телефонной линии:

1. Нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, затем дважды щелкните значок **Сетевые подключения**.
2. В группе **Типичные задачи** щелкните ссылку **Мастер сетевого подключения** и затем нажмите кнопку **Далее**.
3. Выберите вариант **Подключить к сети на рабочем месте** и нажмите кнопку **Далее**.
4. Выберите переключатель **Подключение удаленного доступа**, нажмите кнопку **Далее** и следуйте указаниям мастера нового подключения.

Удаленный доступ к компьютеру обеспечивается службой **Диспетчер автоподключений удаленного доступа**, которая запускается по умолчанию на компьютерах Windows XP Professional, не являющихся членами доменов, а также в Windows XP Home Edition. Если ваш компьютер включен в домен, или Диспетчер автоподключений удаленного доступа отключен по другой причине, его не трудно включить. Чтобы запустить Диспетчер автоподключений удаленного доступа:

1. Откройте последовательно **Панель управления | Администрирование | Управление компьютером | Службы и приложения | Службы**.
2. В правой панели окна **Управление компьютером** щелкните правой кнопкой мыши службу **Диспетчер автоподключений удаленного доступа** и выберите команду **Запустить**.
3. В столбце **Состояние** появится пометка **Работает**.

Windows XP позволяет управлять своими службами из командной строки. Это позволяет подключать к Интернету удаленный компьютер по расписанию. Для запуска и остановки службы **Диспетчер автоподключений удаленного доступа**

достаточно в BAT-файл включить команду `sc start RasAuto` или `sc stop RasAuto`. При этом, если ваш компьютер настроен и на прием факсов, а модем не может отличить попытку удаленного доступа от передачи факса, можно управлять и службой Fax, применив команды `sc start Fax` и `sc stop Fax`. Надо сказать, что в Windows XP практически все службы допускают управление из командной строки. Возможна автоматизация процессов вызова и приема вызова компьютером. Для включения вызова по телефону можно использовать команду `rasdial` с параметрами, которые можно узнать в справке по команде. Команда `rasdial`, выполненная без параметров, показывает состояние текущих подключений.

## Настраиваем рабочую станцию с динамическим IP-адресом

В этом случае остается выполнить совсем немного действий.

1. Зайдите на страницу <http://www.dyndns.com/>. Это страница созданной в 1998 году службы DynDNS (Dynamic Network Services, Inc., динамический сетевой сервис). Зарегистрируйтесь в этой службе (регистрация совершенно бесплатна). Запомните имя входа и пароль! Для своей учетной записи (**Account**) в сервисе Dynamic DNS создайте домен, например с именем *<любое\_имя>.homeip.net*.

Возможны и другие имена доменов, вам будет предложен выбор.

2. Скачайте со страницы <https://www.dyndns.com/support/clients/> или <http://www.kanasolution.com/> программу DynDNS Updater — программа-клиент, которая сможет регулярно сообщать сервису текущий IP-адрес вашего компьютера. По первой ссылке также доступен клиент для Linux.
3. Установите эту программу и подключитесь к сервису (потребуется данные регистрации).
4. После этого останется не забывать, что вы подключены к этому сервису. Через какой-то период вашей неактивности вашу учетную запись могут заблокировать.

Интересна еще одна возможность, которую предоставляет этот сервис.

Ряд провайдеров закрывают многие распространенные порты для входа на ваш компьютер. Но только распространенные, а другие остаются открытыми. Вы можете зарегистрировать услугу WebHop, которая позволит перенаправить подключение со стандартного порта на тот, который вы сами выберете. Это может быть удобно для организации Web-сайта, например, на подключенном через такого провайдера компьютере.

Сайт имеет только англоязычную версию, поэтому тот, кто плохо знаком с этим языком, столкнется с дополнительными трудностями в переводе информации на сайте. Но труд будет вознагражден!

## Доступ к удаленному рабочему столу Linux

Некоторые операционные системы не имеют штатных средств доступа к рабочему столу, например, домашние версии Windows. В состав ОС Linux обычно входит клиент доступа к удаленному рабочему столу Windows, что позволяет с успехом применять рабочую станцию Linux для администрирования сервера Windows. Но нам хотелось бы получить доступ к нашим компьютерам домашними версиями Windows и Linux. После достаточно продолжительных поисков и подбора программ автору удалось найти почти универсальное решение. Таким решением оказалась известная многим, но существующая во множестве версий VNC (Virtual Network Computing — система удаленного доступа к рабочему столу с открытым исходным кодом).

Задача состояла в том, чтобы подобрать пару клиент-сервер, которые можно было бы использовать и на Windows, и на Linux, да так, чтобы качество изображения рабочего стола было нормальным и можно было осуществить обмен файлами. Оказалось, что программа UltraVNC (<http://sourceforge.net/projects/ultravnc>) последних версий поддерживает работу с Windows Vista и Windows 7, имеет средства обмена файлами и текстовой информацией (чат).

При этом во многие дистрибутивы Linux входит программа X11VNC. Это VNC-сервер, совместимый с UltraVNC, которая существует только для Windows. Автору не удалось заставить работать чат между Windows Vista и Linux, но передача файлов работает отлично. Таким образом удалось связать все компьютеры домашней сети автора и получить к ним доступ из Интернета. Установка программ не вызывает трудностей, поэтому коротко рассмотрим работу с упомянутыми программами.

Для того чтобы получить доступ к домашнему компьютеру под управлением Linux из Интернета, на этот компьютер был установлен клиент DynDNS для Linux Inadyn, доступный для загрузки по адресу в Интернете <http://cdn.dyndns.com/inadyn.zip>. Впрочем, если в вашей сети несколько компьютеров и есть машины под управлением Windows, можно обойтись и Windows-клиентом, ведь внешний IP-адрес для всех компьютеров сети один и тот же. В любом случае маршрутизатор должен быть настроен на перенаправление портов, используемых UltraVNC и X11VNC на внутренний IP-адрес компьютера, на котором они установлены. Как вариант, для обеспечения доступа к компьютеру через Интернет можно применить и кроссплатформенную программу и сервис Hamachi, создающие VPN-канал между компьютерами (см. главу 4).

Итак, на компьютере с ОС Windows Vista установлена UltraVNC Viewer, и компьютер подключен к Интернету, а на домашней машине с Mandriva Linux установлены и запущены X11VNC и клиент DynDNS, Firewall настроен для свободного доступа по порту 5900. Маршрутизатор, через который домашняя сеть подключена к Интернету, перенаправляет пакеты по порту 5900 на IP-адрес домашнего компьютера.

X11VNC должна быть запущена командой `x11vnc -usepw -scale 2/2 -forever -ultrafilexfer -permitfiletransfer`, которая может быть помещена в значок запуска на рабочем столе, а Inadyn командой `/bin/linux/inadyn --input_file /etc/`

inadyn.conf, которая также может быть помещена в значок запуска. При этом значок запуска настраивается для запуска приложения в окне терминала.

Запускаем UltraVNC Viewer (рис. 22.8).

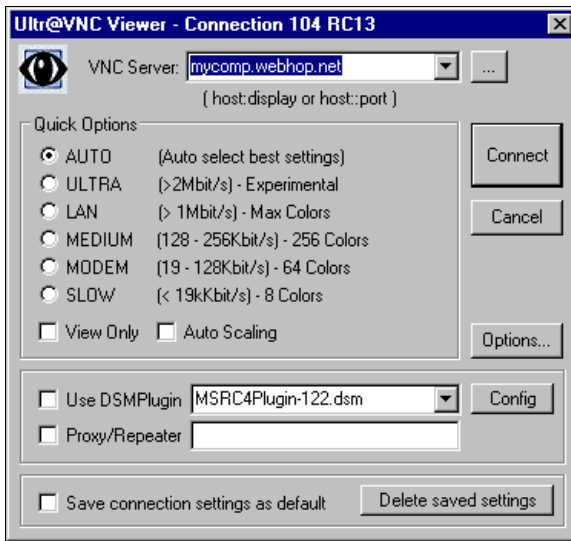


Рис. 22.8. Окно UltraVNC Viewer

В раскрывающийся список **VNC Server** вводим адрес домашнего компьютера, который назначен в сервисе DynDNS, и нажимаем кнопку **Connect**.

В появившемся окне ввода пароля вводим заранее установленный в приложении X11VNC пароль. И через несколько мгновений откроется окно UltraVNC-сервера с изображением рабочего стола удаленного компьютера (рис. 22.9).

Если весь рабочий стол удаленного компьютера не умещается в окне и это вызывает неудобство в работе, то можно, нажав третью кнопку на панели под заголовком окна, вызвать окно **Connection Options**, в котором в разделе **Display** в раскрывающемся списке **Viewer Scale: by** установить уменьшение изображения рабочего стола в процентах (рис. 22.10).

Мы говорили, что на домашнем компьютере запущены приложения X11VNC и Inadyn. Окна, в которых видна работа этих приложений, были помещены на второе рабочее место (Linux позволяет по умолчанию использовать четыре рабочих места). Щелкнув мышью по значку этого рабочего места в нижней части рабочего стола удаленного компьютера, можно переключиться на него и посмотреть сообщения запущенных программ (рис. 22.11).

#### ПРИМЕЧАНИЕ

Не закрывайте эти окна, чтобы не остановить работу программ, обеспечивающих связь с компьютером! Лучше в удаленном режиме не использовать рабочее место, где они находятся.

Теперь вы можете работать как на локальном, так и на удаленном компьютере. Дистрибутив UltraVNC вы можете носить с собой на флэшке. Это позволит полу-

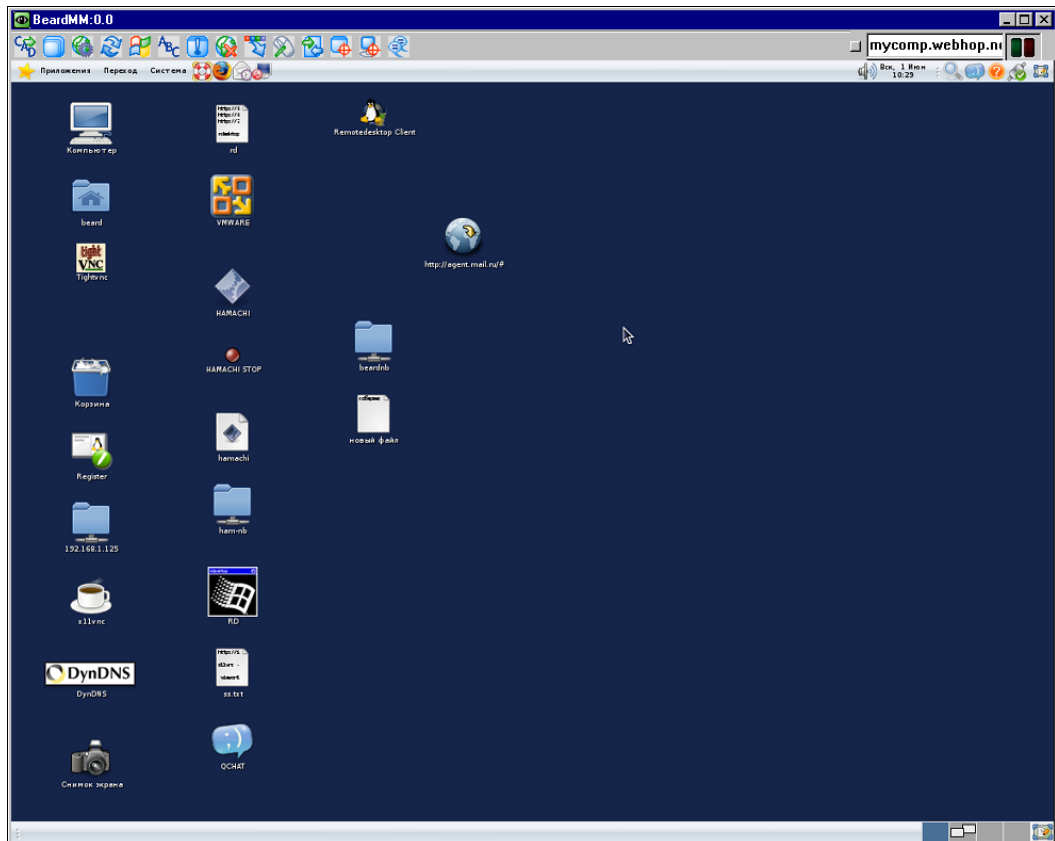


Рис. 22.9. Окно UltraVNC Server — рабочий стол удаленного компьютера

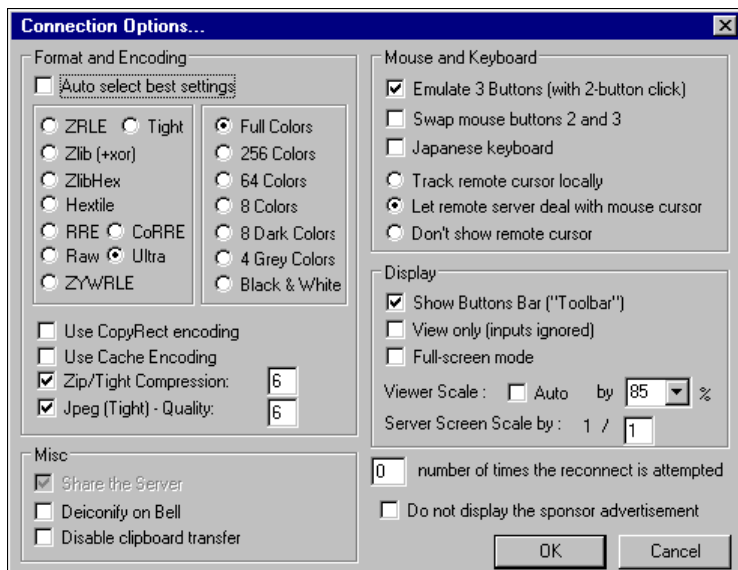


Рис. 22.10. Окно Connection Options UltraVNC-сервера

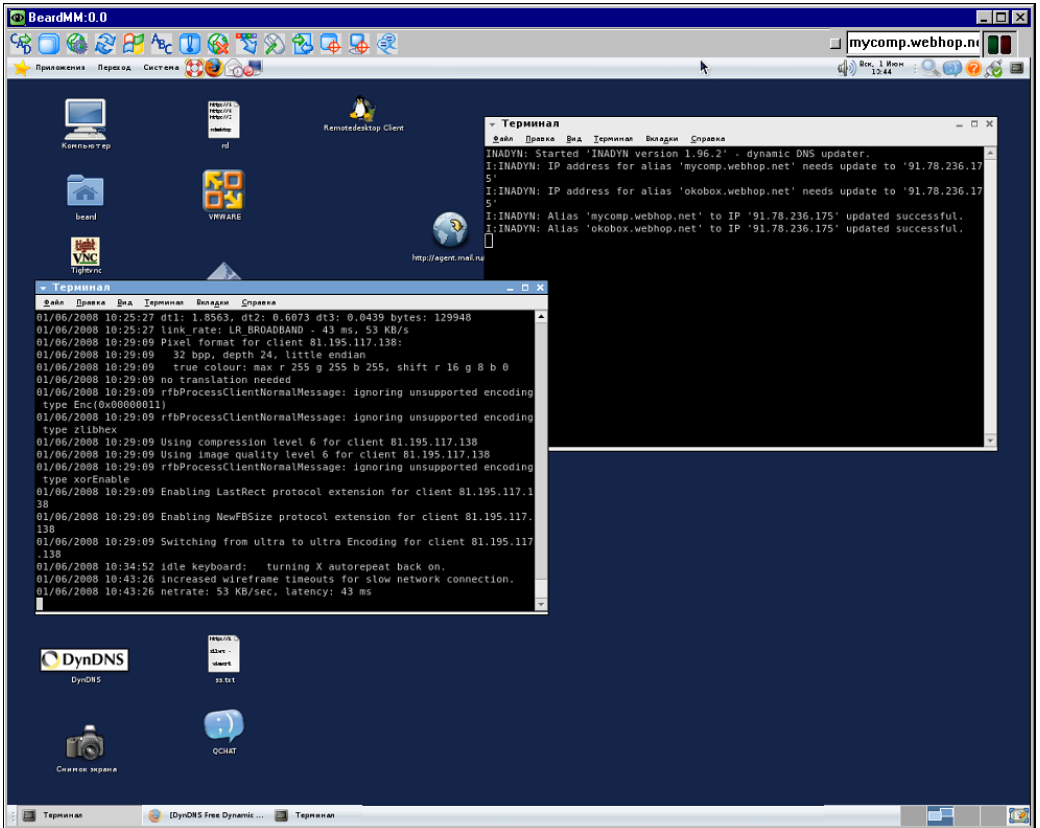


Рис. 22.11. Окно UltraVNC Server — рабочий стол удаленного компьютера (рабочее место № 2)

чать доступ к своему компьютеру из любой точки земного шара, где есть компьютер, подключенный к Интернету. Одиннадцатая кнопка на панели под заголовком окна вызывает окно **File Transfer** (обмен файлами), с помощью которого можно перемещать и копировать файлы между компьютерами. При подключении к компьютеру под управлением Linux не работает чат. Но этот недостаток можно легко обойти, создав текстовый файл на удаленном компьютере и поместив в него ваши сообщения, если в этом есть необходимость. Можно использовать и программы для обмена текстовыми сообщениями через Интернет, часть из которых описана в *приложении 1*. Желательно отключить на удаленном компьютере заставку (хранитель экрана), чтобы не ждать прорисовки заставки после перерыва в работе.

Возможно, вас заинтересует возможность доступа к Windows-компьютерам через сервис LogMeIn (<https://secure.logmein.com/>). Сервис позволяет подключаться к компьютерам, имеющим выход в Интернет, используя промежуточный сервер. Правда, сервис не позволяет подключаться к компьютерам под управлением Linux, но к машинам с ОС Windows можно подключаться с Linux-машин.

## Подключение к компьютеру с помощью LogMeIn

Описанный ранее способ подключения к удаленному компьютеру для управления им требует предварительной подготовки в виде регистрации на сайте DynDNS и/или настройки OpenVPN, применения Natchi, настройки маршрутизаторов, брандмауэров и файрволов, если они применяются. Но в Интернете есть сервисы, которые могут обеспечить работу на удаленном компьютере после регистрации и установки программного обеспечения на компьютер, к которому будет осуществляться доступ. На компьютере, с которого выполняется подключение, никаких программ устанавливать не надо. Подключение выполняется через интернет-браузер, поддерживающий работу с Java. Компьютер, к которому выполняется подключение, должен быть под управлением Windows. Подключаться можно и с компьютера под управлением Linux.

Зарегистрироваться и загрузить программу на управляемый компьютер можно с сайта <https://logmein.com/home.asp?lang=ru>.

Для подключения к удаленному компьютеру необходимо выполнить следующее:

- Зайти на сайт <https://logmein.com> и ввести свои учетные данные.
- Попад на страницу пользователя, выбрать управляемый компьютер (рис. 22.12).

The screenshot shows a web browser window displaying the LogMeIn website. The browser's address bar contains the URL <https://secure.logmein.com/computers.asp>. The website's header includes the LogMeIn logo and navigation links such as 'Компания', 'Продукты', 'Цены', 'Поддержка', 'Лэбс', 'Контакты', and a language selector set to 'Русский'. The main content area is titled 'Мои компьютеры' (My Computers) and features a sidebar with links for 'Мои компьютеры', 'Учетная запись', 'Купить подписку', and 'Ресурсы'. A central message box states: 'Благодарим за подписку на LogMeIn Free. В качестве дополнительного бонуса вы получите бесплатную пробную версию LogMeIn Pro с дополнительными функциями. Ознакомительный срок длится 30 дней или 2 полных часа использования (в зависимости от того, что закончится раньше). По окончании срока использования вы можете обновить программу до версии LogMeIn Pro или перейти на использование LogMeIn Free. Автоматически откроется окно запроса, и вам необходимо будет сделать выбор.' Below this, there is a table listing computers, with one entry: 'BEARD-NB'. At the bottom right, contact information is provided: 'Поддержка: +36-1-462-6028' and 'Отдел продаж: +36-1-462-6028'. The footer contains the copyright notice: 'Copyright © LogMeIn, Inc., 2003-2008. Все права защищены. Юридическая информация'.

Рис. 22.12. Рабочий стол Mandriva Linux — страница пользователя LogMeIn

- На открывшейся странице меню пользователя (рис. 22.13) LogMeIn выбрать требуемое действие.

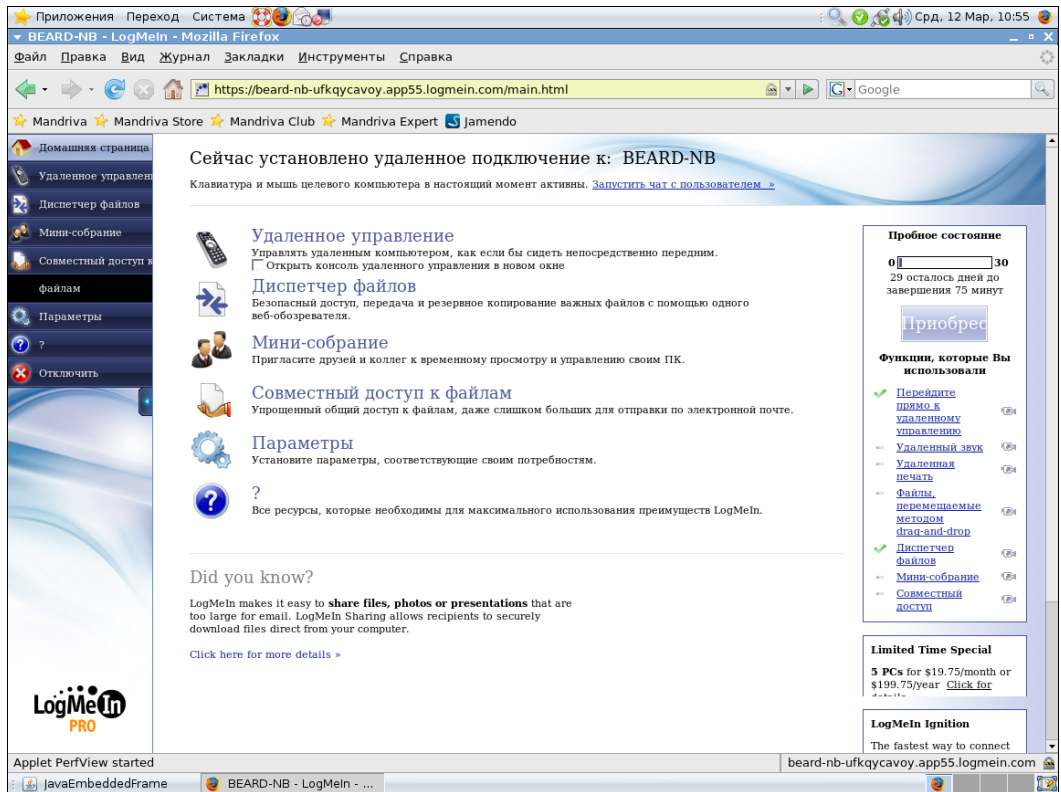


Рис. 22.13. Рабочий стол Mandriva Linux — меню пользователя LogMeIn

При выборе удаленного управления в окне браузера откроется рабочий стол удаленного компьютера (рис. 22.14).

Из этого окна можно открыть файловый менеджер, в двух окнах которого видны файлы локального и удаленного компьютера, выбрав в меню **Диспетчер файлов** (рис. 22.15), или инициировать чат с удаленным пользователем (рис. 22.16).

Посредством LogMeIn можно организовать удаленную помощь пользователям компьютеров под управлением Windows.

Конечно, хорошо когда не надо выполнять дополнительные настройки для подключения к удаленному компьютеру. Но рассмотренная программа в бесплатном варианте позволяет только два часа использовать дополнительные возможности, а затем потребуются оплачивать каждый месяц или довольствоваться только подключением к рабочему столу. Настроив же OpenVPN и применив UltraVNC, можно подключаться и к компьютерам под управлением Linux, передавать файлы по виртуальной сети. А общение с пользователями Linux возможно через программы мгновенных сообщений. Вместо оплаты достаточно приложить немного своих усилий для настройки удаленного доступа.



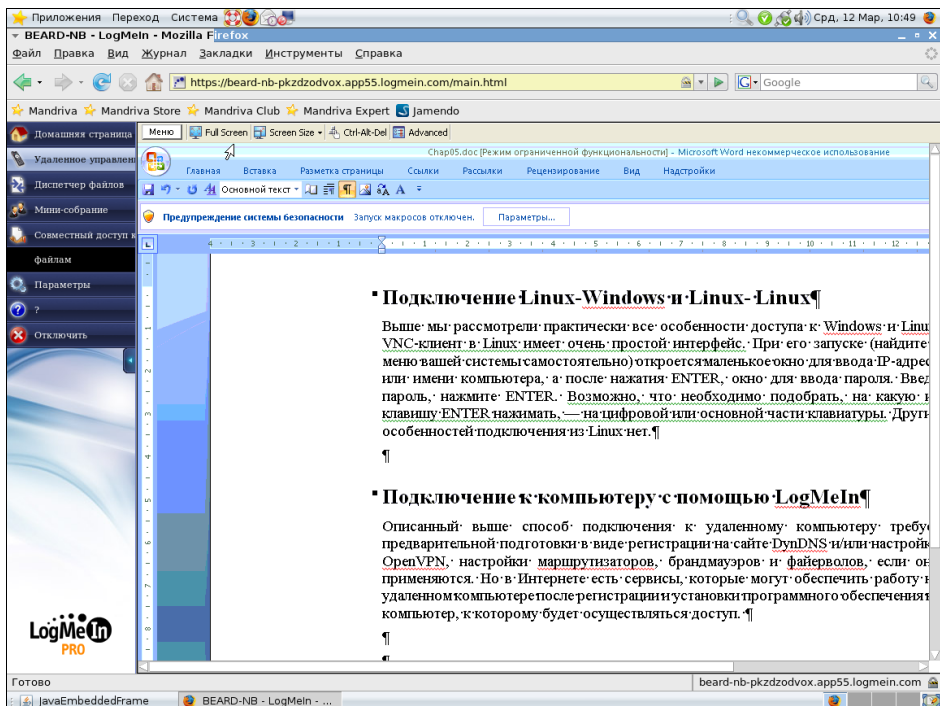


Рис. 22.14. Рабочий стол Mandriva Linux — документ, открытый на удаленном компьютере

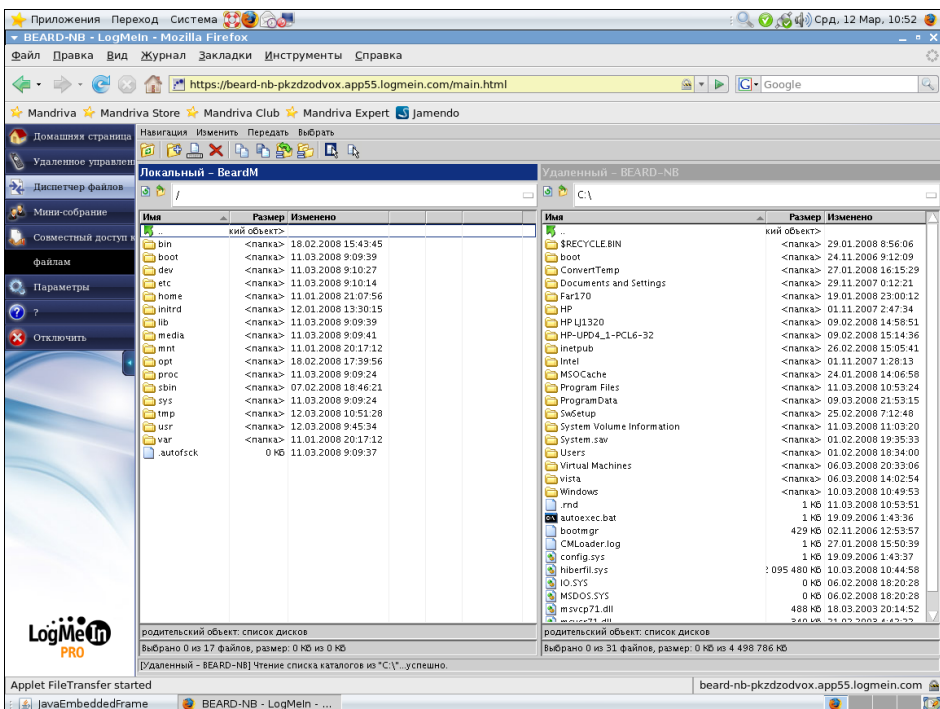


Рис. 22.15. Рабочий стол Mandriva Linux — страница файлового менеджера

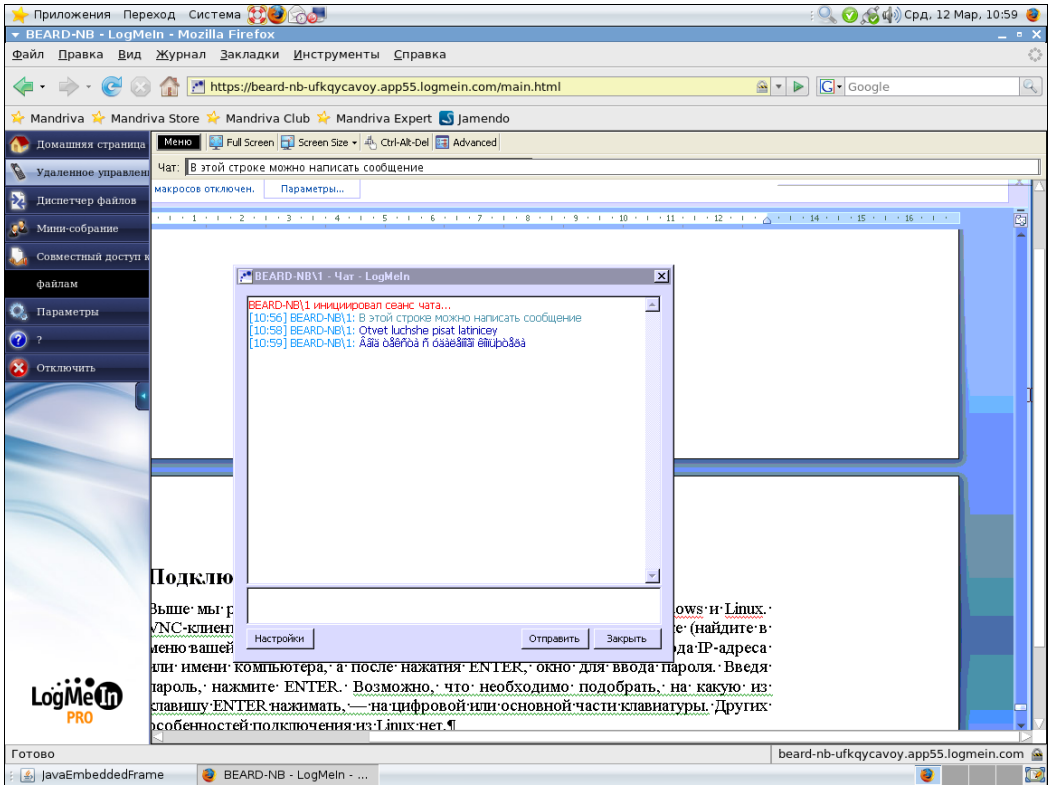


Рис. 22.16. Рабочий стол Mandriva Linux — чат с удаленным пользователем

Если вы заинтересовались вопросом удаленного доступа к компьютеру, то можете самостоятельно ознакомиться с другими средствами. На странице в Интернете <http://networkforpeople.blogspot.com/2007/10/40.html> описано более сорока способов удаленного доступа. После написания этой статьи появились и другие программы, например Teamviewer (<http://www.teamviewer.com/>). Эта программа должна быть установлена на оба компьютера, других настроек она не требует, но бесплатно проработает месяц или 25 часов.

Практически все программы для удаленного управления рабочим столом через Интернет используют какие-либо дополнительные сервисы. Именно за их использование и надо платить. Но самостоятельно выполняя необходимые настройки и используя бесплатный сервис DynDNS и/или программу OpenVPN, вы можете настроить бесплатный и неограниченный доступ к своему компьютеру независимо от того, какая ОС установлена на нем.

## ГЛАВА 23



# Подсчитываем трафик

Эта задача может возникать в сети любого уровня и даже на отдельно стоящем компьютере. Необходимость учета *трафика*<sup>1</sup> (traffic), использованного как всей сетью, так и отдельными пользователями может быть вызвана разными причинами. Это и учет долей оплаты за использованный трафик, и учет нагрузки на сеть, оптимизация нагрузки по часам суток и дням недели, обнаружение проблем в системе сетевой безопасности, и... Каждый администратор, столкнувшись с необходимостью учета сетевого трафика, понимает для чего это ему надо. Поэтому в данной главе мы просто рассмотрим один из способов учета трафика. На самом деле таких способов довольно много. Многие из них недоступны пользователям малых сетей ввиду дороговизны или сложности реализации. Но существуют относительно недорогие и достаточно простые в использовании программы учета трафика в сети, с одной из которых мы и познакомимся. Называется она BWMeter (<http://www.desksoft.com/BWMeter.htm>).

Для корректного учета трафика Интернета необходимо, чтобы весь этот трафик проходил через сетевые адаптеры, доступные программе. А это значит, что должен быть компьютер, который исполняет роль шлюза в Интернет для всей сети. Если подключение к Интернету выполнено через модем-маршрутизатор D-Link 500T или подобный, то учет трафика необходимо будет делать на каждом компьютере, подключенном к этому шлюзу. Правда, программа имеет средства удаленного контроля. Установив программу на несколько компьютеров, можно контролировать трафик с одного из них.

## Возможности программы BWMeter

Прежде всего, хочется отметить возможности программы:

- учет трафика раздельно по каждому сетевому интерфейсу;
- учет трафика клиентов сети по каждому IP-адресу или по MAC-адресу;

---

<sup>1</sup> Объем информации, передаваемой по сети за определенный период времени.

- ❑ ограничение исходящего и/или входящего трафика для каждого фильтра;
- ❑ создание исключений в фильтрах, что позволяет запретить трафик для всех, но разрешить для отдельных клиентов;
- ❑ вывод на экран графической информации об использовании трафика по каждому фильтру. Если фильтров много, есть возможность выводить информацию на экран только при наличии сетевой активности клиентов;
- ❑ вывод на экран и экспорт в файл отчетов о расходе трафика за любой период и для любых выбранных фильтров с разбивкой информации по часам, дням, неделям или месяцам;
- ❑ блокирование трафика или снижение скорости клиента при перерасходе за заранее заданный период;
- ❑ учет трафика по MAC-адресам позволяет исключить подмену IP-адреса клиентом для обхода контроля.

Программа может работать в качестве службы. Но этот режим есть смысл применять, когда установлен удаленный контроль статистики.

Если программа установлена на сервере, к которому возможны терминальные подключения, следует отключить автозапуск программы при входе в систему. Два экземпляра программы на одном компьютере могут конфликтовать.

В программе не предусмотрена возможность финансового учета. Если это необходимо, то придется расчеты выполнять вручную, экспортировав отчеты в Excel. Конечно, продвинутые пользователи могут написать макрос в Excel, который будет выполнять эти расчеты.

Есть ограничение на число исключений в одном фильтре. Обычно их удается ввести не более пятнадцати. Для обхода этого лимита фильтры должны содержать ограниченное число контролируемых адресов, а самих фильтров должно быть несколько. Например, каждый фильтр может учитывать трафик для диапазона из пятнадцати IP-адресов, что позволит включать в исключения даже все адреса фильтра. На практике обычно достаточно иметь диапазоны по пятьдесят адресов, что в обычных локальных сетях достаточно удобно.

Словом, для небольшой локальной сети программа подходит почти идеально.

## Настраиваем программу

После установки программа сама пытается определить интерфейсы, подключенные к локальной сети и к Интернету. Но это ей не всегда удается сделать корректно. Поэтому может оказаться необходимым удалить информацию об интерфейсах, определенную программой, и вручную указать верную.

На рис. 23.1 показано окно реально работающей программы, в которой контроль трафика установлен только по одному интерфейсу, принадлежащему локальной сети. Интерфейс, выходящий в Интернет, контролировать нет необходимости, поскольку это сервер, и на нем никто не работает. На этой вкладке указано так же, что значок программы должен находиться в системном лотке (флажок **Show BWMeter tray icon**), указан IP-адрес локальной сети (**IP addresses of local network**).

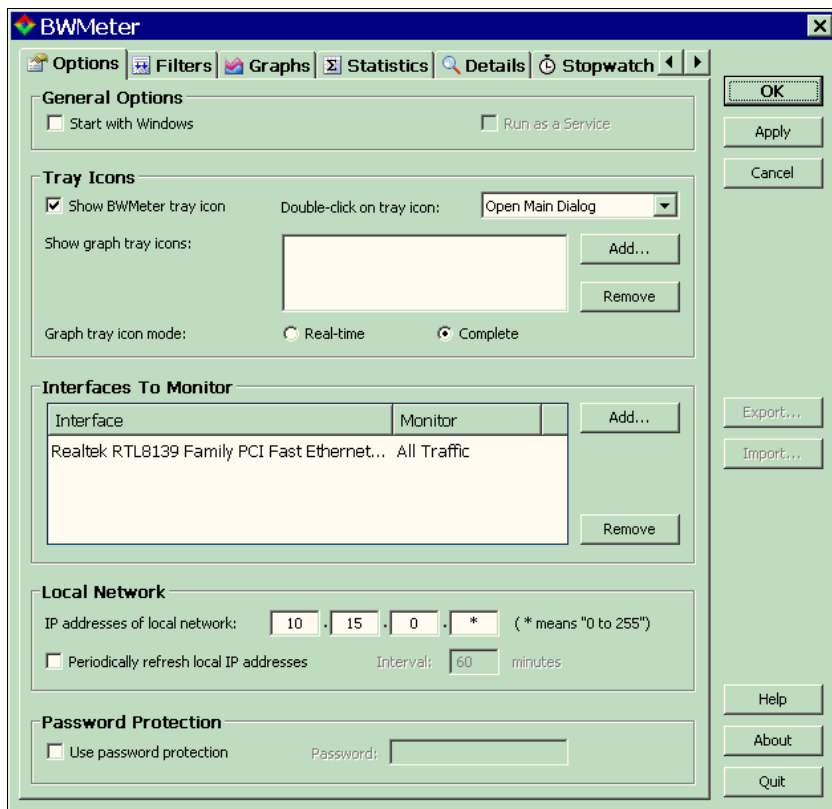


Рис. 23.1. Окно BWMeter, вкладка Options

Вкладка **Filters** позволяет настроить фильтры (рис. 23.2). На рисунке видны как диапазонные фильтры, включающие по пятьдесят адресов, так и индивидуальные. Диапазонные фильтры настроены на запрет трафика (флажок **Stop traffic**), а индивидуальные на его контроль. Для того чтобы это было возможно, MAC-адреса клиентов, для которых созданы разрешающие фильтры, включены в исключения (exclude) диапазонного фильтра. Настройка фильтров может быть выполнена очень гибко, для этого в программе предусмотрено очень много параметров.

На вкладке **Graphs** можно для каждого фильтра настроить режим отображения на экране (рис. 23.3). Естественно, что для запрещающих фильтров настраивать нечего, ведь трафик, контролируемый ими, всегда нулевой. А для разрешающих фильтров можно настроить несколько параметров, включая порог активности, начиная с которого график фильтра будет показан на экране.

На вкладке **Statistics** (рис. 23.4) можно посмотреть статистику работы клиентов, а так же экспортировать данные в файл для сохранения и отчетности.

На вкладке **Details** (рис. 23.5) есть возможность просмотра адресов Интернета, к которым клиент подключается. Эта полезно для выявления "нехороших" адресов. После их обнаружения можно установить фильтрацию средствами сервера. Адреса станут недоступными из сети.

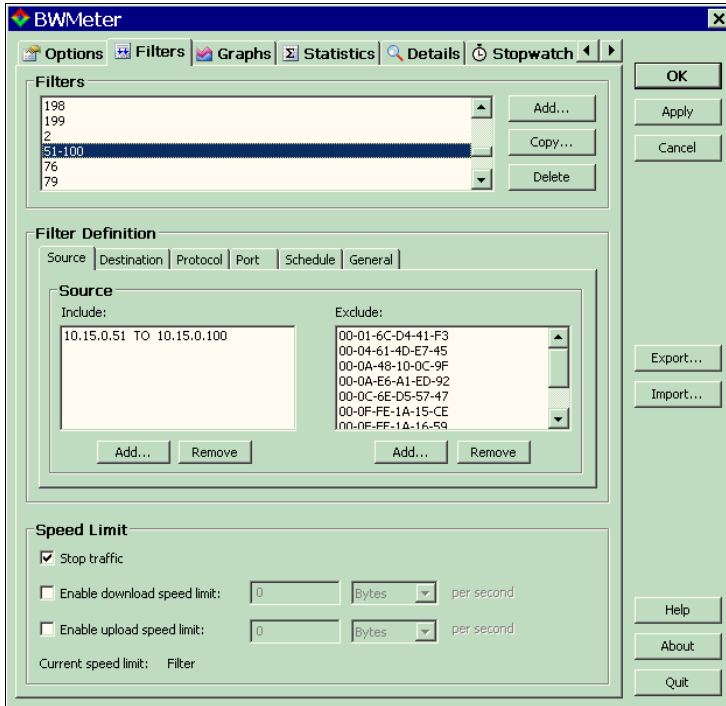


Рис. 23.2. Окно BWMeter, вкладка Filters

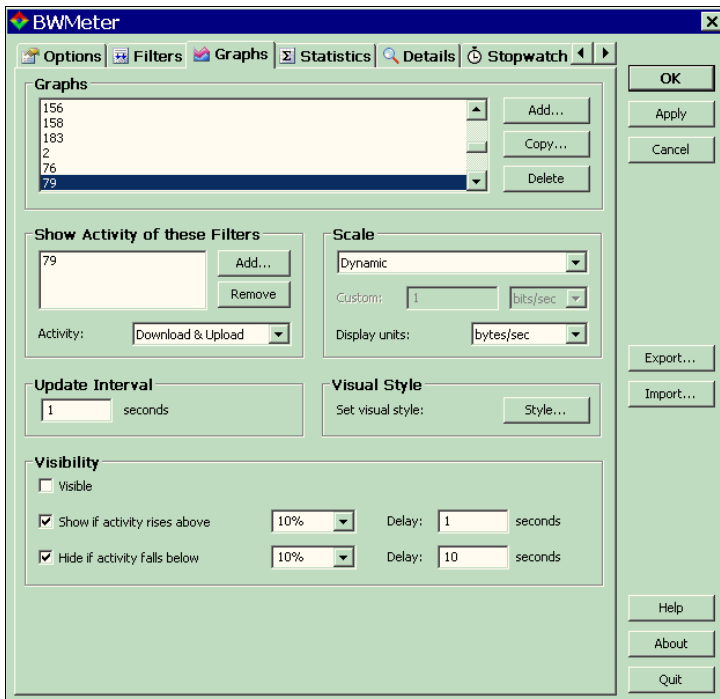


Рис. 23.3. Окно BWMeter, вкладка Graphs

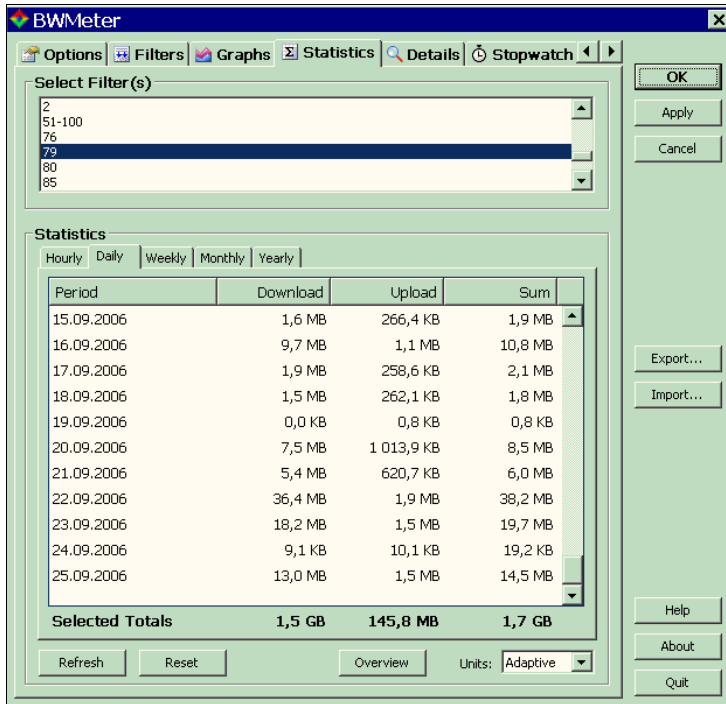


Рис. 23.4. Окно BWMeter, вкладка Statistics

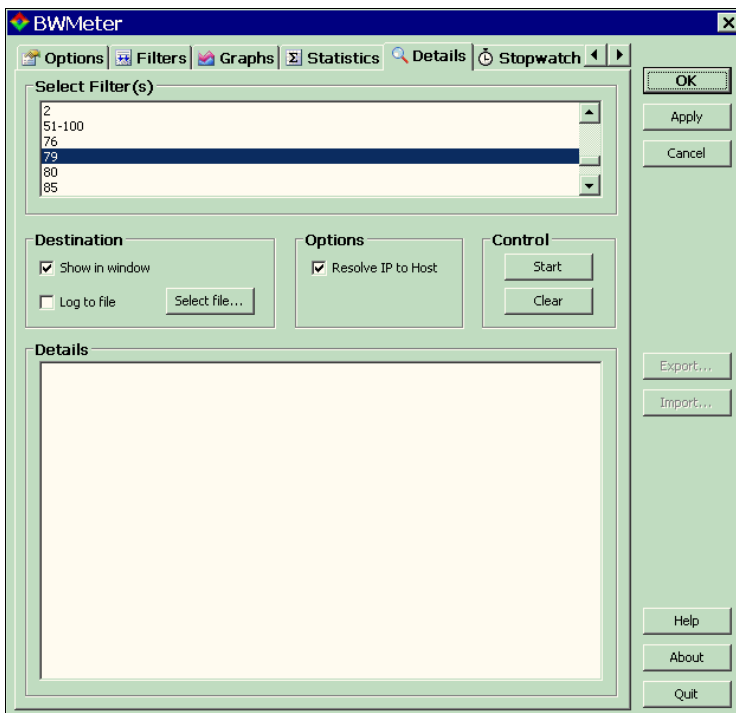


Рис. 23.5. Окно BWMeter, вкладка Details

Есть еще несколько вкладок, которые могут оказаться полезными для вас, а могут никогда и не пригодиться. Компактность программы обманчива. Начав в ней разбираться, вы можете потратить несколько часов для того только, чтобы рассмотреть все ее возможности. У программы есть справочная система, которая может помочь в сложной ситуации. Но в большинстве случаев, если вы знаете, чего хотите от программы, то без труда найдете необходимые настройки.

## Ссылки

Описание BWMeter и других программ подобного назначения можно найти по адресу <http://www.grani.ru/Techno/m.77220.html>. Некоторые ссылки из этой статьи устарели, и описание таких программ ищите через систему поиска по имени программы.

Существуют и специализированные биллинговые системы для домашних и офисных систем. Есть даже бесплатные, но они рассчитаны на работу с ОС Linux или FreeBSD, хотя клиентами могут быть и Windows-машины. Их возможности шире, с их помощью можно проводить финансовый учет и предоставлять соответствующую информацию клиентам. Для их работы требуется установка клиентской части программы на машину клиента. Одна из таких систем — StarGazer, о которой можно подробно узнать и даже скачать ее по ссылке <http://stargazer.dp.ua/doc.php>.

Ну вот, пожалуй, и все. Информации, приведенной в книге, должно быть достаточно, чтобы создать простую сеть, или сети и получить возможность доступа к ним из Интернета. Рассмотрены средства, повышающие удобство администрирования сетей, удаленного управления своими компьютерами под управлением Windows и Linux. Большинство средств практически бесплатны. В приложениях вы можете ознакомиться с дополнительной информацией, которая будет полезна при создании своих сетей и обеспечении доступа к ним.





# ПРИЛОЖЕНИЯ



# ПРИЛОЖЕНИЕ 1

## Общение через домашнюю сеть и Интернет

Настроив подключение к Интернету и подключение к телефонной линии, вы можете использовать возможности связи с людьми в сети и по всему миру. Часть средств, предназначенных для связи, существует как в ОС Windows, так и в Linux, другую часть можно получить через Интернет. Используя возможности связи через Интернет, вы сможете найти много новых знакомых и друзей, возможность найти интересную работу или подработку. Интернет объединяет людей, помогает найти единомышленников. И в локальной сети нередко требуются средства общения пользователей. Если сеть подключена к Интернету, множество программ, предназначенных для общения через Интернет, можно применить и для общения внутри сети. Описанные далее средства не являются необходимыми для локальной сети, но могут существенно повысить комфортность работы в ней.

### Средства связи

Еще до изобретения компьютера человек получил в свое распоряжение средства связи. Это была обычная почта, затем телеграф и радио. Для того чтобы воспользоваться услугами почты, требуется написать письмо, положить его в почтовый ящик и ждать, когда его доставят получателю, который в свою очередь напишет ответ вам. Обмен сообщениями может занять не одну неделю. Телеграмма доходит до получателя существенно быстрее, но тоже не мгновенно. Беседа с помощью телеграфа может затянуться на несколько дней. Радиосвязь на большие расстояния возможна при наличии специального оборудования и разрешений на ее использование. Конечно, есть еще телефон, факсимильные аппараты. Эти средства повышают оперативность отправки и получения информации, но тоже имеют определенные ограничения.

Персональный компьютер позволяет снять практически все ограничения и получить возможность практически моментальной связи с друзьями, родственниками или сотрудниками.

Рассмотрим средства связи, которые нам может предоставить компьютер с операционной системой Windows Vista.

## Факс в Windows

Персональный компьютер, дополненный обычным модемом, позволяет передавать и получать *факсимильные сообщения*, не приобретая факсимильный аппарат, не расходуя бумагу. Компьютерные технологии предоставляют возможность обойтись без бумаги во многих случаях, и только консерватизм нашей бюрократической машины нередко заставляет все же печатать бумажные документы, несмотря на то, что реальной необходимости в этом уже нет.

Неужели вы не доверяете электронному документу, полученному от вашего друга? Бывает, конечно, и такое. Но даже в этом случае вы можете воспользоваться *электронной подписью*. Пока для обычных пользователей применение электронной подписи может быть не очень простой задачей. Происходит это только потому, что электронная подпись еще не стала стандартной, программное обеспечение для использования электронной подписи еще имеет много версий. Но автор уверен, что пройдет совсем немного времени и электронная подпись станет таким же обычным атрибутом каждого электронного документа. Общение же друзей, основанное на доверии, не требует электронной подписи, подлинность которой должна быть подтверждена специальными службами, поэтому в данной книге технологии электронной подписи мы рассматривать не будем. Вы сами сможете найти материалы по этому вопросу и скачать необходимые программы, когда освоитесь в Интернете, когда поиск информации для вас перестанет быть сложной задачей.

Итак, мы доверяем нашим корреспондентам, а они доверяют нам, и мы хотим обменяться факсимильными сообщениями.

Модем мы подключили и установили, при необходимости, соответствующий драйвер модема. Автор использует старый Courier Robotics, для которого уже давно не выпускают новых драйверов, но Windows Vista позволяет его использовать в качестве стандартного модема, драйвер которого есть в составе самой системы.

Для отправки факса надо настроить программу Факсы и сканирование Windows. Настоящие факсимильные сообщения требуют наличие бумажного оригинала. В этой программе предусмотрена возможность сканировать оригинал, если он есть. Но если у вас нет сканера, то можно просто создать новый документ и отправить его.

Рассмотрим работу с программой подробнее. Окно программы показано на рис. П1.1.

При первом запуске программы (**Пуск | Все программы | Факсы и сканирование Windows**) она попросит вас создать **Учетную запись факса**. Если во время работы мастера вы не сориентировались и отменили его работу, то можно создать учетную запись, выбрав в меню программы **Сервис | Учетные записи факсов**. Для создания учетной записи (рис. П1.2) требуется только подключенный аналоговый модем.

Соображения этики требуют, чтобы получатель видел сведения об отправителе факсимильного сообщения. Для того чтобы не вносить их при каждой отправке факса, следует заполнить форму (рис. П1.3), окно которой вызывается из меню **Сервис | Сведения об отправителе**.

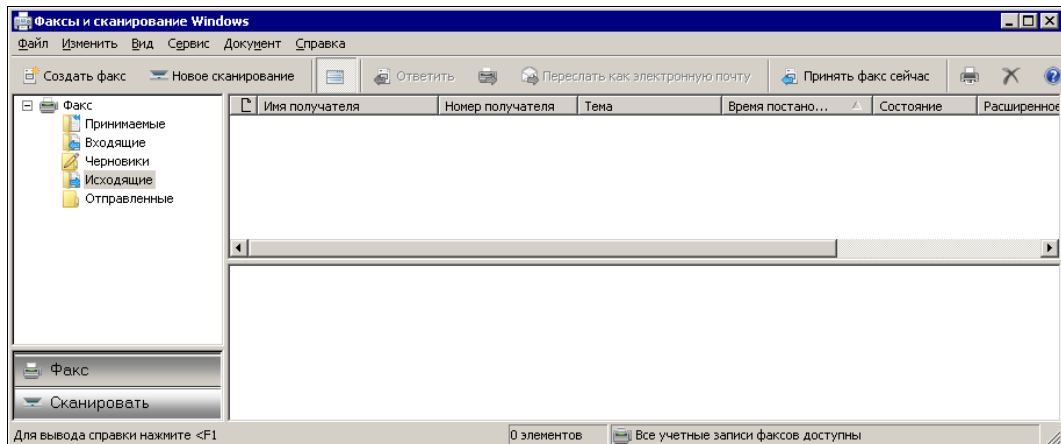


Рис. П1.1. Окно Факсы и сканирование Windows

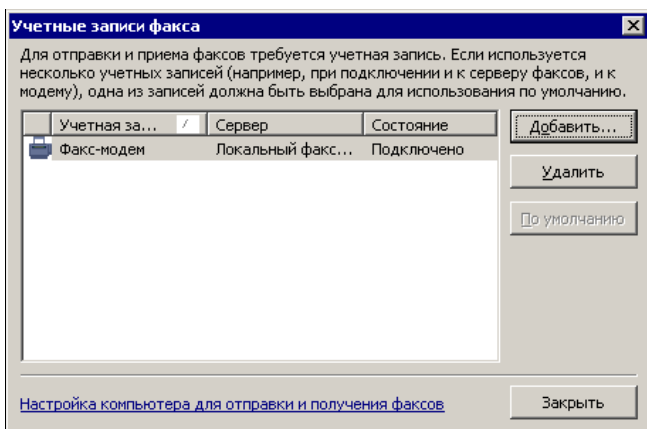


Рис. П1.2. Окно Учетные записи факса

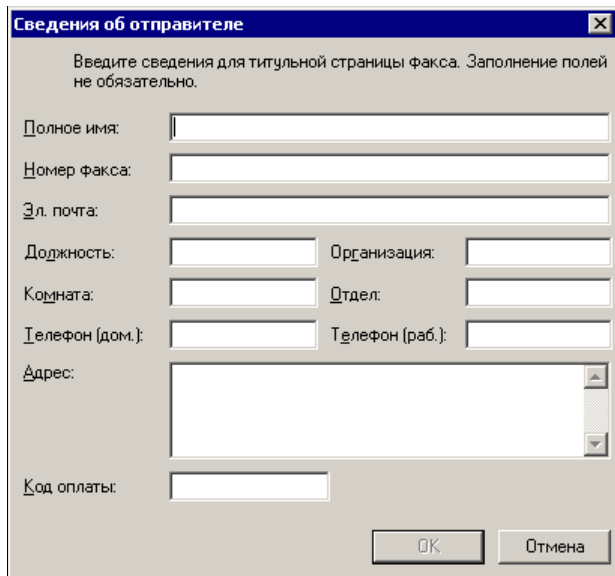


Рис. П1.3. Окно Сведения об отправителе

В этом окне можно заполнить только те поля, которые предоставят получателю сведения, достаточные для вашего идентификации.

Теперь все готово для того, чтобы создать факс. Нажмите кнопку **Создать факс** (см. рис. П1.1). Появится окно создания вашего сообщения с заголовком, соответствующим его теме (рис. П1.4).

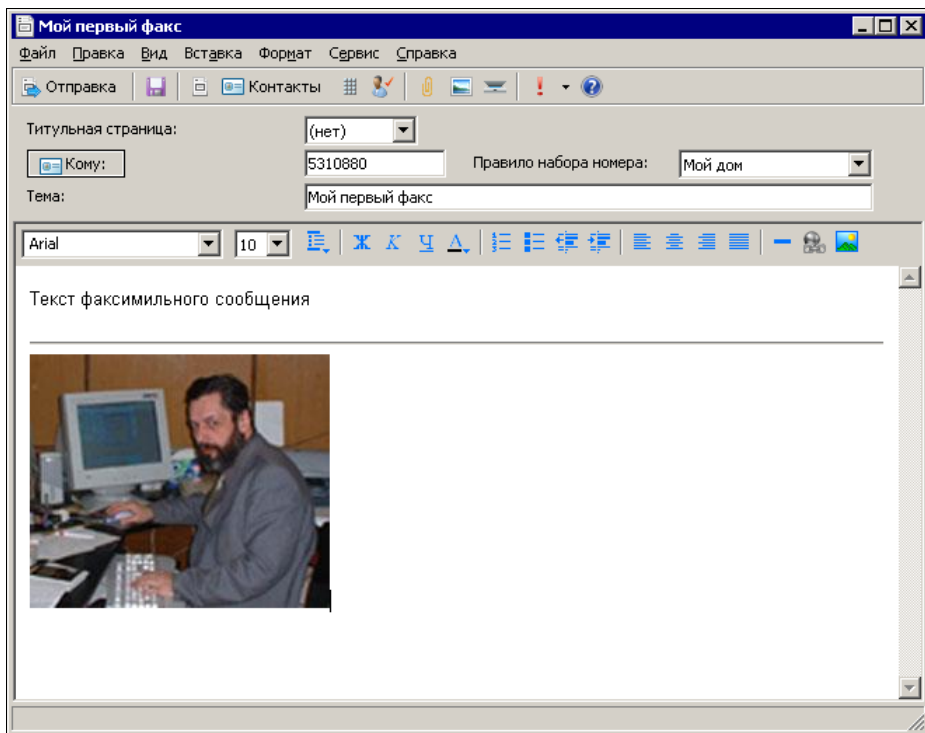


Рис. П1.4. Окно **Мой первый факс**

Вы можете написать любой текст, отформатировав его по вашему желанию, вставить изображение из вашей коллекции. В поле **Кому** необходимо ввести номер телефона, по которому будет отправлено ваше сообщение. Если вы заполняли **Контакты Windows**, то получателя можно выбрать из списка контактов, нажав кнопку **Кому**.

Если сообщение готово, остается нажать кнопку **Отправка**, и начнется отправка факса. При этом вы увидите окно, в котором будет комментироваться процесс отправки и будут указываться проблемы, вероятно возникающие при отправке (рис. П1.5).

В меню **Сервис | Параметры факса** программы **Факсы и сканирование Windows** можно настроить большое число полезных параметров, например режим получения факсов. Либо программа будет отвечать на звонки сама, либо вы вручную должны принять факс (рис. П1.6).

Есть и много других параметров, с которыми вы можете ознакомиться самостоятельно, если решите использовать эту программу.

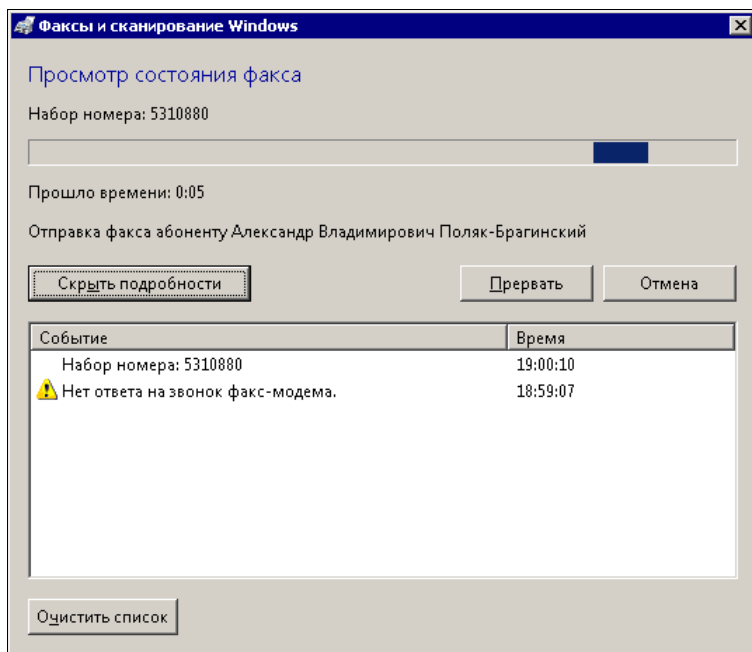


Рис. П1.5. Окно Факсы и сканирование Windows — Просмотр состояния факса

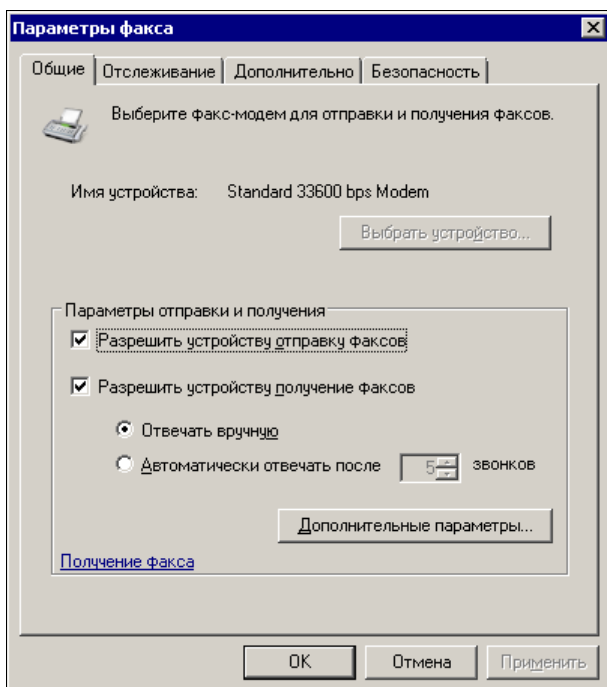


Рис. П1.6. Окно Параметры факса

## Факс в Linux

В Linux после установки системы вы, скорее всего, не обнаружите программы для отправки и получения факсов. Но это не значит, что Linux не позволяет использовать эту возможность. На самом деле на диске с дистрибутивом или в репозиториях — хранилищах файлов для Linux, или же в Интернете обязательно найдется программа для отправки факсов, и не одна. С помощью встроенного графического средства **Управление программами** (рис. П1.7) (это в ОС Mandriva Linux, а в других дистрибутивах название может быть иным) вы всегда можете установить необходимые пакеты.

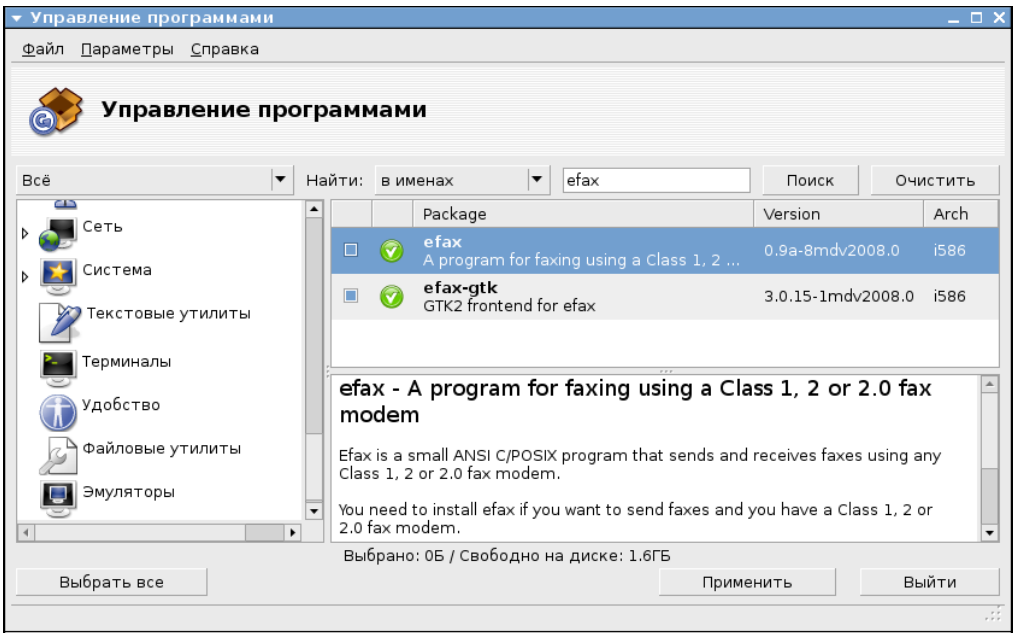


Рис. П1.7. Окно Управление программами

В перечне доступных программ найдите `efax` и установите ее, если она не установлена. Дополнительно установите графический интерфейс для этой программы — `efax-gtk`.

Скорее всего, в меню **Приложения** в разделе программ для офиса появится пункт `efax-gtk`. Запустив эту программу, вы увидите одноименное окно (рис. П1.8). Практически все текстовые редакторы для Linux могут сохранять документы в формате PDF. Этот формат может быть использован для подготовки факсов. Если модем уже был установлен и настроен для подключения к Интернету, программа обнаружит его, и вы сможете отправить подготовленный файл или получить факс.

Настроек у `efax-gtk` не так-то много, и все они достаточно просты для понимания. Если же нужна более подробная справка, нажмите клавишу `<F1>`. Интерфейс программы и справка по ней в ОС Mandriva Linux представлены на языке системы (в данном случае на русском).



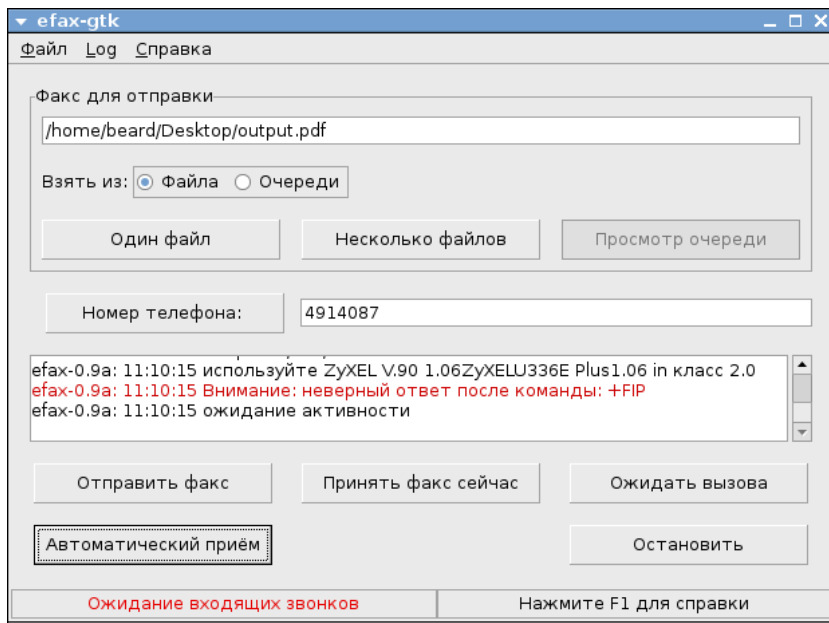


Рис. П1.8. Окно efax-gtk

## Электронная почта в Windows

Для отправки факсов подключение к Интернету не требуется, а вот электронная почта без Интернета работать не будет. Объясняется это тем, что почтовые серверы доступны только через Интернет, а создание и отправка почтовых сообщений выполняется с помощью специализированных программ.

Например, в ОС Windows Vista входит почтовая программа Почта Windows (рис. П1.9).

Для работы с этой программой, как и для работы с другими программами обмена сообщениями, которые будут рассмотрены далее, требуется подключение к Интернету в момент отправки или приема сообщений.

Во время настройки программы или подготовки сообщения для отправки, а также при чтении полученных сообщений подключение к Интернету не требуется. При первом открытии программы вы увидите первое сообщение, которое вам адресовали ее разработчики.

Для того чтобы использовать электронную почту, необходимо иметь учетную запись электронной почты. Получить ее можно у провайдера, через которого вы подключаетесь к Интернету, или воспользоваться платными или бесплатными услугами, предоставляемыми различными почтовыми сервисами. Их вы можете найти в Интернете, набрав в поисковике фразу "Бесплатный почтовый сервис". Пройдя на сайт поставщика услуги, ознакомьтесь с правилами ее предоставления. Важно, чтобы была возможность использовать протокол POP3. Если такая возможность есть, то вы сможете пользоваться почтовым сервисом с помощью вашей программы.

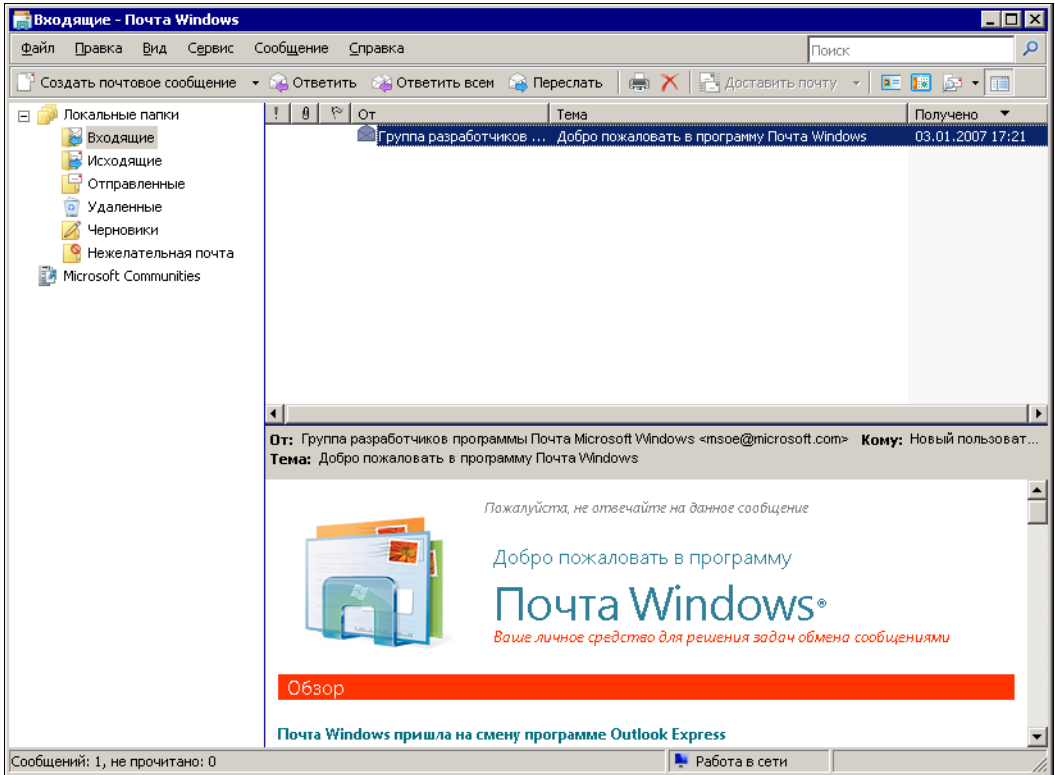


Рис. П1.9. Окно Входящие — Почта Windows

Получив данные своей учетной записи, внесите их в программу. Для этого в меню **Сервис** выберите **Учетные записи**, а в открывшемся окне **Учетные записи в Интернете** нажмите кнопку **Добавить** и выберите **Учетная запись электронной почты**. Теперь заполняйте поля форм, которые будут открываться, и нажимайте кнопку **Далее**.

Завершив создание учетной записи, напишите сами себе тестовое письмо. Если через непродолжительное время вы его получите, то можете использовать настроенную программу для общения с другими людьми.

Вы можете изменить свойства учетной записи после ее создания, в окне свойств учетной записи (рис. П1.10). Если вы не хотите, чтобы программа самостоятельно проверяла вашу почту, то можно снять флажок **Использовать при получении почты или синхронизации**. В этом случае вам потребуется явно указывать имя вашей учетной записи в меню под кнопкой **Доставить почту** для получения и отправки почты (рис. П1.11).

Существует достаточно много почтовых программ. Со временем, когда вы в совершенстве будете знать программу Почта Windows, возможно, у вас появится желание попробовать другие программы, например, проходящую пока тестирование почтовую программу Windows Live Mail (рис. П1.12).

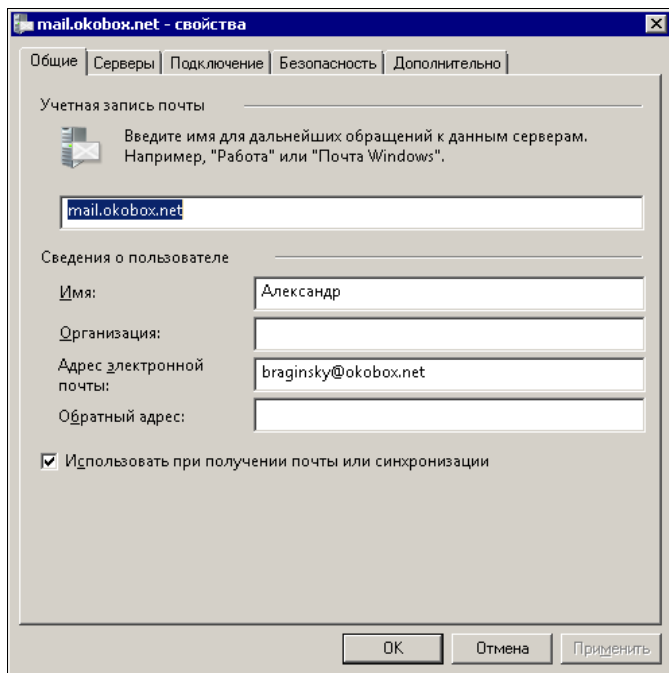


Рис. П1.10. Окно &lt;имя\_учетной\_записи&gt; — свойства

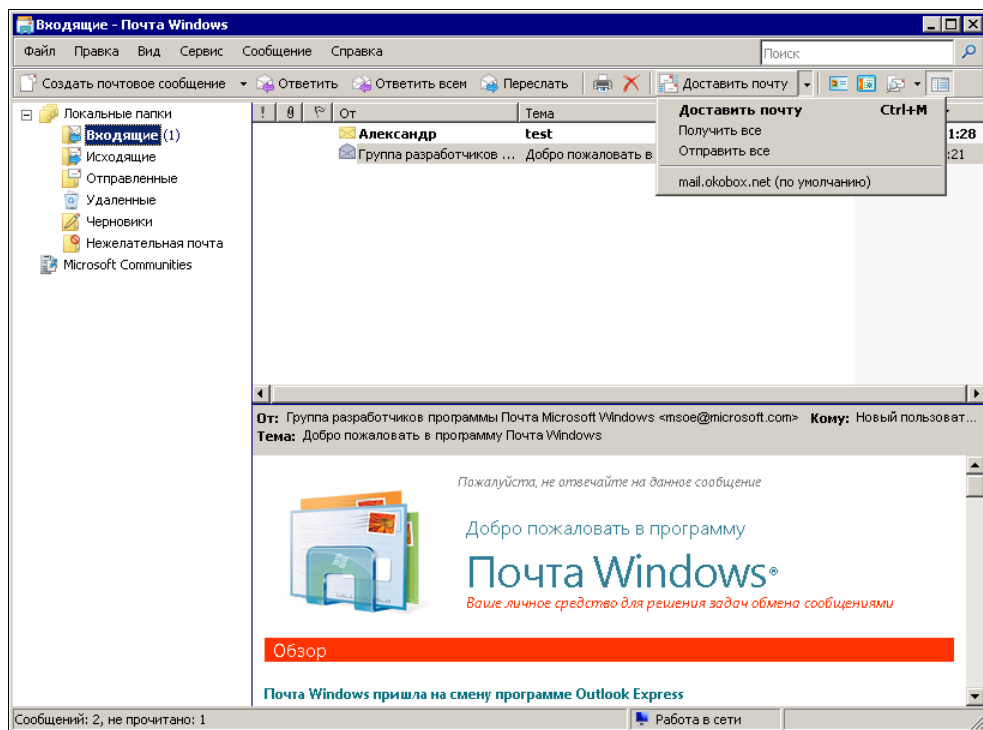


Рис. П1.11. Окно Входящие — Почта Windows — меню Доставить почту

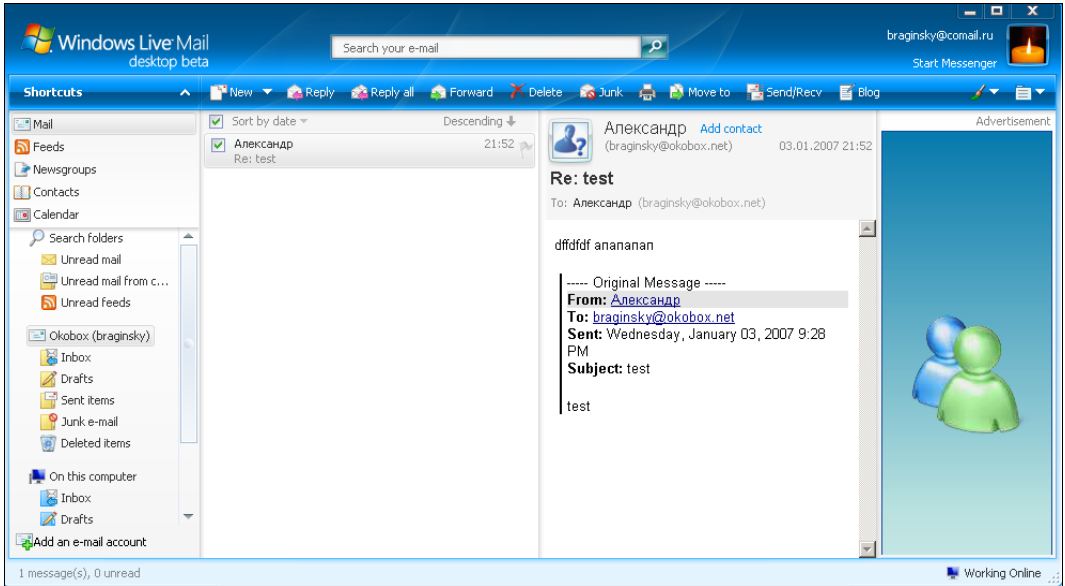


Рис. П1.12. Окно Windows Live Mail

Основные настройки для каждой почтовой программы выполняются аналогично, но каждая программа имеет свои особенности, которые могут заинтересовать опытного пользователя.

## Электронная почта в Linux

Для работы с электронной почтой для Linux написано множество программ. Но в каждом дистрибутиве Linux обычно присутствует программа Evolution — почтовый клиент и ежедневник.

При первом ее запуске вы увидите окно **Помощник по установке Evolution** (рис. П1.13). Нажимая кнопку **Далее**, переходя от окна к окну, которые будут выводить Помощник по установке Evolution, вы можете настроить программу. Настройка практически всех почтовых клиентов очень похожа. Настроив Evolution и запустив ее, вы увидите окно программы (рис. П1.14), откуда будут доступны любые действия с вашими учетными записями и письмами.

Кроме собственно почтового клиента программа содержит ежедневник. Переключаться между режимами работы этой программы можно с помощью определенных комбинаций клавиш:

- Основной режим — <Ctrl>+<1>
- Контакты — <Ctrl>+<2>
- Календари — <Ctrl>+<3>
- Задачи — <Ctrl>+<4>
- Заметки — <Ctrl>+<5>



Рис. П1.13. Окно Помощник по установке Evolution

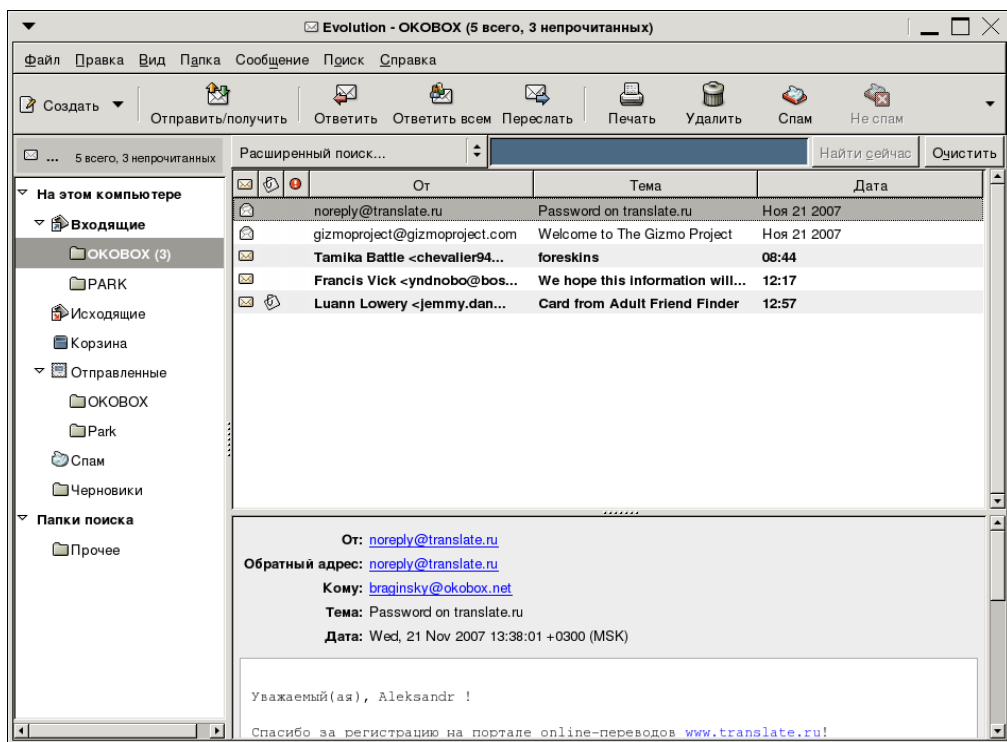


Рис. П1.14. Окно Evolution

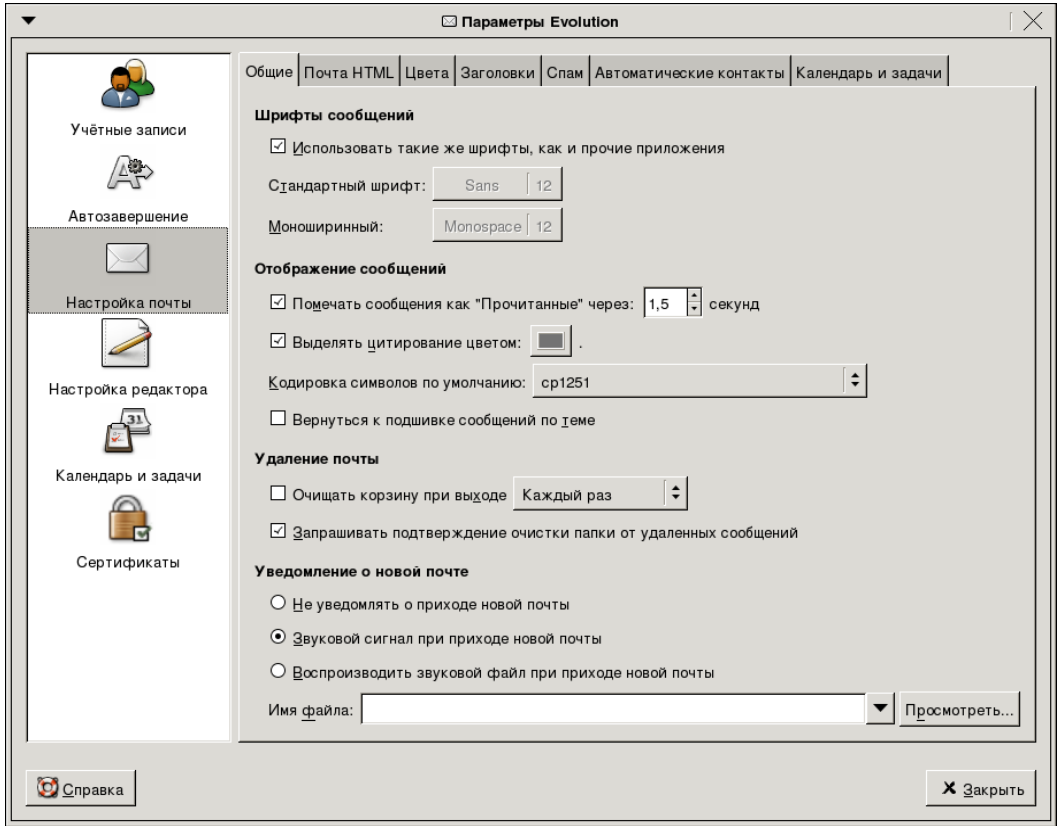


Рис. П1.15. Окно Параметры Evolution

Через меню программы **Правка | Параметры** доступны настройки, которые вам могут потребоваться после работы **Помощника по установке Evolution** (рис. П1.15).

На сайтах в Интернете и в репозиториях вы можете обнаружить множество других почтовых клиентов. Один из наиболее популярных почтовых клиентов, существующий в версиях для различных операционных систем, — Mozilla Thunderbird, который можно найти на сайте <http://www.mozilla-russia.org/products/thunderbird>.

## Программы обмена мгновенными сообщениями, голосом и видео в Windows

Эти программы не входят в состав Windows Vista, их необходимо скачать дополнительно, как и Windows Live Mail. Существует довольно много таких программ, но здесь мы рассмотрим всего три из них, которые пользуются популярностью у пользователей персональных компьютеров. Первая из рассматриваемых программ разработана, как и Windows, корпорацией Microsoft.

## Windows Live Messenger

Программа Windows Live Messenger (рис. П1.16) тесно интегрирована в систему сервисов Windows Live, как и Windows Live Mail.

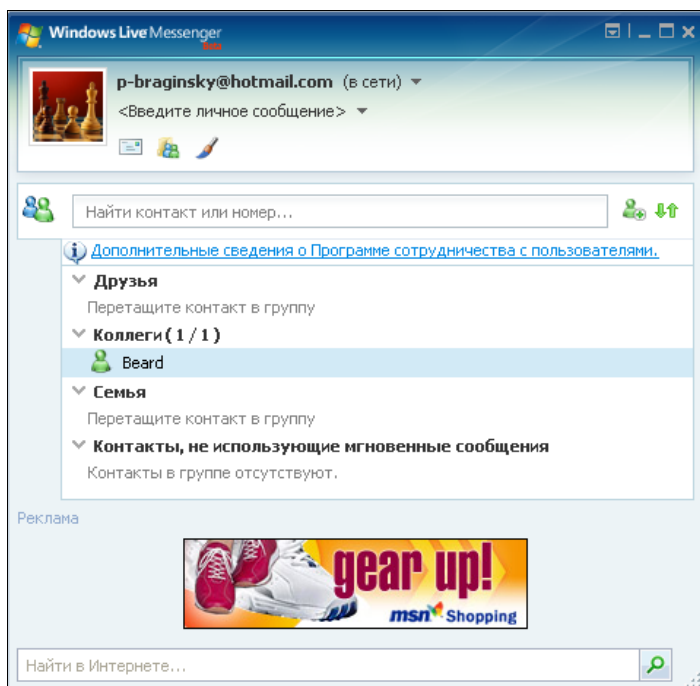


Рис. П1.16. Окно Windows Live Messenger

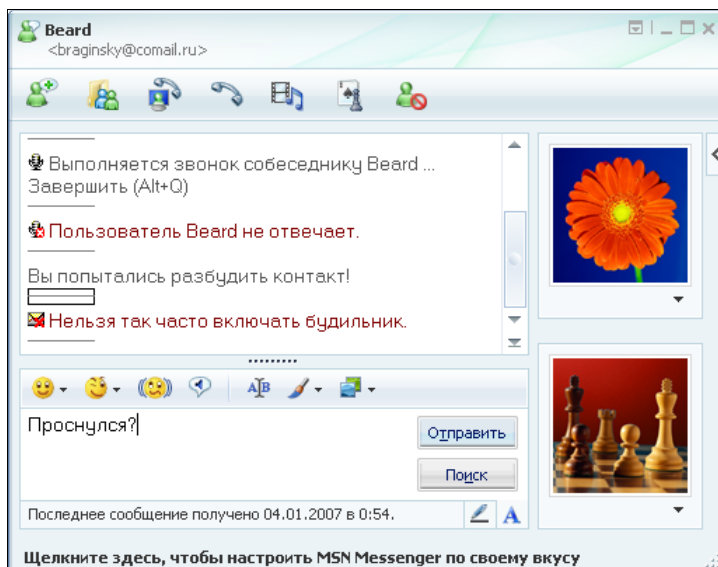


Рис. П1.17. Окно программы Windows Live Messenger (сеанс связи)

Windows Live Messenger позволяет обмениваться текстовыми сообщениями (рис. П1.17), файлами, проводить сеансы видео- и аудиообщения (звонок с компьютера на компьютер).

В рамках сервисов Windows Live пользователи персональных компьютеров получают все больше разнообразных возможностей. Если у вас есть желание, вы можете ознакомиться с сервисами Windows Live и скачать приложения на странице в Интернете <http://ideas.live.com/>.

## Rambler-ICQ

Программа Rambler-ICQ (рис. П1.18) несколько более распространена в России, чем Windows Live Messenger.

Она позволяет также вести обмен информацией в текстовом режиме, есть возможность подключить Web-камеру для видеосвязи, возможна и голосовая связь. В отличие от Windows Live Messenger, ICQ распространяется уже не в бета-версии.

Скачать русскую версию программы и зарегистрироваться можно по адресу <http://www.rambler.ru/>. При этом вы получите почтовый адрес на сайте rambler.ru.

Возможности программы аналогичны Windows Live Messenger, функциональность программы основана на интеграции с несколькими сервисами, включая электронную почту и персональные блоги.

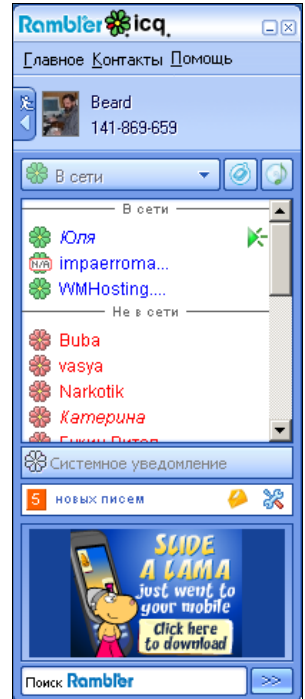


Рис. П1.18. Окно Rambler-ICQ

## Skype

Программа Skype (рис. П1.19) предназначена не столько для текстового общения, сколько для голосового. Skype позволяет выполнять звонки как на компьютеры, так и на обычные и мобильные телефоны. Есть возможность отправки SMS-сообщений (Short-Message Service — служба коротких сообщений), организации телеконференций. Возможна переадресация звонков, поступивших на ваш компьютер, на ваш стационарный или сотовый телефон. Программу можно загрузить по адресу в Интернете <http://www.skype.com/intl/ru/helloagain.html>.

Программа постоянно развивается, появляются различные дополнения к ней. В новых версиях программы есть возможность подключать Web-камеру и показывать собеседнику себя. Оплата за использование платных сервисов возможна через электронную платежную систему Яндекс.Деньги.



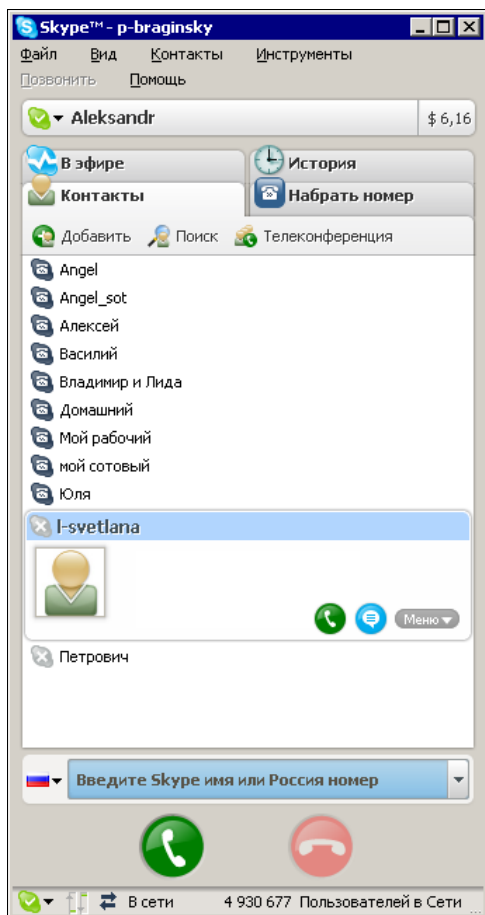


Рис. П1.19. Окно Skype



Рис. П1.20. Окно QIP Infium

## QIP Infium

Пожалуй, программа QIP Infium (рис. П1.20) заслуживает особого внимания ([http://qip.ru/ru/pages/qipinfium\\_beta\\_ru](http://qip.ru/ru/pages/qipinfium_beta_ru)).

В ней осуществлена возможность работы с большим числом служб обмена сообщениями. Это и ICQ, и mail.ru, и Jaber, и VoIP-оператор — SIPNET (<http://www.sipnet.ru>), который предлагает звонки по Москве и Петербургу бесплатно... И обмен сообщениями и голосовое общение доступно через эту программу. Возможны звонки на стационарные телефоны. Как и в программе Skype, можно использовать usb-телефонное оборудование. Пока QIP Infium существует только в бета-версиях, но уже для большинства пользователей работает полноценно.

## Comilfon

Существуют программы, которые предназначены исключительно для голосового общения и звонков на обычные телефоны. Одна из таких программ Comilfon

(рис. П1.21) (<http://www.comilfon.ru>). Пользователям этой программы можно звонить на компьютер со стационарных и сотовых телефонов. Как и в Skype, можно переадресовать вызов с компьютера на обычный телефон.

На сайте [www.comilfon.ru/](http://www.comilfon.ru/) есть подробные объяснения по вопросам использования программы.



Рис. П1.21. Окно COMILFON



Рис. П1.22. Окно Telphin

## Telphin

Еще одна программа для голосового общения (рис. П1.22) — это программа Telphin. По функциональности Telphin похожа на COMILFON, подробности о предоставляемых услугах можно найти на странице <http://www.telphin.ru/>.

Настройки программы для услуг оператора связи "Телфин" выполняются автоматически, но есть возможность настроить дополнительную учетную запись (дополнительный аккаунт) через другого оператора связи, например SIPNET.

Поиск в Интернете, вы сможете обнаружить еще множество программ, позволяющих общаться как через Интернет в режиме Компьютер-Компьютер, так и с использованием стационарных и мобильных телефонных линий.

## Программы обмена мгновенными сообщениями, голосового и видеообщения в Linux

Большинство пользователей ПК так привыкли к Windows, что не могут себе представить работу в привычных программах, но под управлением другой опера-

ционной системы. Тем не менее, для Linux написано множество программ для общения через Интернет.

## Skype для Linux

Многие программы пишутся сразу для нескольких ОС, как например Skype. На рис. П1.23 приведено изображение окна этой программы, снятое с экрана Linux.

К сожалению, производители программ считают Windows основной операционной системой у обычных пользователей. В версию для Linux может быть не включена функциональность программы, появившаяся недавно в последних версиях для Windows. Чем больше будет пользователей Linux, тем больше полнофункциональных программ будет для этой операционной системы. Но основные возможности Skype — это текстовое и голосовое общение через Интернет, звонки на стационарные и мобильные телефоны присутствуют и в этой версии. Программа входит в дистрибутив ОС Mandriva Linux.

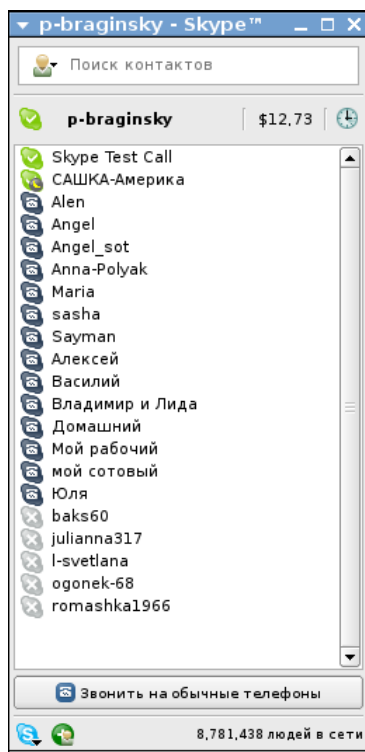


Рис. П1.23. Окно Skype ОС Linux

## Ekiga

Программа Ekiga разработана специально под ОС Linux для голосового и видеобщения, обмена мгновенными сообщениями (рис. П1.24). Программа доступна по адресу в Интернете <http://www.gnomemeeting.org>.

Она входит в большинство дистрибутивов системы Linux и имеет следующие возможности, такие как:

- совместимость с протоколом SIP (Session Initiation Protocol);
- возможность одновременной регистрации нескольких аккаунтов;
- поддержка работы через прокси-сервер;
- поддержка мгновенных сообщений;
- совместимость с протоколом H.323v4;
- поддержка следующих кодеков: iLBC, GSM-06.10, MS-GSM, G.711-Alaw, G.711-uLaw, G.726, G.721, Speex Audio Codecs;
- расширенная адресная книга;

- поддержка номеров для быстрого дозвона;
- лог-файл звонков;
- возможность блокирования администратором некоторых настроек;
- поддержка видеоконференций;
- автоопределение устройств;
- гибкое конфигурирование звуковых оповещений;
- совместимость с KDE и Gnome — оконными менеджерами;
- руководство пользователя;
- перевод на множество языков.

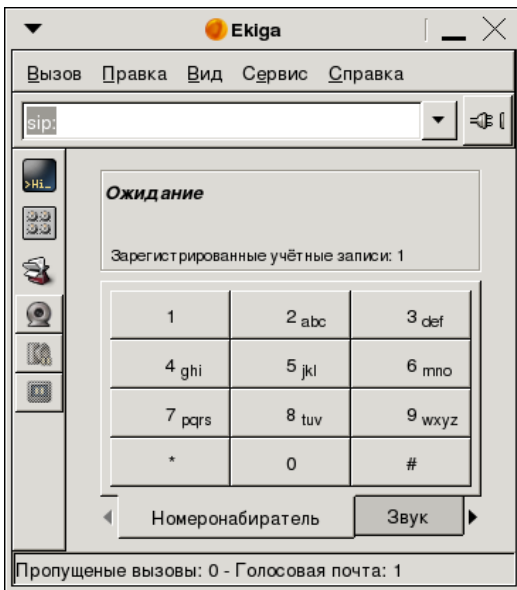


Рис. П1.24. Окно Ekiga

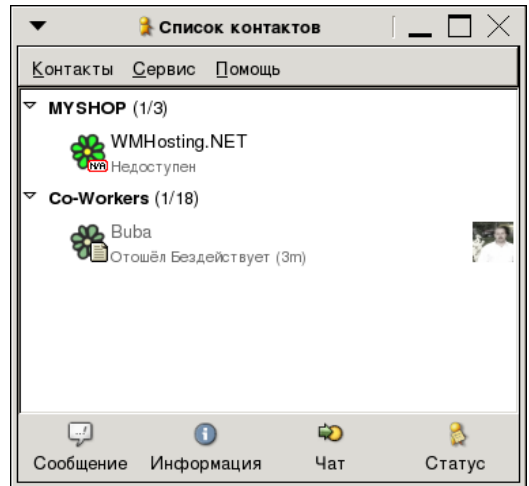


Рис. П1.25. Окно Gaim

## Gaim – Pidgin

Gaim — это программа мгновенного обмена сообщениями (рис. П1.25). В Gaim поддерживается множество протоколов на основе модулей, включающих AIM, ICQ, Yahoo!, MSN, Jabber, IRC, Napster, Gadu-Gadu и Zephyr. Программа Gaim функционально во многом схожа с другими аналогичными программами, но в то же время обладает многими уникальными возможностями.

В связи с претензиями со стороны AOL/Time Warner, группа разработчиков Gaim приняла решение отказаться от использования имени "Gaim". Клиент для мгновенного обмена сообщениями Gaim переименован в Pidgin, библиотека libgaim — в libpurple, а консольный клиент gaim-text — в Finch. Последние версии программы можно найти по адресу в Интернете <http://www.pidgin.im/about>.

## Q\_Chat

Программа Q\_Chat позволяет обмениваться текстовыми сообщениями и файлами в локальной сети. Существует она в версиях для Linux и Windows. Найти ее можно по адресу в Интернете <http://www.kde-apps.org/content/show.php/QChat?content=65066>. Там же есть форум, где можно задать вопросы разработчику, почтить отзывы, ознакомиться с решением некоторых проблем. К сожалению, читать обсуждения и задавать вопросы можно только на английском языке. Но программа имеет русский интерфейс, и работать с ней очень удобно (рис. П1.26).

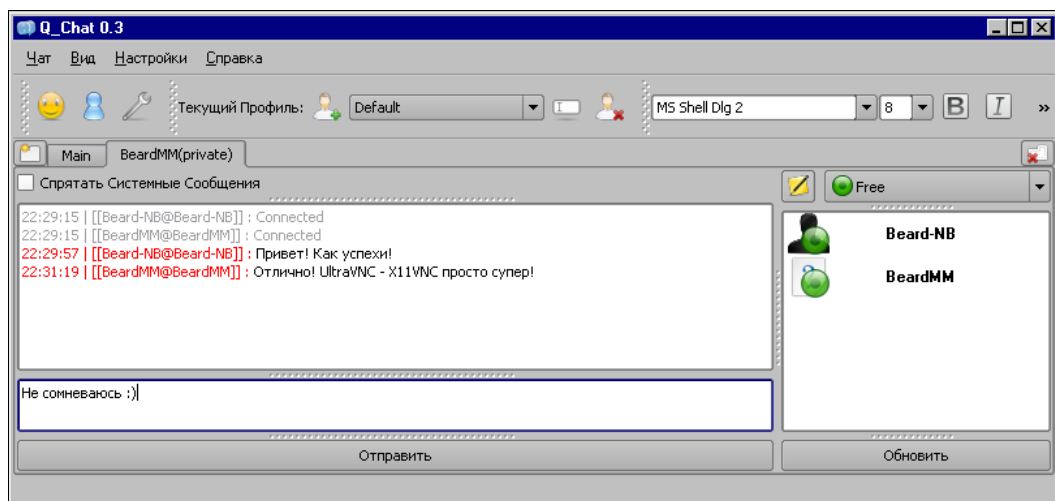


Рис. П1.26. Окно Q\_Chat

Автор рекомендует загрузить и ознакомиться с работой этой программы. Она вам понравится. К сожалению, ее сложно использовать для общения через Интернет, но в локальной сети она может оказаться незаменимой.

Как и для Windows, для Linux существует множество программ для текстового, голосового и видеообщения. Нет смысла описывать здесь все разнообразие программ аналогичного назначения. Важно, что и в Windows, и в Linux есть средства для общения через Интернет, и вы сможете их применять на компьютерах в вашей сети.

## Радио и телевидение в сети

### Видеокамера в сети с компьютерами под Windows

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. 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 (квартирой, детской комнатой);
- передача видео- и аудиоинформации, по локальной сети для ее пользователей;
- организация виртуальных встреч с другими пользователями;
- оперативное создание учебных материалов для пользователей компьютеров в вашей сети (например, для детей и друзей).

Перечень можно продолжать и далее, но мы ограничимся этим списком.

В стандартной поставке вместе с Web-камерой предлагается некоторое 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, но 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 этого 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 звука) кодируется так, что видеoinформация 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, решение которых необходимо для достижения целей.

## Домашнее телевидение

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 заставляла 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 не только просматривать телевизионные передачи и видеофильмы с кассет и дисков, но и просматривать Web-страницы.

Правда, Web-страницы можно просматривать и на обычном ПК (собственно, телепередачи и видеофильмы тоже можно просматривать на домашнем компьютере). Таким образом, современная техника, становящаяся все более доступной, позволяет включать ее в компьютерные сети. Если есть возможность просматривать Web-страницы, то кто-то эти страницы делает. Владелец 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 свои 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 живого 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 получаете возможность как транслировать, так и просматривать видеопрограммы достаточно высокого качества (чем выше качество, тем большего объема трафик требуется для передачи видеoinформации).

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 видеoinформацию, как настроить передачу этой информации в Интернет. В программе ConquerCam вы сможете разобраться самостоятельно. Да она и не позволяет передавать в Интернет динамическое изображение. При использовании этой программы доступны только статические картинки, хотя и обновляемые при нажатии кнопки **Обновить** в браузере Internet Explorer. Совсем другое дело — Кодировщик Windows Media 9 Series. С помощью этой бесплатной программы вы можете передавать на свою страницу в Интернете видеoinформацию 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 щелкните правой кнопкой и из появившегося контекстного меню выберите пункт **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 задайте по своему вкусу.
6. Выберите ячейку, в которой должно быть видеоизображение. В нашем примере остановим выбор на ячейке 2×2. На своей странице можете выбрать и другую ячейку.
7. Щелкните левой кнопкой мыши на выбранной ячейке.
8. В главном меню программы выберите **Вставка | Веб-компонент**, а в открывшейся форме **Дополнительные элементы | Элемент ActiveX**.
9. Затем 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 щелкните правой кнопкой на вставленном элементе (он занимает всю ячейку) и в контекстном меню 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 помещается 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 указывается в адресной строке браузера. Другой сервер — дополнительный, предназначенный для трансляции видеопотока. Его адрес должен быть указан в свойствах ActiveX-элемента. 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 странице будет виден Windows Media Player в виде небольшой панели управления и черного экрана. Пока закройте эту 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.

В этом случае вам потребуется выполнить следующие действия:

1. Нажмите кнопку **Новый сеанс**.
2. В открывшемся окне **Новый сеанс** на вкладке **Мастера** выберите значок **Живая трансляция** и щелкните 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 аудиопараметры компьютера самостоятельно, то, возможно, придется и здесь самостоятельно выбрать необходимое значение из выпадающего списка.
4. Нажимаем 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. Затем на следующем экране указываем выбранный порт (3333). Если у вас есть сомнения в том, что на вашем компьютере этот порт свободен, то с помощью кнопки **Найти свободный порт** можно найти свободный порт. В этом случае и в свойствах элемента ActiveX на Web-странице потребуется смена значения порта.
7. На следующем экране в поле **Скорость** выберите необходимую вам скорость. 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 выбрать 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, то 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 настройки прямого вещания вы сможете разобраться самостоятельно.
9. Далее будет предложено выбрать файлы для вступления, антракта и финала или производить кодирование только с выбранных устройств. Задаем кодирование только с выбранных устройств и нажимаем кнопку **Далее**.
10. На следующем экране вводим информацию о заголовке, авторе и другую текстовую информацию, или не вводим ничего. Снова нажимаем кнопку **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. П1.27).

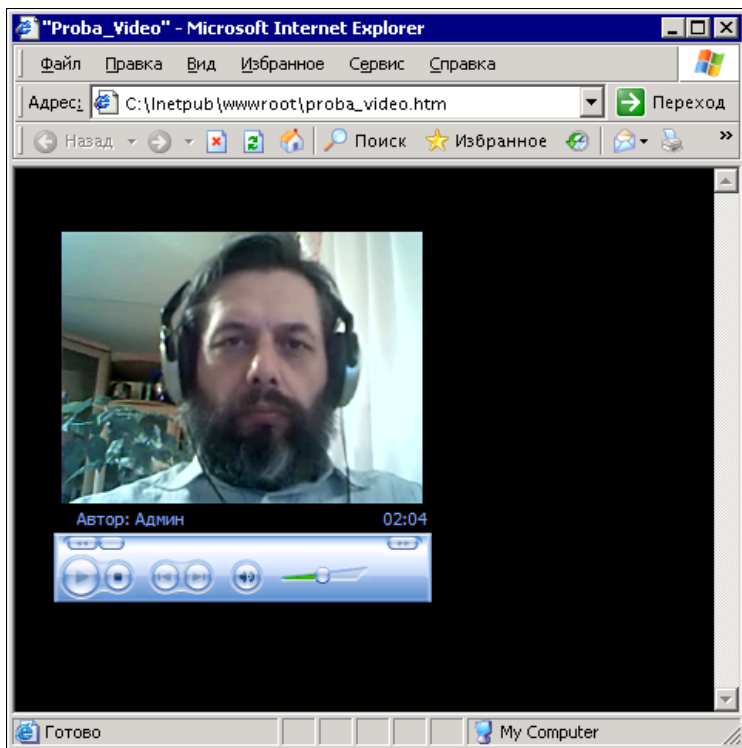


Рис. П1.27. Окно браузера с только что созданной страницей

Теперь, поэкспериментировав с камерой и программами, чтобы добиться желаемого вами результата, вы можете поместить страницу на доступный другим пользователям сервер, настроив соответственно на получение изображения с сервера, где установлен Кодировщик Windows Media 9 Series. Сервером в данном случае может быть ваш собственный компьютер.

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.

Автор не удержался от описания системы, которая работает только под управлением Windows. Передача изображения и звука описанным способом применялась в домашней сети автора. Но есть средства, которые вероятно не покажутся вам очень простыми с первого взгляда, но освоив их, вы сможете передавать аудио- и видеоинформацию в своей сети на компьютеры и с компьютеров под управлением любой операционной системы. Более того, программа, которую мы сейчас рассмотрим, позволяет не только передавать информацию, но и просто проигрывать ее на своем компьютере из файлов или с дисков, а также принимать интернет-радио и телевидение. Принимаемые передачи можно транслировать в свою сеть...

## VLC-медиаплеер

VideoLAN-клиент (<http://www.videolan.org>) существует как для Windows, так и для Linux. Версии по функциональности равнозначны, но для Linux создано больше различных дополнений. VideoLAN может воспроизводить передаваемое по сети видео и ретранслировать потоковые данные в форматах UDP Unicast, UDP Multicast (MPEG-TS), HTTP, RTP/RTSP, MMS. Если на данном этапе вам непонятны сведения о потоковых данных, — не расстраивайтесь. Мы рассмотрим пример ретрансляции с помощью VideoLAN-программы интернет-телевидения с компьютера под управлением Windows Vista на компьютер под управлением Mandriva Linux. Операционная система в данном случае не имеет значения. Если вы решите транслировать по сети видеoinформацию с дисков или созданную самостоятельно, то процедура настройки не будет очень сильно отличаться от описанной. Иногда, разве что, придется немного поэкспериментировать.

## Ретрансляция радио и телевизионных передач

Для начала необходимо просто настроить VLC на прием потоковых данных. Программа имеет как бы два слоя управления. Один слой для обычных пользователей, а другой для продвинутых. Мы воспользуемся самыми простыми средствами, которые лежат на поверхности.

Запускаем VLC media player (рис. П1.28).

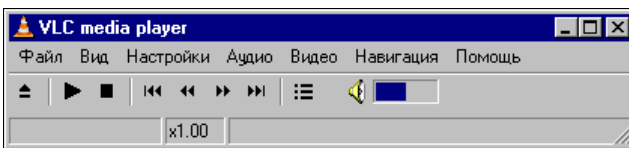


Рис. П1.28. Окно VLC media player

Воспользовавшись меню **Вид | Плейлист**, откройте одноименное окно **Плейлист** (рис. П1.29), в котором с помощью меню **Управление | Поиск сервисов** запустите поиск **Shoutcast TV**.

Выберите любой из найденных потоков, щелкнув на строке мышью. На вашем компьютере начнется воспроизведение потока.

Теперь из меню **Файл** выполните команду **Мастер вещания/кодирования** (рис. П1.30).

Выберите переключатель **Вещание в сеть** и нажмите кнопку **Next**. Откроется окно **Мастер вещания/кодирования — Ввод** (рис. П1.31).

Выберите в этом окне строку потока, который уже воспроизводится, и нажмите кнопку **Next**.

Откроется окно **Мастер вещания/кодирования — Вещание** (рис. П1.32), в котором можно с помощью соответствующего переключателя выбрать метод рассылки потока. Переключатель **RTP Unicast** позволяет направить поток избирательно на определенный компьютер в сети. При этом необходимо указать его IP-адрес в

поле **Адрес**. Переключатель **RTP Multicast** позволяет вещать на всю сеть. К сожалению, параметры нашей сети могут не совпадать с теми, что предусмотрены для этого метода вещания. Переключатель **HTTP** тоже позволяет вещать на всю сеть. На компьютере-приемнике необходимо будет указать IP-адрес передающего компьютера.

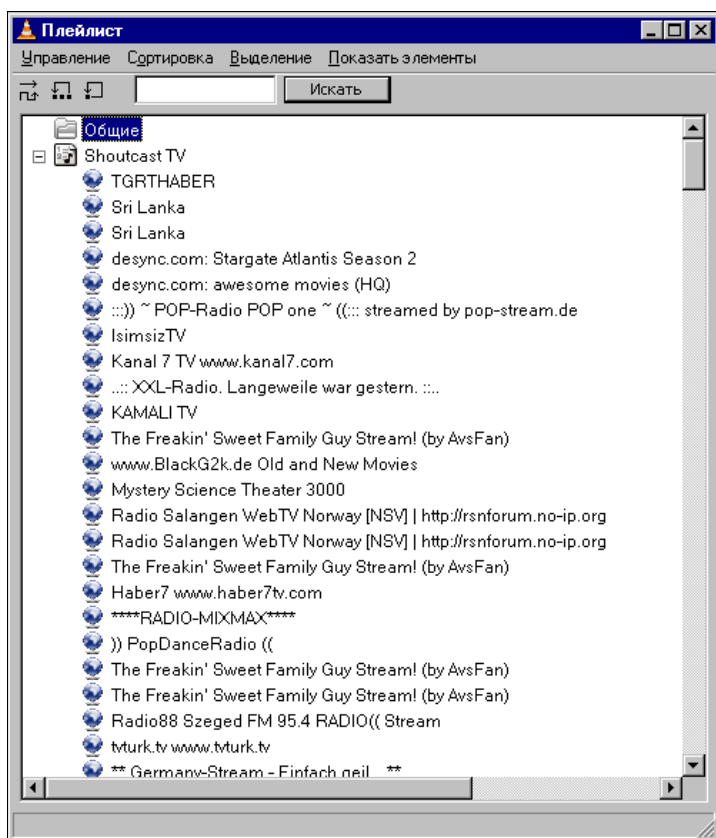


Рис. П1.29. Окно Плейлист

В следующих окнах ничего выбирать не надо, просто нажимайте кнопку **Next**.

Начнется передача потока. На компьютере-приемнике запустите VLC media player и в меню **Файл** выберите **Открыть URL**, указав прием по UDP или HTTP и IP-адрес компьютера передатчика, а также порт 8080. В окне плейлиста появятся строки с информацией о принимаемых потоках (рис. П1.33), а на экране VLC и в динамиках появится передаваемая информация (рис. П1.34).

Если вместо потока из Интернета указать устройства самого компьютера, такие как Web-камера, например, то в сеть можно передавать изображение, передаваемое этой камерой (рис. П1.35). Конечно, возможна и передача видео из сохраненных файлов. Практически все, что необходимо для организации простой теле-радиостанции, имеется в VLC.

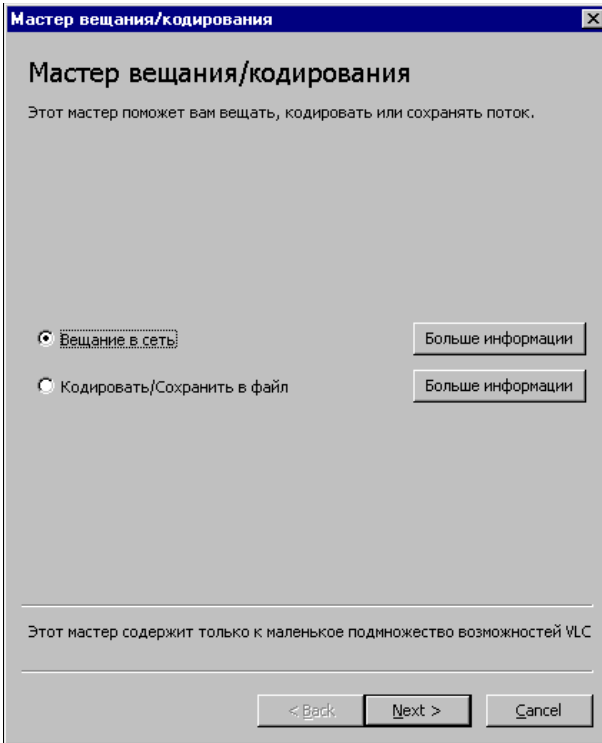


Рис. П1.30. Окно Мастер вещания/кодирования

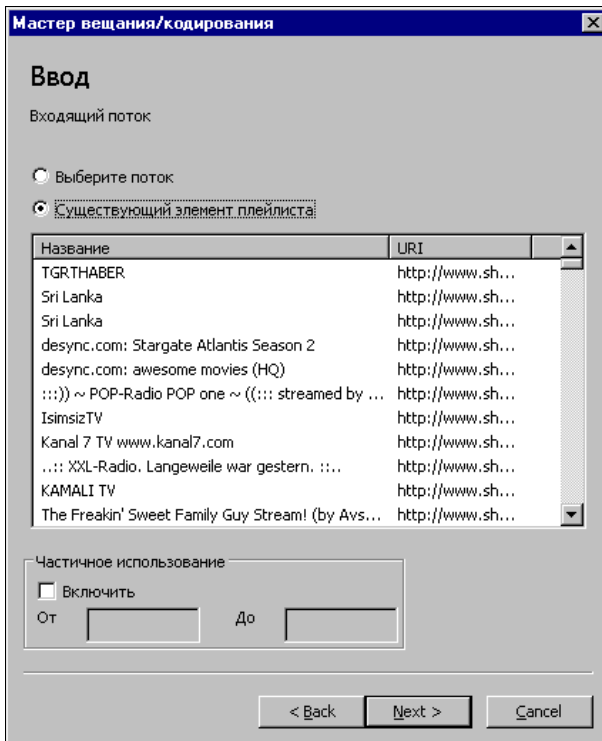


Рис. П1.31. Окно Мастер вещания/кодирования — Ввод

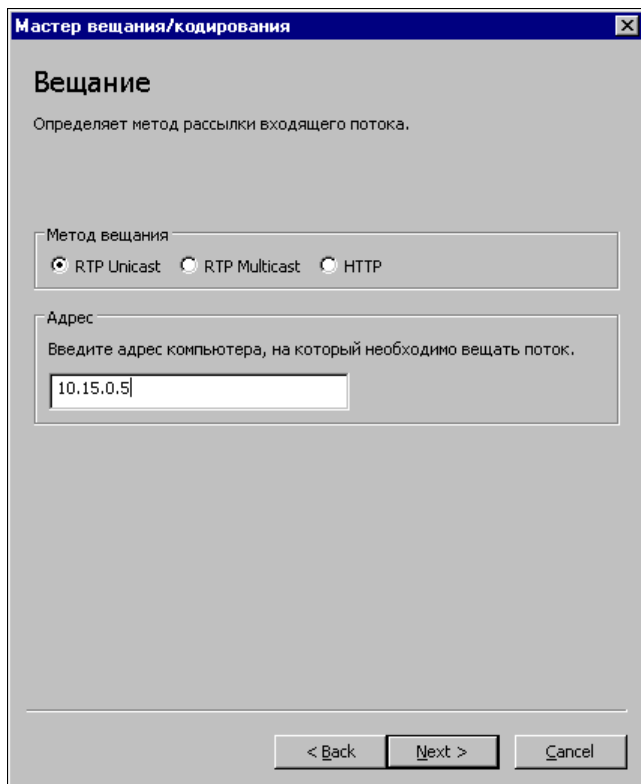


Рис. П1.32. Окно Мастер вещания/кодирования — Вещание

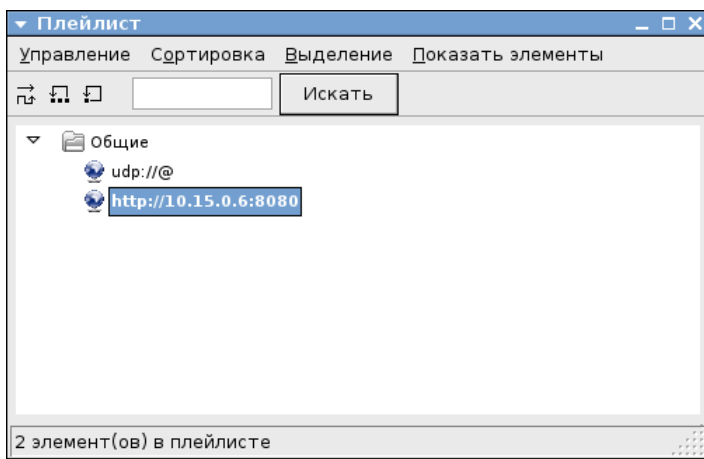


Рис. П1.33. Окно Плейлист (в Linux)

Интерфейс VLC можно выбрать по своему усмотрению в настройках программы. Один из вариантов интерфейса показан на рис. П1.35.

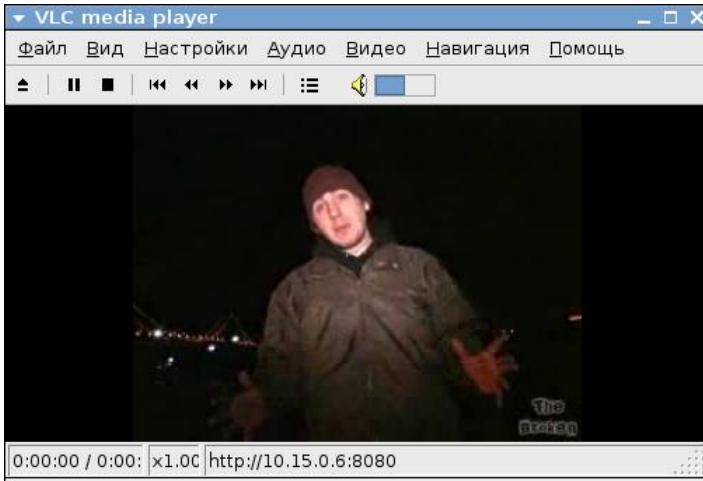


Рис. П1.34. Окно VLC media player (в Linux)

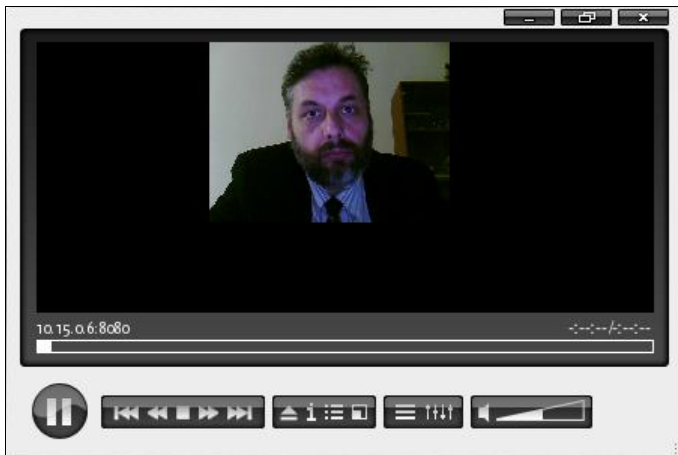


Рис. П1.35. Вариант интерфейса окна VLC media player (в Linux)



# ПРИЛОЖЕНИЕ 2

## Советы начинающему администратору локальной сети

### Что должен знать администратор локальной сети?

Такой вопрос мне иногда задают начинающие администраторы. Что же можно на это ответить? — Чем больше, тем лучше. Здесь и знание технического английского языка, и компетентность в технических вопросах организации локальных сетей и даже в вопросах, связанных со строительством при организации сетей.

Где можно получить эти знания? Значительная часть знаний может быть получена из Интернета. Также с помощью Интернета можно узнать об учебных заведениях, которые могут дать необходимые знания.

Строя сеть на основе ОС Windows, требуются знания, источником которых является сама фирма Microsoft, которая для специалистов организовала разнообразные курсы. О них можно узнать по адресу в Интернете <http://www.avalon.ru/ITCourses/Microsoft/>.

Чтобы ваша сеть соответствовала принятым стандартам, необходимо познакомиться с содержанием этих стандартов. Перечень стандартов, на которые следует ориентироваться, можно найти по адресу <http://www.ecolan.ru/standards.htm>.

Сети в наше время строятся в соответствии с требованиями к СКС (структурированным кабельным сетям). Наиболее употребительны три стандарта:

- EIA/TIA-568A Commercial Building Telecommunications Wiring Standard (американский);
- ISO/IEC IS 11801 Information Technology — Generic cabling for customer premises cabling (международный);
- CENELEC EN50173 Performance Requirements of Generic Cabling Schemes (европейский).

О построении сетей в соответствии с этими стандартами можно почитать по ссылке <http://www.daascom.com/computer/consultation/HardwareLAN.htm>.

В России требуется еще соблюдение СНИП (строительных норм и правил). Они также доступны в Интернете по адресу <http://www.vashdom.ru/snip/30506-85/>.

Вообще о стандартизации в области компьютерных сетей можно почитать по ссылкам:

- <http://www.osp.ru/lan/2006/01/050.htm>;
- [http://www.daascom.com/computer/consultation/lan\\_shielded.html](http://www.daascom.com/computer/consultation/lan_shielded.html).

## Где можно получить необходимые программы?

Возможностей есть несколько. Самый прямой путь — это обращение на сайт разработчиков программы. Поиск можно начинать на популярных сайтах, которые собирают на своих страницах ссылки на программы различных разработчиков, как коммерческие, так и свободно распространяемые:

- <http://www.softportal.com/>;
- <http://www.softforfree.com/>;
- <http://www.freesoft.ru/>;
- <http://soft.mail.ru/>;
- <http://www.tucows.com/>;
- <http://www.oszone.net/>.

Перечень ссылок на коллекции программ можно продолжать до бесконечности. Это могут быть и частные страницы, и форумы. Часто форумы есть на сайтах с коллекциями программного обеспечения, но существуют и самостоятельные. На форумах, кроме самих программ, можно найти их обсуждения и рекомендации по использованию:

- <http://forum.ru-board.com/>;
- <http://forum.oszone.net/>;
- <http://www.bestfilez.net/>.

Только беглое знакомство с этими форумами займет у вас немало времени.

## Поиск информации в Интернете

Конечно, самостоятельный поиск в поисковых машинах тоже поможет вам найти необходимые материалы. Для тех, кто еще не освоился с поиском в Интернете, сам Интернет предоставляет возможность научиться:

- <http://www.teenclub.ru/index.php?e=193>;
- <http://websearch.report.ru/>;
- [http://www.kursy.ru/int\\_srch/index.htm](http://www.kursy.ru/int_srch/index.htm);
- <http://second.kubok.yandex.ru/howfind.xhtml>.

Чтобы получить верный ответ, надо правильно задать вопрос. Иногда человек понимает, что он хочет, но, не владея терминологией и некоторыми базовыми знаниями, не может сформулировать вопрос. Для того чтобы упростить жизнь начинающим администраторам, в *приложениях 3 и 4* приведены сведения об основных сетевых понятиях, объяснено достаточно большое число терминов, которые встретятся вам при организации сети и работе в ней. Перечень терминов далеко не полный, но знания всегда растут как снежный ком. Важно начать и не останавливаться в процессе их освоения.

# ПРИЛОЖЕНИЕ 3

## Краткий словарь терминов и сокращений

### **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).

### **100BASE-FX**

(Оптоволоконный кабель 100 Мбит/с)

Реализация сети Ethernet на оптоволоконном кабеле, обеспечивающая скорость передачи данных 100 Мбит/с.

### **100BASE-T**

(Fast Ethernet)

Технология 100 Мбит/с, основанная на методе доступа Ethernet/CD и использующая кабель "витая пара".

### **10BASE-T**

(Витая пара 10 Мбит/с)

Спецификация IEEE 802.3 сетей Ethernet на неэкранированном кабеле "витая пара" (UTP).

### **Active Directory**

Термин "Active Directory" используется как для обозначения каталога с информацией о пользователях, компьютерах и других объектах сети, так и для обозначения

ния 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. Более подробное описание Active Directory приведено в *приложении 4*.

### **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 автораспознавания способны также определить качество канала и автоматически выбрать максимальную скорость передачи.

### **AUI**

AUI (Access Unit Interface) — интерфейс устройств доступа; интерфейс подключаемых устройств. *N*-контактный кабельный интерфейс штекерного типа, используемый в магистральных соединениях.

### **BNS**

Кабельный интерфейс для соединения коаксиального кабеля в магистральных сетях.

### **Bridge**

(Мост)

Комбинация аппаратного и программного обеспечения, соединяющая две локальные сети и позволяющая осуществлять коммуникации между их станциями. Мосты функционируют на канальном (втором) уровне эталонной модели OSI.

### **Bridge/Router**

(Мост/маршрутизатор)

Устройство, функционирующее как мост, как маршрутизатор или как оба 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.

### **DHCP (Dynamic Host Configuration Protocol)**

Служба динамического выделения сетевых адресов. Позволяет не загружать администратора сети проблемами распределения адресов, работает автоматически.

### **DNS (Domain Name System)**

- 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.
- Распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в Интернете. 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 95/98, Microsoft Windows for Workgroups, Microsoft LAN Manager, Banyan VINES, Artisoft LANtastic, IBM LAN Server, HP LAN Manager и многие другие.

### **Ethernet**

Самый распространенный стандарт компьютерных сетей. Имеет несколько модификаций и вариантов, которые совместимы друг с другом. Конкретные реализации обозначаются как 802.10T — обычные локальные сети, 802.11b — радиосети, существуют и другие варианты.

### **Fast Ethernet**

Широко распространенный протокол локальной сети, поддерживающий скорости передачи данных 10 и 100 Мбит/с.

### **FTP (File Transfer Protocol)**

Протокол передачи данных в сети. Применяется для передачи файлов.

**Hub**

См. *концентратор*.

**HTML (Hypertext Markup Language)**

Язык гипертекстовой разметки. Средство создания страниц для публикации в Интернете и последующего просмотра с помощью браузера. HTML-страницы могут применяться для обмена информацией в локальной сети, а также для хранения информации в виде HTML-файлов.

**Interface**

- Физическое устройство, соединяющее две системы или два устройства.
- Стандарт (такой как RS-232C), специфицирующий взаимодействие систем.

**ISDN (Integrated Service Digital Network)**

Международный стандарт передачи голоса, видео и данных по цифровым телефонным линиям.

**LAN (Local Area Network)**

Локальная компьютерная (вычислительная) сеть. Русскоязычное сокращение — ЛВС.

**LINKLOCAL**

Диапазон сетевых адресов, применяемых в локальных компьютерных сетях и не применяемых в глобальных сетях.

**MAC-адрес**

Аппаратный адрес сетевого устройства. Не может повторяться, обеспечивает идентификацию сетевого устройства независимо от назначаемого адреса или имени.

**NetBEUI (NETBIOS Enhanced User Interface)****NetBIOS (Network Basic Input/Output System)**

NetBEUI — это протокол, дополняющий спецификацию интерфейса NetBIOS, используемую сетевой операционной системой. NetBEUI формализует кадр транспортного уровня, не стандартизованный в NetBIOS, не маршрутизируемый протокол. Этот протокол понимает обычные буквенно-цифровые имена и отвечает за сеансы передачи данных между узлами сети.

**Proxy Server**

Proxy Server — это система, находящаяся между исполняемыми приложениями (такими как Internet Explorer) и соединением с Интернетом. Она перехватывает запросы к серверу, рассматривая возможность выполнить их самостоятельно, что увеличивает быстродействие за счет отсеечения повторных запросов одной и той же информации из Интернета. Proxy Server может кэшировать загружаемые из Интер-

нета страницы (файлы). Используя этот метод, если кто-то еще запрашивает страницу (файл), ранее уже кем-либо запрашиваемый Proxu Server выдает эту страницу из своего кэша, что значительно быстрее, чем снова загружать ее из Интернета. Proxu-серверы также могут выступать в качестве сетевого экрана, фильтруя IP-трафик по порту или IP-адресу.

### **Telnet**

Telnet — это один из старейших протоколов Интернета. Он появился в 1969 году в ARPANET. Имя этого протокола является сокращением от Telecommunications Network Protocol — сетевой коммуникационный протокол. Его описание находится в RFC 854. Этот протокол позволяет вам подсоединиться к удаленному компьютеру, находящемуся в сети, и работать с ним, как будто бы вы работаете на удаленном компьютере, т. е. в режиме терминала. Ваши возможности лимитируются тем уровнем доступа, который задан для вас администратором удаленной системы.

В поставку Windows входит одноименная программа, которую вы можете запустить через **Пуск | Выполнить**.

### **TCP/IP (Transmission Control Protocol/Internet Protocol)**

Современный сетевой протокол. Подробно описан в *приложении 3*.

### **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 (Unshielded Twisted Pair)**

(Неэкранированная витая пара)

Неэкранированная витая пара — самый популярный тип кабеля, используемый для соединения настольных систем и рабочих групп.

### **Virtual LAN**

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 не обязательно должны находиться (географически) 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 применяются для управления трафиком, обеспечения защиты и для контроля широковещательной рассылки.

### **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.

### **Wi-Fi или WiFi (Wireless Fidelity)**

См. *Беспроводная сеть*.

### **Беспроводная сеть**

Сеть, построенная на основе беспроводных сетевых адаптеров и концентраторов. Среди других изделий и фирм обращают на себя внимание изделия фирмы Intel. Intel PRO/Wireless 2011 LAN Access Point — точка доступа для связи удаленного компьютера с локальной сетью, может применяться и как репитер (повторитель) для увеличения максимального расстояния для подключения. Intel PRO/Wireless 2011 LAN PC Card — беспроводный сетевой адаптер для компьютеров.

В последнее время получают все большее развитие сети Wi-Fi. Работа в таких сетях возможна везде, где есть точки доступа. В аэропортах, в кафе, в учреждениях все чаще можно увидеть такие точки доступа и получить возможность выхода в Интернет со своего ноутбука или карманного компьютера.

По ссылке <http://ru.wikipedia.org/wiki/wi-fi> есть очень подробная статья об этой технологии.

### **Витая пара**

Кабели на основе витой пары находят широкое применение в сетях передачи данных. Для кабеля на основе витых пар используются медные проводники 0,51—0,64 мм в диаметре. В качестве материала изоляции обычно используется 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 ее цветной пары, другой цветной — синий, оранжевый, зеленый, коричневый. Конструктивно все кабели делятся на экранированные и неэкранированные конструкции. Экранированные конструкции более помехозащищены 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 производится кабель 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 кодируется дата производства (1002 — октябрь 2002) и отметка метровой длины (иногда футы). Кроме того, на кабеле могут быть указания на материал оболочки, систему 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*.**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 мксек) направляет этот пакет в соответствующий порт. Таким образом, когда пакет еще целиком не прошел через входной порт, его заголовок уже передается через выходной.

**Коаксиальный кабель**

Представляет собой два соосных гибких металлических цилиндра, разделенных диэлектриком. Название произошло от латинского *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 применение толстого коаксиального кабеля для связи территориально удаленных на расстояние до 180 м и более участков сети.

**Компьютерная сеть**

Компьютерная сеть — это компьютеры, соединенные между собой средствами передачи информации. Эти средства достаточно разнообразны, чтобы учесть большинство возникающих на практике вопросов. 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 панель. 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. Таким кабелем можно подключить рабочее

место, удаленное на 2000 м. Но стоимость такого 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 следует только задействовать, изменив конфигурацию операционной системы. Для более эффективной реализации работы в сети необходимо использовать специализированный компьютер — *сервер*, который будет выделен 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 него 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 типа "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 лежит в пределах от 4 до 32.

### **Маршрутизатор (роутер)**

Маршрутизатор распознает адрес получателя и перенаправляет пакет только туда, куда ему, пакету, предназначено. Вполне возможно, для этих целей применять отдельный компьютер с двумя и более сетевыми адаптерами. Можно применять 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.

## 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.

## 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 др.), так и *программные*, определяющие диапазон памяти процессора, который используется для подключения. Так, интернет-соединения используют порты 80 (HTML), 21 (FTP) и др. Применение того или иного номера порта обусловлено лишь стандартами и договоренностями, чтобы распределить нагрузку на память компьютера, позволив 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 — протокол управления передачей данных/протокол Интернета, ему посвящены целые книги. Сложный протокол, в домашней сети его имеет смысл использовать в случае наличия систем UNIX, маршрутизатора и/или выхода в Интернет, а также при работе с приложениями, использующими этот протокол.

## "Расшаренный диск"

Диск 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: маршрутизатор, мост, коммутатор.

## Сервер

□ 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.

- Главная программа, управляющая работой подчиненных программ — клиентов в клиент-серверной технологии.

### **Сервер удаленного доступа**

Программное средство, обеспечивающее доступ к компьютеру для пользователей, находящихся вне локальной сети.

### **Сетевой адаптер**

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 множеством производителей, среди них: 3com, Intel, DEC, AMD, Cabletron и др., но самая массовая и популярная 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 шести байтов типа 1E:34:00:00:FF:12, который называется *Ethernet-адресом* или *MAC-адресом*. 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 типа "витая пара". В настоящее время коаксиальный кабель применяется реже витой пары ввиду большей свободы, предоставляемой витой парой для расширения и модификации локальной сети.

### **Сетевая плата**

См. *Сетевой адаптер*.

# ПРИЛОЖЕНИЕ 4

## Справочные сведения

### Создание Web-страниц

Обмен информацией с помощью Web-страниц может быть более безопасным, чем обмен с помощью документов MS Word. Простые HTML-страницы не могут содержать опасных макросов и, соответственно, вирусов. Простые Web-страницы можно создавать самостоятельно, не применяя специального программного обеспечения. Тем не менее существует много редакторов Web-страниц, которые повышают удобство их создания и позволяют ускорить получение готовой страницы с достаточно сложным оформлением. К таким редакторам можно отнести MS Word, в котором достаточно выбрать команду **Сохранить как** и указать расширение документа htm или html. Могут применяться и специализированные редакторы типа Front Page Express. Создание Web-страницы с помощью обычного текстового редактора более трудоемко, но позволяет сделать код страницы более компактным. Используя заранее подготовленные шаблоны, можно также сократить время создания новых страниц, внося лишь изменяемую часть текста.

### Основа Web-страницы

Каждый HTML-документ должен содержать следующие основные теги (метки, используемые в языке HTML):

- `<html>` — указывает, что документ — HTML-документ;
- `<head>` — заголовок и специальные отметки, относящиеся ко всему документу;
- `<title>` — определяет текст, отображаемый в заголовке окна просмотра;
- `<body>` — определяет часть документа, которая отображается в окне просмотра.

Пример:

```
<html>
<head>
  <title>
    Название документа
  </title>
</head>
```

```
<body>
  Текст, отображаемый в окне браузера
</body>
</html>
```

## Форматирование Web-страницы

Для управления форматированием HTML-документа применяются специальные теги:

- **Headings** — HTML поддерживает 6 уровней заголовка, от `<h1>` до `<h6>`. Можно применять `<h1>` для форматирования первого заголовка на странице, но это не обязательно. Для форматирования строгих правил нет;
- **Paragraph** — тег `<p>` начинает новый абзац.

Пример:

```
<html>
<head><title>
  Название документа
</title></head>
<body>
  <h1>Текст первого заголовка</h1>
  <p>Основной текст абзаца.
  <p>Другой абзац.
</body>
</html>
```

### **ПРИМЕЧАНИЕ**

В отличие от большинства тегов, `<p>` не требует завершающего — `</p>`.

Добавляя атрибуты, которые может включать тег, можно управлять свойствами текста.

```
<h1 align=center>Центрированный заголовок</h1>
<p align=center>Центрированный абзац с <b>полуужирным</b> текстом.
<p>Еще один абзац с <i>курсивным</i> текстом.
```

Регистр символов в тегах значения не имеет.

## Специальные символы

В тексте HTML-страниц можно применять специальные символы, даже если их нельзя ввести с клавиатуры. Наиболее часто применяются следующие специальные символы:

- `&lt;` — СИМВОЛ `<`;
- `&gt;` — СИМВОЛ `>`;

- `&amp;` — символ `&`;
- `&copy;` — символ ©;
- `&nbsp;` — неразрывный пробел.

Символ неразрывного пробела может быть введен несколько раз, но отображаться будет только один пробел.

Есть возможность ввода символов, которые вы можете найти в Таблице символов. Это приложение, которое может быть установлено, как компонент Windows, и быть вызвано из меню **Программы | Стандартные**. Для этого необходимо указать ASCII-код символа из таблицы в формате `&#169` (этот код соответствует символу ©).

## Ссылки

Для быстрого перехода к необходимой части страницы, файлу или адресу в Интернете или в вашей сети можно применять символ ссылки.

- `<a href="имя файла с расширением">текст, сопутствующий ссылке</a>`
- `<a href="http://www.firma.domen">текст, сопутствующий ссылке</a>`
- `<a href="#метка в тексте">текст, сопутствующий ссылке</a>`

Для того чтобы работала последняя ссылка, в тексте должна быть метка для перехода по этой ссылке вида:

```
<a name="Метка в тексте">
```

"Метка в тексте" — это имя метки, написанное латинскими буквами.

## Графика на Web-странице

Страница может содержать рисунки. Рисунки должны быть выполнены в форматах GIF, PNG или JPEG. Для отображения рисунка на странице применяется тег `<img>`.

Для помещения на страницу рисунка в формате JPEG следует в тексте страницы поместить следующую строку:

```

```

При этом сам файл рисунка должен находиться в одном каталоге с файлом страницы. Иначе говоря, имя файла должно содержать полный путь к нему.

Как и строки, изображения на странице можно форматировать. В следующем примере применены уже знакомые параметры форматирования, но в применении к рисункам:

```


```

Есть возможность указать размер рисунка:

```

```



## Управление цветом

HTML-элементам можно задавать определенные цвета.

Стандартный набор цветов, применяемый на Web-страницах, следующий:

- |  |   |
|--|---|
| <input type="checkbox"/> aqua — голубой;               | <input type="checkbox"/> lime — ярко-зеленый; |
| <input type="checkbox"/> gray — серый;                 | <input type="checkbox"/> olive — оливковый;   |
| <input type="checkbox"/> navy — морской (темно-синий); | <input type="checkbox"/> teal — сине-зеленый; |
| <input type="checkbox"/> silver — серебристый;         | <input type="checkbox"/> purple — фиолетовый; |
| <input type="checkbox"/> blue — синий;                 | <input type="checkbox"/> red — красный;       |
| <input type="checkbox"/> green — зеленый;              | <input type="checkbox"/> yellow — желтый;     |
| <input type="checkbox"/> maroon — коричневый;          | <input type="checkbox"/> fuchsia — сиреневый. |

Для задания цвета тексту можно применить следующую строку:

```
<font color=blue>текст заданного цвета</font>
```

Можно определить цвет фона и цвет текста страницы:

```
<body bgcolor=black text=aqua>
```

## Таблицы

Для отображения таблицы необходимо определить строки и ячейки. Строки определяются парой тегов `<tr></tr>`, которые должны находиться внутри секции, определяемой тегами `<table></table>`. Атрибуты следующие:

- height= "*значение*" — высота строки в пикселах или процентах;
- bgcolor="цвет" — цвет фона строки;
- background="ссылка на файл рисунка" — рисунок фона.

Данные могут помещаться только в ячейках. Ячейка определяется внутри строки парой тегов `<td></td>`. Атрибуты те же, что и у строки, но добавляется еще атрибут width.

Получается следующая иерархия:

```
<table border="1">
  <tr>
    <td>Данные1</td>
  </tr>
</table>
```

Таблицы можно вкладывать одну в другую. Вот пример:

```
<table width="75%" border="1" bgcolor="#FFFF00">
  <tr>
    <td width="33%">Ячейка 1</td>
    <td bgcolor="#0000FF" width="33%">
      <table width="100%" border="1" bgcolor="#FFFFFF">
        <tr>
```

```

        <td height="14">Вложенная таблица </td>
    </tr>
    <tr>
        <td> </td>
    </tr>
    <tr>
        <td> </td>
    </tr>
</table>
</td>
<td width="33%" bgcolor="#FF0000">Ячейка 3</td>
</tr>
</table>

```

Таблицы используют не только для отображения табличных данных. Практически все авторы Web-страниц форматируют документы с помощью таблиц. Таблицы помогают разместить данные на странице в требуемом порядке. Например, без таблицы трудно разместить обычный текст в две колонки либо создать дополнительную колонку со ссылками или меню.

При создании таблиц следует помнить о том, что ширина таблицы никогда не будет меньше той, что указана в атрибуте `width` тега `<table>`, но будет всегда больше значения этого атрибута, если суммирующая ширина ячеек больше этого значения. То же справедливо и для высоты. Ширина или высота ячеек будет всегда больше определяемой параметрами, если в ячейке помещен элемент с большей шириной или высотой (например, рисунок). Высота ячеек в одной строке всегда будет одинакова или равна заданной высоте (`<tr height="30">`, например) или высоте ячейки с самым "высоким" элементом. Ширина и высота складывается не только из заданных значений, к ним нужно еще прибавлять расстояния между ячейками (атрибут `cellspacing` в теге `<table>`). Цвет и рисунок фона можно переопределять, как в примере, приведенном ранее — для всей таблицы — один цвет, для определенной строки — другой, для каждой отдельной ячейки тоже можно установить свой цвет фона или рисунок.

При создании таблиц можно пользоваться еще парой тегов `<th></th>`. Они определяют заголовки колонок. Их можно вставлять непосредственно за тегом `<table>`, т. е. необязательно внутри строки.

Само собой разумеется, что можно размещать текст и изображения внутри ячеек таблиц.

Рассмотренные средства — это минимум, необходимый для создания простых Web-страниц. Приобретите печатное руководство по языку HTML или посетите страницы по ссылке <http://www.citforum.ru/internet/html/index.shtml>.

## Что такое служба каталогов?

Каталог (directory) — это информационный ресурс, используемый для хранения сведений о каком-либо объекте. Например, телефонный справочник (каталог теле-

фонных номеров) содержит информацию об абонентах телефонной сети. В файловой системе каталоги хранят информацию о файлах.

В распределенной вычислительной системе или в компьютерной сети общего пользования, как например Интернет, имеется множество объектов, например, принтеры, факс-серверы, приложения, базы данных и др. Пользователи хотят иметь доступ к каждому из таких объектов и работать с ними, а администраторы — управлять правилами использования этих объектов.

Термины "каталог" (directory) и "служба каталогов" (directory service) относятся к каталогам, размещаемым в частных сетях и сетях общего пользования. Служба каталогов отличается от каталога тем, что она является не только информационным ресурсом, но также представляет собой услугу, обеспечивающую поиск и доставку пользователю необходимой ему информации.

## Зачем нужна служба каталогов?

Служба каталогов — одна из наиболее важных составных частей развитой компьютерной системы. Пользователи и администраторы зачастую не знают точных имен нужных им объектов, которые им в данный момент требуются. Они могут знать один или несколько их признаков или атрибутов и могут послать запрос к каталогу, получив в ответ список тех объектов, атрибуты которых совпадают с указанными в запросе. Например, запрос может выглядеть следующим образом: "Найти все дуплексные принтеры в здании 2б". Служба каталогов позволяет найти любой объект по одному из его атрибутов.

Служба каталогов позволяет:

- обеспечивать защиту информации от вмешательства посторонних лиц в рамках, установленных администратором системы;
- распространять каталог среди других компьютеров в сети;
- проводить репликацию (тиражирование) каталога, делая его доступным для большего числа пользователей и более защищенным от потери данных;
- разделять каталог на несколько частей, обеспечивая возможность хранения очень большого числа объектов.

Служба каталогов — это одновременно и инструмент управления, и пользовательский инструмент. По мере роста числа объектов в сети служба каталогов начинает играть все более важную роль. Можно сказать, что служба каталогов — это та основа, на которой строится вся работа крупной распределенной компьютерной системы.

## Active Directory

Active Directory — это служба каталогов, входящая в Windows 2000 Server. Она не только расширяет возможности служб каталогов предыдущих Windows-систем, но и обладает совершенно новыми свойствами. Служба Active Directory является защищенной, распределенной, сегментированной и реплицируемой. Она предназначена для надежной работы в системе любого размера — от отдельного сервера, работающего с несколькими сотнями объектов, до нескольких тысяч серверов

с миллионами объектов. Active Directory обладает рядом новых свойств, которые облегчают поиск объектов и управление большими объемами информации; она также обеспечивает экономию времени пользователей и администраторов системы.

## Основные понятия

Часть понятий и терминов, используемых для описания Active Directory, не представляет ничего нового, другие же раньше не использовались. К сожалению, некоторые из использовавшихся ранее терминов не имеют однозначного толкования. Прежде чем приступить к знакомству с Active Directory, определим значения ряда терминов применительно к этой службе каталогов.

### Область действия

Область действия Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать несколько объединенных сетей. Некоторые из рассматриваемых далее терминов относятся к группе сетей, поэтому важно помнить, что Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

### Пространство имен

Active Directory, как и любая другая служба каталогов, является, прежде всего, пространством имен. *Пространство имен* — это такая ограниченная область, в которой может быть распознано данное имя. Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Например, телефонный справочник представляет собой пространство имен, в котором именам телефонных абонентов могут быть поставлены в соответствие телефонные номера. Файловая система Windows образует пространство имен, в котором имя файла может быть поставлено в соответствие конкретному файлу.

Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

### Объект

*Объект* — это непустой, именованный набор атрибутов, обозначающий нечто конкретное, например пользователя, принтер или приложение. Атрибуты содержат информацию, однозначно описывающую данный объект. Атрибуты пользователя могут включать имя пользователя, его фамилию и адрес электронной почты.

### Контейнер

*Контейнер* аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имен. Однако, в отличие от объекта, контейнер не обо-

значает ничего конкретного — он может содержать группу объектов или другие контейнеры.

## Дерево

Термин "дерево" используется в данном документе для описания иерархии объектов и контейнеров. Как правило, конечными элементами дерева являются объекты. В узлах (точках ветвления) дерева располагаются контейнеры. Дерево отражает взаимосвязь между объектами или указывает путь от одного объекта к другому. Простой каталог представляет собой контейнер. Компьютерная сеть или домен тоже являются контейнерами. *Непрерывным поддеревом* называют любую непрерывную часть дерева, включающую все элементы каждого входящего в нее контейнера.

## Имя

Имена используются для различения объектов в Active Directory. Служба Active Directory допускает существование двух типов имен.

### Уникальное имя

Каждый объект в Active Directory имеет *уникальное имя* (Distinguished Name, DN). Это имя содержит указание на домен, в котором находится объект, и полный путь в иерархической структуре контейнеров, который приводит к данному объекту. Типичным уникальным именем (DN) является имя

```
/O=Internet/DC=COM/DC=Microsoft/CN=Users/CN=James Smith
```

Это имя обозначает объект типа "пользователь" с именем "James Smith", находящийся в домене Microsoft.com.

### Относительное имя

Относительное уникальное имя объекта (Relative Distinguished Name, RDN) — это та часть имени, которая сама является частью атрибута объекта. В приведенном ранее примере RDN-именем объекта "James Smith" является групповое имя (CN) CN=James Smith. RDN-именем родительского объекта является имя CN=Users.

### Контексты имен и сегменты

Active Directory может состоять из одного или нескольких контекстов имен или сегментов. Контекстом имен может быть любое непрерывное поддерево каталога. Контексты имен являются единицами репликации.

В Active Directory каждый сервер всегда содержит не менее трех контекстов имен:

- логическую структуру;
- конфигурацию (топологию репликации и соответствующие метаданные);
- один или несколько пользовательских контекстов имен (поддерева, содержащие объединенные в каталог объекты).

## Домены

Домен — это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows NT или Windows 2000. (Более подробную информацию о доменах можно найти в документации по операционным системам Windows.) Active Directory состоит из одного или нескольких доменов. Применительно к отдельной рабочей станции доменом является сама рабочая станция. Границы одного домена могут охватывать более чем одно физическое устройство. Каждый домен может иметь свои правила защиты информации и правила взаимодействия с другими доменами. Если несколько доменов связаны друг с другом доверительными отношениями и имеют единую логическую структуру, конфигурацию и глобальный каталог, то говорят о дереве доменов. Несколько доменных деревьев могут быть объединены в лес.

## Дерево доменов

Дерево доменов (дерево) состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное пространство имен. Домены в дереве связаны между собой доверительными отношениями. Active Directory является множеством, которому принадлежат одно или несколько деревьев.

Дерево графически можно представить двумя способами: либо через доверительные отношения между доменами, либо через пространство имен доменного дерева.

### Представление доменного дерева через доверительные отношения

Доверительные отношения между несколькими доменами, объединенными в дерево, можно представить в виде схемы.

Доверительные отношения между доменами в ОС Windows 2000 устанавливаются на основе протокола безопасности Kerberos. Отношения, установленные с помощью этого протокола, обладают свойствами транзитивности и иерархичности: если домен А доверяет домену В и домен В доверяет домену С, то домен А доверяет и домену С.

### Представление доменного дерева через пространство имен

Доменное дерево можно также схематически изобразить с помощью пространства имен. Уникальное имя объекта можно определить, двигаясь вверх по доменному дереву, начиная с объекта. Такой метод оказывается удобным при объединении объектов в логическую, иерархическую структуру. Главное достоинство непрерывного пространства имен состоит в том, что глубокий поиск, проводимый от корня дерева, позволяет просмотреть все иерархические уровни пространства имен.

## Лес

*Лесом* называется одно или несколько деревьев, которые не образуют непрерывного пространства имен. Все деревья одного леса имеют общие логическую

структуру, конфигурацию и глобальный каталог. Все деревья данного леса поддерживают друг с другом транзитивные иерархические, доверительные отношения, устанавливаемые на основе протокола Kerberos. В отличие от дерева, лес может не иметь какого-то определенного имени. Лес существует в виде совокупности объектов с перекрестными ссылками и доверительных отношений на основе протокола Kerberos, установленных для входящих в лес деревьев. Поддержка протокола Kerberos требует, чтобы деревья одного леса составляли иерархическую структуру: имя дерева, располагающегося в корне этой структуры, может использоваться для обозначения всего данного леса деревьев.

## Узлы

*Узлом* называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP и характеризующихся хорошим качеством связи. "Хорошее" качество связи в данном случае подразумевает высокую надежность и скорость передачи данных (например, для локальных сетей это означает скорость передачи порядка 10 Мбит/с или выше). Определение узла как совокупности подсетей позволяет администратору быстро и без больших затрат настроить топологию доступа и репликации в Active Directory и полнее использовать достоинства физического расположения устройств в сети. Когда пользователь входит в систему, клиент Active Directory ищет серверы Active Directory, расположенные в узле пользователя. Поскольку компьютеры, принадлежащие к одному узлу, в масштабах сети можно считать расположенными близко друг к другу, связь между ними должна быть быстрой, надежной и эффективной. Распознавание локального узла в момент входа в систему не составляет труда, т. к. рабочая станция пользователя уже знает, в какой из подсетей TCP/IP она находится, а подсети напрямую соответствуют узлам Active Directory.

Создавая простую сеть на основе Windows 2000 Server, начинающие администраторы стараются упростить настройки сервера и не устанавливают Active Directory. Но практически все основные возможности, связанные с рациональным управлением сетью на основе новых операционных систем семейства Windows, основаны на возможностях Active Directory. Не поленитесь, потратьте день-другой на установку и настройку Active Directory. Впоследствии вы не пожалеете об этом. Даже в простой сети вы сможете более эффективно управлять правами пользователей и компьютеров. Некоторые задачи, которые в простой сети, не использующей Active Directory, могут быть решены лишь с применением дополнительного оборудования (маршрутизаторов, например), с Active Directory могут быть решены средствами самой операционной системы. Так, например, можно гибко распределить права на ресурсы сети между пользователями и компьютерами, разрешив использовать отдельные принтеры некоторой группе пользователей, но запретив доступ к другим ресурсам компьютеров, к которым эти принтеры подключены. Создавая локальные и глобальные группы пользователей, можно глобальной группе дать права на доступ к ресурсам второго домена сети (нужен второй сервер).

## Спецификации на допустимые расстояния кабеля в сети Ethernet

### □ 10BASE-T (витая пара)

Максимальная длина сегмента — 300 футов или 100 м. Концентратор может использовать 100-омные разъемы RJ-45 или Telco RJ-21.

### □ 100BASE TX (витая пара)

Максимальная длина сегмента — 300 футов или 100 м. RJ-45. Используются 100-омные разъемы.

### □ 100BASE-FX (оптоволоконный кабель)

Оптоволоконная линия 100BASE-FX поддерживает расстояние между коммутаторами 1320 футов или 400 м (по кабелю 62,5/125 мкм). Применяются разъемы SC.

### □ 10BASE-5 (коаксиальный кабель, для связи с концентратором нужен трансивер)

Максимальная длина сегмента — 1650 футов или 500 м. 100 трансиверов на сегмент. Расстояние между трансиверами — 7,7 футов или 2,5 м. Абсолютный максимум длины маршрута между оконечным оборудованием данных (DTE) — 9900 футов или 3000 м. Используются 50-омные разъемы *N*-типа.

### □ 10BASE-2 (тонкий коаксиальный кабель)

Максимальная длина сегмента — 613,5 футов или 185 м. До 30 трансиверов на сегмент. Минимальное расстояние между трансиверами — 1,55 фута или 0,5 м. Абсолютный максимум длины маршрута между оконечным оборудованием данных (DTE) — 4620 футов или 1400 м. Применяются 50-омные разъемы BNC.

### □ 10BASE-FL (оптоволоконный кабель)

Оптоволоконные линии 10BASE-FL поддерживают расстояние 6600 футов или 2000 м для кабеля 62,5 или 125 мкм. Абсолютный максимум длины маршрута между оконечным оборудованием данных (DTE) — 13200 футов или 4000 м.



# ПРИЛОЖЕНИЕ 5

## Наиболее используемые команды Linux

В этом приложении приведены наиболее употребительные команды Linux в виде примеров их выполнения и пояснениями к примерам. Таблица П5.1 может быть справочным руководством по командам, которые распределены по нескольким разделам. Дополнительную информацию о командах можно получить, введя команду без параметров или с параметром `-h`.

*Таблица П5.1. Наиболее употребительные команды Linux*

Системная информация		
№	Команда	Описание
1	<code>Arch</code>	Показать архитектуру машины (1)
2	<code>uname -m</code>	Показать архитектуру машины (2)
3	<code>uname -r</code>	Показать версию используемого ядра
4	<code>dmidecode -q</code>	Показать аппаратные компоненты системы (SMBIOS/DMI)
5	<code>hdparm -i /dev/hda</code>	Отобразить характеристики жесткого диска
6	<code>hdparm -tT /dev/sda</code>	Выполнить тест чтения жесткого диска
7	<code>cat /proc/cpuinfo</code>	Показать информацию о процессоре
8	<code>cat /proc/interrupts</code>	Показать прерывания
9	<code>cat /proc/meminfo</code>	Проверить использование памяти
10	<code>cat /proc/swaps</code>	Показать swar-файл(ы)
11	<code>cat /proc/version</code>	Показать версию ядра
12	<code>cat /proc/net/dev</code>	Показать сетевые адаптеры и статистику
13	<code>cat /proc/mounts</code>	Показать смонтированные файловые системы
14	<code>lspci -tv</code>	Отобразить устройства PCI
15	<code>lsusb -tv</code>	Показать устройства USB
16	<code>date</code>	Показать системную дату
17	<code>Cal 2008</code>	Показать календарь на 2008 год

Таблица П5.1 (продолжение)

<b>Системная информация</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
18	date 081219302008.15	Установить дату и время — <МесяцДеньЧасМинутыГод.Секунды>
19	clock -w	Сохранить изменения даты в BIOS
<b>Завершение работы, перезагрузка, завершение сеанса</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
20	shutdown -h now	Завершить работу системы (1)
21	shutdown -h hours:minutes &	Запланировать завершение работы системы (выключение компьютера)
22	shutdown -c	Отменить запланированное завершение работы системы
23	shutdown -r now	Перезагрузить (1)
23	reboot	Перезагрузить (2)
25	logout	Завершение сеанса
<b>Файлы и директории</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
26	cd /home	Перейти в каталог /home
27	cd ..	Перейти в каталог на один уровень выше
28	cd ../../	Перейти в каталог на два уровня выше
29	cd	Перейти в домашний каталог
30	cd ~user1	Перейти в домашний каталог
31	cd -	Перейти в предыдущий каталог
32	pwd	Показать путь к рабочему каталогу
33	ls	Просмотр списка файлов в каталоге
34	ls -F	Просмотр списка файлов в каталоге
35	ls -l	Показать детализированную информацию о файлах и каталогах (права доступа, время соз- дания, владелец, размер)
36	ls -a	Показать скрытые файлы
37	ls *[0-9]*	Показать файлы и каталоги, имена которых содержат числа
38	mkdir dir1	Создать каталог с именем "dir1"
39	mkdir dir1 dir2	Создать два каталога одновременно
40	mkdir -p /tmp/dir1/dir2	Создать вложенные каталоги
41	rm -f file1	Удалить файл с именем "file1"
42	rmdir dir1	Удалить каталог с именем "dir1"
43	rm -rf dir1	Рекурсивно удалить каталог "dir1" и его содер- жимое

Таблица П5.1 (продолжение)

Файлы и директории		
№	Команда	Описание
44	<code>rm -rf dir1 dir2</code>	Рекурсивно удалить два каталога "dir1" и "dir2" и их содержимое
45	<code>mv dir1 new_dir</code>	Переименовать/переместить файл или каталог
46	<code>cp file1 file2</code>	Копировать файл
47	<code>cp dir/* .</code>	Копировать все файлы каталога в рабочий каталог
48	<code>cp -a /tmp/dir1 .</code>	Копировать каталог в рабочий каталог
49	<code>cp -a dir1 dir2</code>	Копировать каталог
50	<code>ln -s file1 lnk1</code>	Создать символическую ссылку на каталог или файл
51	<code>ln file1 lnk1</code>	Создать физическую ссылку на каталог или файл
52	<code>touch -t 0712250000 file1</code>	Изменить штамп времени файла или каталога <YYMMDDhhmm>
53	<code>file file1</code>	Выводит в виде текста информацию о типе файла
54	<code>iconv -l</code>	Выводит список известных кодировок
55	<code>iconv -f fromEncoding -t toEncoding inputFile &gt; outputFile</code>	Перекодирует файл "inputFile" из кодировки fromEncoding в кодировку toEncoding, создавая новый файл "outputFile"
56	<code>find . -maxdepth 1 -name *.jpg -print -exec convert '{}' -resize 80x60 "thumbs/{}" \;</code>	Пакет команд изменяет размеры графических файлов из текущего каталога и создает измененные копии (эскизы) в каталоге thumbs (требуется наличия конвертера из Imagemagick)
Поиск файлов		
№	Команда	Описание
57	<code>find / -name file1</code>	Поиск файла или каталога в файловой системе, начиная с корневого каталога
58	<code>find / -user user1</code>	Поиск файлов или каталогов, принадлежащих пользователю "user1"
59	<code>find /home/user1 -name \*.bin</code>	Поиск файлов с расширением bin в каталоге /home/user1
60	<code>find /usr/bin -type f -atime +100</code>	Поиск бинарных файлов, не использовавшихся за прошедшие 100 дней
61	<code>find /usr/bin -type f -mtime -10</code>	Поиск файлов или каталогов, измененных за прошедшие 10 дней
62	<code>find / -name \*.rpm -exec chmod 755 '{}'</code> <code>\;</code>	Поиск файлов с расширением rpm и изменение прав доступа к ним
63	<code>find / -xdev -name \*.rpm</code>	Поиск файлов с расширением rpm только на жестких дисках. Сменные носители игнорируются

Таблица П5.1 (продолжение)

Поиск файлов		
№	Команда	Описание
64	<code>locate \*.ps</code>	Поиск файлов с расширением ps (предварительно необходимо выполнить команду <code>updatedb</code> )
65	<code>whereis halt</code>	Показать местоположение бинарного исполняемого файла, содержащего руководства, относящиеся к файлу "halt"
66	<code>which halt</code>	Отображает полный путь к файлу "halt"
Монтирование файловых систем		
№	Команда	Описание
67	<code>mount /dev/hda2 /mnt/hda2</code>	Монтировать диск с именем hda2 с проверкой существования каталога /mnt/hda2
68	<code>umount /dev/hda2</code>	Монтировать диск с именем hda2. Необходим выход из точки монтирования mnt/hda2
69	<code>fuser -km /mnt/hda2</code>	Быстрое монтирование, когда устройство занято
70	<code>umount -n /mnt/hda2</code>	Выполнение команды <code>umount</code> без записи в файл <code>/etc/mtab</code> . Полезно, когда файл только для чтения или жесткий диск переполнен
71	<code>mount /dev/fd0 /mnt/floppy</code>	Монтировать гибкий диск
72	<code>mount /dev/cdrom /mnt/cdrom</code>	Монтировать CD или DVD
73	<code>mount /dev/hdc /mnt/cdrecorder</code>	Монтировать CD-R/CD-RW или DVD-R/DVD-RW(±)
74	<code>mount -o loop file.iso /mnt/cdrom</code>	Монтировать файл ISO-образа диска
75	<code>mount -t vfat /dev/hda5 /mnt/hda5</code>	Монтировать файловую систему FAT32
76	<code>mount /dev/sda1 /mnt/usbdisk</code>	Монтировать USB флэш-диск
77	<code>mount -t smbfs -o username=user,password=pass //WinClient/share /mnt/share</code>	Монтировать ресурс сети Windows
78	<code>mount -o bind /home/user/prg /var/ftp/user</code>	Монтирует каталог в каталог (binding). Доступна с версии ядра 2.4.0. Полезна, например, для предоставления содержимого пользовательского каталога через FTP. Выполнение данной команды сделает копию содержимого <code>/home/user/prg</code> в <code>/var/ftp/user</code>
Дисковое пространство		
№	Команда	Описание
79	<code>df -h</code>	Показать список примонтированных разделов
80	<code>ls -lSr   more</code>	Показать размер файлов и каталогов, упорядоченных по размеру
81	<code>du -sh dir1</code>	Оценить место, используемое каталогом "dir1"
82	<code>du -sk *   sort -rn</code>	Показать размер файлов и каталогов, отсортированных по размеру

Таблица П5.1 (продолжение)

Дисквое пространство		
№	Команда	Описание
83	<code>rpm -q -a --qf '%10{SIZE}t%{NAME}n'   sort -k1,1n</code>	Показать размер дискового пространства, используемого RPM-пакетами, с сортировкой по размеру (в системах Fedora, RedHat и на их основе)
84	<code>dpkg-query -W -f='\${Installed-Size;10}t\${Package}n'   sort -k1,1n</code>	Показать место, используемое DEB-пакетами, установив сортировку по размеру (в системах Ubuntu, Debian и на их основе)
Пользователи и группы		
№	Команда	Описание
85	<code>groupadd group_name</code>	Создание новой группы
86	<code>groupdel group_name</code>	Удаление группы
87	<code>groupmod -n new_group_name old_group_name</code>	Переименование группы
88	<code>useradd -c "Name Surname " -g admin -d /home/user1 -s /bin/bash user1</code>	Создание нового пользователя, принадлежащего группе admin
89	<code>useradd user1</code>	Создание нового пользователя
90	<code>userdel -r user1</code>	Удаление пользователя (-r удаляет домашний каталог)
91	<code>usermod -c "User FTP" -g system -d /ftp/user1 -s /bin/nologin user1</code>	Изменить пользовательские атрибуты
92	<code>gpasswd -a (-d)userid group-name</code>	Добавить (удалить) члена группы. Используется числовой идентификатор пользователя.
93	<code>passwd</code>	Сменить пароль
94	<code>passwd user1</code>	Изменить пользовательский пароль (доступно только администратору)
95	<code>chage -E 2005-12-31 user1</code>	Установить дату окончания действия учетной записи пользователя "user1"
96	<code>pwck</code>	Проверка синтаксиса и формата файла /etc/passwd, существования пользователей и их каталогов
97	<code>grpck</code>	Проверка синтаксиса и формата файла /etc/group, существования групп
98	<code>newgrp group_name</code>	Вход в новую группу, чтобы изменить группу по умолчанию для вновь создаваемых файлов
Права доступа к файлам		
№	Команда	Описание
99	<code>ls -lh</code>	Показать права доступа
100	<code>ls /tmp   pr -T5 -W\$COLUMNS</code>	Вывод списка файлов и каталогов с разделением его в терминале на пять колонок
101	<code>chmod ugo+rxw directory1</code> или <code>chmod 777 directory1</code>	Установка разрешений доступа на чтение (r), запись (w), исполнение (x) для пользователей владельцев (u), групп (g) и других (o)

Таблица П5.1 (продолжение)

Права доступа к файлам		
№	Команда	Описание
102	<code>chmod go-rwx directory1</code>	Удалить разрешения доступа на чтение (r), запись (w), исполнение (x) для группы пользователей (g) и других (o)
103	<code>chown user1 file1</code>	Назначить владельцем файла пользователя "user1"
104	<code>chown -R user1 directory1</code>	Назначить владельцем каталога и всех файлов и каталогов, содержащихся внутри, пользователя "user1"
105	<code>chgrp group1 file1</code>	Изменить группу-владельца файла
106	<code>chown user1:group1 file1</code>	Изменить владельца и группу-владельца файла
107	<code>find / -perm -u+s</code>	Просмотреть все файлы в системе с установленным атрибутом SUID
108	<code>chmod u+s /bin/file1</code>	Установка атрибута SUID для бинарного файла, чтобы пользователь при его исполнении получил права владельца этого файла
109	<code>chmod u-s /bin/file1</code>	Снятие атрибута SUID для бинарного файла
110	<code>chmod g+s /home/public</code>	Установка атрибута SGID для каталога (передаются права группы владельца)
111	<code>chmod g-s /home/public</code>	Снятие атрибута SGID для каталога
112	<code>chmod o+t /home/public</code>	Установка атрибута STICKY для каталога — позволяет удаление файлов только законным владельцам
113	<code>chmod o-t /home/public</code>	Снятие атрибута STICKY для каталога
Специальные атрибуты файлов		
№	Команда	Описание
114	<code>chattr +a file1</code>	Разрешает запись в файл только в режиме добавления
115	<code>chattr +c file1</code>	Разрешает сжатие и распаковку файла автоматически ядром
116	<code>chattr +d file1</code>	Указывает утилите <code>dump</code> игнорировать данный файл во время выполнения <code>backup</code>
117	<code>chattr +i file1</code>	Этот атрибут делает невозможным удаление, изменение, переименование или связывание (создание ссылки)
118	<code>chattr +S file1</code>	Указывает, что при сохранении изменений будет произведена синхронизация, как при выполнении команды <code>sync</code>
119	<code>chattr +s file1</code>	Разрешает безопасное удаление файла, место, занимаемое файлом на диске, заполняется нулями, что предотвращает возможность восстановления данных

Таблица П5.1 (продолжение)

Специальные атрибуты файлов		
№	Команда	Описание
120	chattr +u file1	Позволяет восстанавливать содержание файла, даже если файл будет удален
121	lsattr	Показать специальные атрибуты
Архивирование и сжатие файлов		
№	Команда	Описание
122	bunzip2 file1.bz2	Распаковать файл "file1.bz2"
123	bzip2 file1	Сжать файл "file1"
124	gunzip file1.gz	Распаковать файл "file1.gz"
125	gzip file1	Сжать файл "file1"
126	gzip -9 file1	Архивирование с максимальным сжатием
127	rar a file1.rar test_file	Создать rar-архив "file1.rar"
128	rar a file1.rar file1 file2 dir1	Сжать "file1", "file2" и "dir1" одновременно
129	rar x file1.rar	Создать архив rar
130	unrar x file1.rar	Распаковать архив rar
131	tar -cvf archive.tar file1	Создать несжатый tarball
132	tar -cvf archive.tar file1 file2 dir1	Создать архив, содержащий "file1", "file2" и "dir1"
133	tar -tf archive.tar	Показать содержание архива
134	tar -xvf archive.tar	Извлечение tarball
135	tar -xvf archive.tar -C /tmp	Извлечение tarball в /tmp
136	tar -cvfj archive.tar.bz2 dir1	Создать tarball, сжатый в bzip2
137	tar -xvfj archive.tar.bz2	Распаковать архив tar, сжатый в bzip2
138	tar -cvfz archive.tar.gz dir1	Создать tarball, сжатый в gzip
139	tar -xvfz archive.tar.gz	Декомпрессируйте сжатый архив tar в gzip
140	zip file1.zip file1	Создать архив, сжатый в zip
141	zip -r file1.zip file1 file2 dir1	Сжатие в zip одновременно нескольких файлов
142	unzip file1.zip	Распаковать архив zip
RPM-пакеты (установка и удаление программ)		
№	Команда	Описание
143	rpm -ivh package.rpm	Установить пакет rpm
144	rpm -ivh --nodeeps package.rpm	Установить пакет rpm, но игнорировать зависимости
145	rpm -U package.rpm	Обновить пакет rpm, не изменяя файлы конфигурации
146	rpm -F package.rpm	Обновить пакет rpm, если он уже установлен
147	rpm -e package_name.rpm	Удалить пакет rpm

Таблица П5.1 (продолжение)

RPM-пакеты (установка и удаление программ)		
№	Команда	Описание
148	<code>rpm -qa</code>	Показать все пакеты rpm, установленные в системе
149	<code>rpm -qa   grep httpd</code>	Показать все пакеты rpm с именем httpd
150	<code>rpm -qi package_name</code>	Получить информацию об установленном пакете
151	<code>rpm -qg "System Environment/Daemons"</code>	Показать пакеты rpm определенной группы приложений
152	<code>rpm -ql package_name</code>	Показать список файлов, созданных установленным пакетом rpm
153	<code>rpm -qc package_name</code>	Показать список файлов конфигурации, созданных установленным пакетом rpm
154	<code>rpm -q package_name --whatrequires</code>	Показать список зависимостей, требуемых для пакета rpm
155	<code>rpm -q package_name --whatprovides</code>	Показать совместимость пакета rpm
156	<code>rpm -q package_name --scripts</code>	Показать сценарии, запущенные при установке/удалении пакета
157	<code>rpm -q package_name --changelog</code>	История просмотров пакета
158	<code>rpm -qf /etc/httpd/conf/httpd.conf</code>	Проверить, какой пакет rpm принадлежит данному файлу
159	<code>rpm -qp package.rpm -l</code>	Показать список файлов, создаваемых пакетом rpm, если он еще не установлен
160	<code>rpm --import /media/cdrom/RPM-GPG-KEY</code>	Импортировать публичный ключ цифровой подписи
161	<code>rpm --checksig package.rpm</code>	Проверить целостность пакета rpm
162	<code>rpm -qa gpg-pubkey</code>	Проверить целостность всех установленных пакетов rpm
163	<code>rpm -V package_name</code>	Проверить размер файла, разрешения, тип, владельца, группу, контрольную сумму MD5 и последнюю модификацию
164	<code>rpm -Va</code>	Проверить все пакеты rpm, установленные в системе. Использовать с предостережением
165	<code>rpm -Vp package.rpm</code>	Проверить пакет rpm, еще не установленный
166	<code>rpm2cpio package.rpm   cpio --extract --make-directories *bin*</code>	Извлечь исполняемый файл из пакета rpm
167	<code>rpm -ivh /usr/src/redhat/RPMS/`arch`/package.rpm</code>	Установить пакет, построенный из исходника rpm
168	<code>Rpmbuild --rebuild package_name.src.rpm</code>	Создать пакет rpm из исходника rpm
YUM-пакеты (установка и удаление программ)		
№	Команда	Описание
169	<code>yum install package_name</code>	Загрузить и установить пакет



Таблица П5.1 (продолжение)

YUM-пакеты (установка и удаление программ)		
№	Команда	Описание
170	<code>yum localinstall package_name.rpm</code>	Установка пакета с попыткой разрешения зависимостей
171	<code>yum update package_name.rpm</code>	Обновить все пакеты, установленные в системе
172	<code>yum update package_name</code>	Обновить пакет
173	<code>yum remove package_name</code>	Удалить пакет
174	<code>yum list</code>	Показать список всех пакетов, установленных в системе
175	<code>yum search package_name</code>	Найти пакет <code>rpm</code> в репозитории
176	<code>yum clean packages</code>	Очистить кэш удаления загруженных пакетов <code>rpm</code>
177	<code>yum clean headers</code>	Удалить все заголовочные файлы, которые система использовала для разрешения зависимостей
178	<code>yum clean all</code>	Удалить из кэша информацию о пакетах и заголовочных файлах
DEB-пакеты (установка и удаление программ)		
№	Команда	Описание
179	<code>dpkg -i package.deb</code>	Установка/обновление <code>deb</code> -пакетов
180	<code>dpkg -r package_name</code>	Удаление <code>deb</code> -пакетов
181	<code>dpkg -l</code>	Показать все <code>deb</code> -пакеты, установленные в системе
182	<code>dpkg -l   grep httpd</code>	Показать все <code>deb</code> -пакеты установленные в системе с именем "httpd"
183	<code>dpkg -s package_name</code>	Получить информацию относительно определенного пакета, установленного в системе
184	<code>dpkg -L package_name</code>	Показать список файлов, принадлежащих пакету, установленному в системе
185	<code>dpkg --contents package.deb</code>	Показать список файлов, принадлежащих установленному пакету; проверить, какой пакет принадлежит данному файлу
186	<code>dpkg -S /bin/ping</code>	Проверить, какой пакет принадлежит данному файлу
187	<code>apt-get install package_name</code>	Установить/обновить пакет
188	<code>apt-cdrom install package_name</code>	Установить/обновить пакет с CD-ROM
189	<code>apt-get update</code>	Обновить список пакетов
190	<code>apt-get upgrade</code>	Обновить все установленные пакеты
191	<code>apt-get remove package_name</code>	Удалить пакет из системы
192	<code>apt-get check</code>	Проверить зависимости
193	<code>apt-get clean</code>	Очистить кэш от загруженных пакетов

Таблица П5.1 (продолжение)

<b>ДЕБ-пакеты (установка и удаление программ)</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
194	<code>apt-cache search searched-package</code>	Получить список пакетов, содержащих строку "searched-packages"
<b>Работа с текстом</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
195	<code>cat file1</code>	Показать содержимое текстового файла (на стандартном устройстве вывода)
196	<code>tac file1</code>	Показать содержимое текстового файла в обратном порядке (на стандартном устройстве вывода)
197	<code>cat file1   command( sed, grep, awk, grep, etc...) &gt; result.txt</code>	Работа с тестом в файле и запись результата в новый файл
198	<code>cat file1   command( sed, grep, awk, grep, etc...) &gt;&gt; result.txt</code>	Работа с тестом в файле, результат добавляется в существующий файл
199	<code>more file1</code>	Постраничный вывод содержимого файла "file1" на стандартное устройство вывода
200	<code>less file1</code>	Постраничный вывод содержимого файла "file1" на стандартное устройство вывода, но с возможностью пролистывания в обе стороны (вверх-вниз), поиска по содержимому и т. п.
201	<code>head -2 file1</code>	Вывести первые две строки файла "file1" на стандартное устройство вывода. По умолчанию выводится десять строк
202	<code>tail -2 file1</code>	Вывести последние две строки файла "file1" на стандартное устройство вывода. По умолчанию выводится десять строк
203	<code>tail -f /var/log/messages</code>	Выводить содержимое файла "/var/log/messages" на стандартное устройство вывода по мере появления в нем текста
204	<code>grep Aug /var/log/messages</code>	Поиск слова "Aug" в файле "/var/log/messages"
205	<code>grep ^Aug /var/log/messages</code>	Поиск слов, которые начинаются с "Aug" в файле "/var/log/messages"
206	<code>grep [0-9] /var/log/messages</code>	Выбрать из файла "/var/log/messages" все строки, которые содержат числа
207	<code>grep Aug -R /var/log/*</code>	Искать строку "Aug" в файлах каталога "/var/log" и вложенных каталогах
208	<code>sed 's/string1/string2/g' example.txt</code>	Заменить строку "string1" на "string2" в файле "example.txt"
209	<code>sed '/^\$/d' example.txt</code>	Удалить все пустые строки из файла "example.txt"
210	<code>sed '/ *#/d; /^\$/d' example.txt</code>	Удалить комментарии и пустые строки в файле "example.txt"
211	<code>echo 'esempio'   tr '[:lower:]' '[:upper:]'</code>	Конвертировать текст из строчных букв в прописные

Таблица П5.1 (продолжение)

Работа с текстом		
№	Команда	Описание
212	<code>sed -e '1d' example.txt</code>	Удалить первую строку из файла "example.txt"
213	<code>sed -n '/string1/p'</code>	Просмотр строк, которые содержат слово "string1"
214	<code>sed -e 's/ *\$//' example.txt</code>	Удалить пустые символы в конце каждой строки
215	<code>sed -e 's/string1//g' example.txt</code>	Удалить из текста слово "string1", оставив остальной текст неизменным
216	<code>sed -n '1,5p;5q' example.txt</code>	Просмотр от 1-й до 5-й строки
217	<code>sed -n '5p;5q' example.txt</code>	Просмотр пятой строки
218	<code>sed -e 's/00*/0/g' example.txt</code>	Заменить несколько нулей единственным нулем
219	<code>cat -n file1</code>	Пронумеровать строки при выводе содержимого файла
220	<code>cat example.txt   awk 'NR%2==1'</code>	При выводе содержимого файла не выводить четные строки файла
221	<code>echo a b c   awk '{print \$1}'</code>	Вывести первую колонку. Разделение по умолчанию, по пробелу/пробелам или символу/символам табуляции
222	<code>echo a b c   awk '{print \$1,\$3}'</code>	Вывести первую и третью колонки. Разделение по умолчанию, по пробелу/пробелам или символу/символам табуляции
223	<code>paste file1 file2</code>	Объединить содержимое "file1" и "file2" в виде таблицы: строка 1 из file1 = строка 1 колонка (1 – n), строка 1 из file2 = строка 1 колонка (n + 1 – m)
224	<code>paste -d '+' file1 file2</code>	Объединить содержимое файлов "file1" и "file2" в виде таблицы с разделителем "+"
225	<code>sort file1 file2</code>	Отсортировать содержимое двух файлов
226	<code>sort file1 file2   uniq</code>	Отсортировать содержимое двух файлов, не отображая повторов
227	<code>sort file1 file2   uniq -u</code>	Отсортировать содержимое двух файлов, отображая только уникальные строки (строки, встречающиеся в обоих файлах, не выводятся на стандартное устройство вывода)
228	<code>sort file1 file2   uniq -d</code>	Отсортировать содержимое двух файлов, отображая только повторяющиеся строки
229	<code>comm -1 file1 file2</code>	Сравнить содержимое двух файлов, не отображая строки, принадлежащие файлу "file1"
230	<code>comm -2 file1 file2</code>	Сравнить содержимое двух файлов, не отображая строки, принадлежащие файлу "file2"
231	<code>comm -3 file1 file2</code>	Сравнить содержимое двух файлов, удаляя строки, встречающиеся в обоих файлах

Таблица П5.1 (продолжение)

Преобразование кодировок и форматов файлов		
№	Команда	Описание
232	<code>dos2unix filedos.txt fileunix.txt</code>	Конвертировать файл текстового формата MS-DOS в UNIX (отличие в символах возврата каретки)
233	<code>unix2dos fileunix.txt filedos.txt</code>	Конвертировать файл текстового формата из UNIX в MS-DOS (отличие в символах возврата каретки)
234	<code>recode ..HTML &lt; page.txt &gt; page.html</code>	Конвертировать содержимое тестового файла "page.txt" в HTML-файл "page.html"
235	<code>recode -l   more</code> или <code>iconv -l   more</code>	Вывести список доступных форматов
Сеть (LAN и WiFi)		
№	Команда	Описание
236	<code>ifconfig eth0</code>	Показать конфигурацию сетевого интерфейса "eth0"
237	<code>ifup eth0</code>	Активировать (поднять) интерфейс "eth0"
238	<code>ifdown eth0</code>	Деактивировать (опустить) интерфейс "eth0"
239	<code>ifconfig eth0 192.168.1.1 netmask 255.255.255.0</code>	Выставить интерфейсу "eth0" IP-адрес и маску подсети
240	<code>ifconfig eth0 promisc</code>	Перевести интерфейс "eth0" в promiscuous-режим для "отлова" пакетов (sniffing)
241	<code>ifconfig eth0 -promisc</code>	Отключить promiscuous-режим на интерфейсе "eth0"
242	<code>dhclient eth0</code>	Активировать интерфейс "eth0" в DHCP-режиме
243	<code>route -n</code>	Вывести локальную таблицу маршрутизации
244	<code>netstat -rn</code>	Вывести локальную таблицу маршрутизации
245	<code>route add -net 0/0 gw IP_Gateway</code>	Задать IP-адрес шлюза по умолчанию (default gateway)
246	<code>route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1</code>	Добавить статический маршрут в сеть 192.168.0.0/16 через шлюз с IP-адресом 192.168.1.1
247	<code>route del 0/0 gw IP_gateway</code>	Удалить IP-адрес шлюза по умолчанию (default gateway)
248	<code>echo "1" &gt; /proc/sys/net/ipv4/ip_forward</code>	Разрешить пересылку пакетов (forwarding)
249	<code>hostname</code>	Отобразить имя компьютера
250	<code>host www.example.com</code>	Разрешить имя хоста в IP-адрес и наоборот (1)
251	<code>nslookup www.example.com</code>	Разрешить имя хоста в IP-адрес и наоборот (2)
252	<code>ip link show</code>	Отобразить состояние всех интерфейсов
253	<code>mii-tool eth0</code>	Отобразить статус и тип соединения для интерфейса "eth0"
254	<code>ethtool eth0</code>	Отображает статистику интерфейса eth0 с выводом такой информации, как поддерживаемые и текущие режимы соединения

Таблица П5.1 (продолжение)

Сеть (LAN и WiFi)		
№	Команда	Описание
255	<code>netstat -tup</code>	Отображает все установленные сетевые соединения по протоколам TCP и UDP без разрешения имен в IP-адреса и PID'ы и имена процессов, обеспечивающих эти соединения
256	<code>netstat -tupl</code>	Отображает все сетевые соединения по протоколам TCP и UDP без разрешения имен в IP-адреса и PID'ы и имена процессов, слушающих порты
257	<code>tcpdump tcp port 80</code>	Отобразить весь трафик на TCP-порт 80 (обычно — HTTP)
258	<code>iwlist scan</code>	Просканировать эфир на предмет доступности беспроводных точек доступа
259	<code>iwconfig eth1</code>	Показать конфигурацию беспроводного сетевого интерфейса "eth1"
260	<code>whois www.example.com</code>	Поиск в базе данных системы Whois
Сеть Microsoft (SAMBA)		
№	Команда	Описание
261	<code>nbtscan ip_addr</code>	Разрешить IP-адрес в NETBIOS-имя
262	<code>nmblookup -A ip_addr</code>	Разрешить IP-адрес в NETBIOS-имя
263	<code>smbclient -L ip_addr/hostname</code>	Показать удаленный ресурс Windows-машины
264	<code>smbget -Rr smb://ip_addr/share</code>	Загрузка файлов с удаленной Windows-машины через smb
265	<code>mount -t smbfs (cifs) -o username=user,password=pass //WinClient/share /mnt/share</code>	Монтировать удаленный ресурс сети Windows
IPTABLES (firewall)		
№	Команда	Описание
266	<code>iptables -t filter -L</code>	Отобразить все цепочки правил в filter-таблице
267	<code>iptables -t nat -L</code>	Отобразить все цепочки правил в NAT-таблице
268	<code>iptables -t filter -F</code>	Очистить все цепочки правил в filter-таблице
269	<code>iptables -t nat -F</code>	Очистить все цепочки правил в NAT-таблице
270	<code>iptables -t filter -X</code>	Удалить любые цепочки, созданные пользователем
271	<code>iptables -t filter -A INPUT -p tcp --dport telnet -j ACCEPT</code>	Разрешить входящее подключение Telnet
272	<code>iptables -t filter -A OUTPUT -p tcp --dport http -j DROP</code>	Блокировать исходящие HTTP-соединения
273	<code>iptables -t filter -A FORWARD -p tcp --dport pop3 -j ACCEPT</code>	Позволить "прокидывать" (forward) POP3-соединения
274	<code>iptables -t filter -A INPUT -j LOG --log-prefix "DROP INPUT"</code>	Включить журналирование ядром пакетов, проходящих через цепочку INPUT, и добавлением к сообщению префикса "DROP INPUT"

Таблица П5.1 (продолжение)

<b>IPTABLES (firewall)</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
275	<code>iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE</code>	Включить NAT (Network Address Translate) исходящих пакетов на интерфейс eth0. Допустимо при использовании с динамически выделяемыми IP-адресами
276	<code>iptables -t nat -A PREROUTING -d 192.168.0.1 -p tcp -m tcp --dport 22 -j DNAT --to-destination 10.0.0.2:22</code>	Переадресовать пакеты, адресованные хосту к другому хосту
277	<code># modprobe iptable_nat # iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE # /proc/sys/net/ipv4/ip_forward</code>	Включить NAT (Network Address Translate) исходящих пакетов на интерфейс "eth2" и разрешить пересылку пакетов (CentOS)
<b>Сеть Novell Netware</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
278	<code># ipx_configure --auto_interface=on --auto_primary=on # ipx_interface add -p eth0 802.2I 777</code>	Настройка IPX (можно указать в файле etc/init.d/rc (SUSE11))
<b>Анализ файловых систем</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
279	<code>badblocks -v /dev/hda1</code>	Проверить раздел hda1 на наличие bad-блоков
280	<code>fsck /dev/hda1</code>	Проверить/восстановить целостность Linux-файловой системы раздела hda1
281	<code>fsck.ext2 /dev/hda1</code>	Проверить/восстановить целостность файловой системы ext2 раздела hda1
282	<code>e2fsck /dev/hda1</code>	Проверить/восстановить целостность файловой системы ext3 раздела hda1
283	<code>e2fsck -j /dev/hda1</code>	Проверить/восстановить целостность файловой системы ext3 раздела hda1 с указанием, что журнал расположен там же
284	<code>fsck.ext3 /dev/hda1</code>	Проверить/восстановить целостность файловой системы ext3 раздела hda1
285	<code>fsck.vfat /dev/hda1</code>	Проверить/восстановить целостность файловой системы FAT раздела hda1
286	<code>fsck.msdos /dev/hda1</code>	Проверить/восстановить целостность файловой системы FAT раздела hda1
287	<code>dosfsck /dev/hda1</code>	Проверить/восстановить целостность файловой системы FAT раздела hda1
<b>Форматирование файловых систем</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
288	<code>mkfs /dev/hda1</code>	Создать Linux-файловую систему в разделе hda1
289	<code>mke2fs /dev/hda1</code>	Создать файловую систему ext2 в разделе hda1
290	<code>mke2fs -j /dev/hda1</code>	Создать журналирующую файловую систему ext3 в разделе hda1

Таблица П5.1 (продолжение)

<b>Форматирование файловых систем</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
291	<code>mkfs -t vfat 32 -F /dev/hda1</code>	Создать файловую систему FAT32 в разделе hda1
292	<code>fdformat -n /dev/fd0</code>	Форматирование флоппи-диска без проверки
293	<code>mkswap /dev/hda3</code>	Создание swap-пространства в разделе hda3
294	<code>swapon /dev/hda3</code>	Активировать swap-пространство, расположенное в разделе hda3
295	<code>swapon /dev/hda2 /dev/hdb3</code>	Активировать swap-пространства, расположенные в разделах hda2 и hdb3
<b>Резервное копирование</b>		
<b>№</b>	<b>Команда</b>	<b>Описание</b>
296	<code>dump -0aj -f /tmp/home0.bak /home</code>	Создать полную резервную копию каталога /home в файл /tmp/home0.bak
297	<code>dump -1aj -f /tmp/home0.bak /home</code>	Создать инкрементальную резервную копию каталога /home в файл /tmp/home0.bak
298	<code>restore -if /tmp/home0.bak</code>	Восстановить из резервной копии /tmp/home0.bak в интерактивном режиме
299	<code>rsync -rogpav --delete /home /tmp</code>	Синхронизация между каталогами /home и /tmp
300	<code>rsync -rogpav -e ssh --delete /home ip_address:/tmp</code>	Синхронизировать через SSH-туннель
301	<code>rsync -az -e ssh --delete ip_addr:/home/public /home/local</code>	Синхронизировать локальный каталог с удаленным каталогом через ssh со сжатием
302	<code>rsync -az -e ssh --delete /home/local ip_addr:/home/public</code>	Синхронизировать удаленный каталог с локальным каталогом через ssh со сжатием
303	<code>dd bs=1M if=/dev/hda   gzip   ssh user@ip_addr 'dd of=hda.gz'</code>	Создать резервную копию локального жесткого диска на удаленном компьютере через ssh
304	<code>dd if=/dev/sda of=/tmp/file1</code>	Резервная копия содержания жесткого диска в файл
305	<code>tar -Puf backup.tar /home/user</code>	Создать инкрементальную резервную копию каталога /home/user в файл backup.tar с сохранением полномочий
306	<code>( cd /tmp/local/ &amp;&amp; tar c . )   ssh -C user@ip_addr 'cd /home/share/ &amp;&amp; tar x -p'</code>	Копирование содержимого /tmp/local на удаленный компьютер через ssh-туннель в /home/share/
307	<code>( tar c /home )   ssh -C user@ip_addr 'cd /home/backup-home &amp;&amp; tar x -p'</code>	Копирование содержимого /home на удаленный компьютер через ssh-туннель в /home/backup-home
308	<code>tar cf - .   (cd /tmp/backup ; tar xf - )</code>	Копирование одного каталога в другой с сохранением полномочий и ссылок
309	<code>find /home/user1 -name '*.txt'   xargs cp -av --target-directory=/home/backup/ --parents</code>	Поиск в /home/user1 всех файлов с расширением txt и копирование их в другой каталог
310	<code>find /var/log -name '*.log'   tar cv --files-from= -   bzip2 &gt; log.tar.bz2</code>	Поиск в /var/log всех файлов с расширением log и создание bzip-архива из них

Таблица П5.1 (продолжение)

Резервное копирование		
№	Команда	Описание
311	<code>dd if=/dev/hda of=/dev/fd0 bs=512 count=1</code>	Создать копию главной загрузочной записи MBR (Master Boot Record) с /dev/hda на дискету
312	<code>dd if=/dev/fd0 of=/dev/hda bs=512 count=1</code>	Восстановить главную загрузочную запись MBR из резервной копии, сохраненной на дискету
CD-ROM, DVD-ROM		
№	Команда	Описание
313	<code>cdrecord -v gracetime=2 dev=/dev/cdrom -eject blank=fast -force</code>	Очистить перезаписываемый CD-ROM
314	<code>mkisofs /dev/cdrom &gt; cd.iso</code>	Создать ISO-образ диска в файле "cd.iso"
315	<code>mkisofs /dev/cdrom   gzip &gt; cd_iso.gz</code>	Создать сжатый ISO-образ диска в файле "cd_iso.gz"
316	<code>mkisofs -J -allow-leading-dots -R -V "Label CD" -iso-level 4 -o ./cd.iso data_cd</code>	Создать ISO-образ каталога
317	<code>cdrecord -v dev=/dev/cdrom cd.iso</code>	Записать ISO-образ на диск
318	<code>gzip -dc cd_iso.gz   cdrecord dev=/dev/cdrom -</code>	Записать сжатый ISO-образ на диск
319	<code>mount -o loop cd.iso /mnt/iso</code>	Монтировать ISO-образ
320	<code>cd-paranoia -B</code>	Записать треки аудиодиска в WAV-файлы
321	<code>cd-paranoia -- "-3"</code>	Записать первые три трека аудиодиска в WAV-файлы
322	<code>cdrecord --scanbus</code>	Просканировать CD-рекордер на наличие канала SCSI
323	<code>dd if=/dev/hdc   md5sum</code>	Выполнить md5sum для диска
Мониторинг и отладка		
№	Команда	Описание
324	<code>top</code>	Отобразить запущенные процессы, используемые ими ресурсы и другую полезную информацию (с автоматическим обновлением данных)
325	<code>ps -eafw</code>	Отобразить запущенные процессы, используемые ими ресурсы и другую полезную информацию (единожды)
326	<code>ps -e -o pid,args --forest</code>	Вывести PID'ы и процессы в виде дерева
327	<code>Pstree</code>	Отобразить дерево процессов
328	<code>kill -9 98989</code>	Остановить процесс с PID 98989 без соблюдения целостности данных
329	<code>kill -KILL 98989</code>	Остановить процесс с PID 98989 без соблюдения целостности данных
330	<code>kill -TERM 98989</code>	Корректно завершить процесс с PID 98989
331	<code>kill -1 98989</code>	Заставить процесс с PID 98989 и перечитать файл конфигурации



Таблица П5.1 (продолжение)

Мониторинг и отладка		
№	Команда	Описание
332	<code>kill -HUP 98989</code>	Заставить процесс с PID 98989 и перечитать файл конфигурации
333	<code>pstree</code>	Отобразить дерево процессов
334	<code>lsof -p \$\$</code>	Отобразить список файлов, открытых процессами
335	<code>lsof /home/user1</code>	Отобразить список открытых файлов из каталога /home/user1
336	<code>strace -c ls &gt;/dev/null</code>	Вывести список системных вызовов, созданных и полученных процессом ls
337	<code>strace -f -e open ls &gt;/dev/null</code>	Вывести вызовы библиотек
338	<code>watch -n1 'cat /proc/interrupts'</code>	Отобразить прерывания в режиме реального времени
339	<code>last reboot</code>	Отобразить историю перезагрузок системы
340	<code>last user1</code>	Отобразить историю регистрации пользователя "user1" в системе и время его нахождения в ней
341	<code>lsmod</code>	Вывести загруженные модули ядра
342	<code>free -m</code>	Показать состояние оперативной памяти в мегабайтах
343	<code>smartctl -A /dev/hda</code>	Контроль состояния жесткого диска /dev/hda через SMART
344	<code>smartctl -i /dev/hda</code>	Проверить доступность SMART на жестком диске /dev/hda
345	<code>tail /var/log/dmesg</code>	Вывести десять последних записей из журнала загрузки ядра
346	<code>tail /var/log/messages</code>	Вывести десять последних записей из системного журнала
347	<code>apropos ...keyword</code>	Выводит список команд, которые так или иначе относятся к ключевым словам. Полезно, когда вы знаете, что делает программа, но не помните команду
348	<code>man ping</code>	Вызов руководства по работе с программой, в данном случае — <code>ping</code>
349	<code>whatis ...keyword</code>	Отображает описание действий указанной программы
350	<code>mkbootdisk --device /dev/fd0 'uname -r'</code>	Создает загрузочный флоппи-диск
351	<code>gpg -c file1</code>	Шифрует файл "file1" с помощью GNU Privacy Guard
352	<code>gpg file1.gpg</code>	Дешифрует файл "file1" с помощью GNU Privacy Guard
353	<code>wget -r www.example.com</code>	Загружает рекурсивно содержимое сайта <b>www.example.com</b>

Таблица П5.1 (окончание)

Мониторинг и отладка		
№	Команда	Описание
354	wget -c www.example.com/file.iso	Загрузите файл с возможностью остановить загрузку и возобновить позже
355	echo 'wget -c www.example.com/files.iso'   at 09:00	Начать загрузку в указанное данное время
356	ldd /usr/bin/ssh	Вывести список библиотек, необходимых для работы ssh
357	alias hh='history'	Назначить алиас (псевдоним) hh-команде history
358	chsh	Изменить командную оболочку (сменить shell)
359	chsh --list-shells	Показать удаленные подключения
360	who -a	Просмотр информации о текущем пользователе, времени последней загрузки системы и др.
361	startx	Запуск видеосистемы (xserver)
362	Pidof <имя_программы>	Определить идентификатор (PID) по имени программы

# Предметный указатель

## #

100BASE TX 552  
100BASE-FX 532, 552  
100BASE-T 532  
10BASE2 532  
10BASE-2 552  
10BASE5 532  
10BASE-5 552  
10BASE-FL 532, 552  
10BASE-T 532, 552  
802.11b 59, 60  
802.11g 59, 60, 63

## A

Acronis True Image 220  
Active Directory 211, 428—434, 438, 441,  
443—446, 448, 532  
Active Directory (AD) 212, 336, 376, 427, 547  
◇ опубликование принтера 444  
◇ установка 428  
ADSL 41, 397  
ADSL-модем 41, 62, 98, 104, 360  
AES 60  
Analogx Simple Server 357  
AUI 533  
Auto-sensing 10/100 Mbps 533

## B

Backup 225  
Bluetooth 70  
BNS 533  
Bridge 533  
Bridge/Router 533  
Broadcast 533  
Broadcast Domain 533

Broadcast Storm 534  
Browser Appliance 308, 310, 311  
BWMeter 491

## C

Comilfon 513  
ConquerCam 518, 520  
Courier Mail Server 402, 404  
CourierMS 469  
CSMA/CD 19

## D

DES 60  
DHCP (Dynamic Host Configuration Protocol)  
96, 359, 534  
DHCP-сервер 359, 360, 362, 364—367, 370,  
376, 380, 381  
Directory 546  
Directory service 547  
DMZ 110  
DNS 41, 47, 93, 534  
dnsmgmt 378, 379  
DNS-сервер 102, 105, 106, 118, 360, 361, 363,  
375—377, 379—381, 431  
DOS 16, 18  
DOS NDIS 534  
DOS ODI 534  
Driver 538  
DynDNS Apdater 482

## E

Ekiga 515  
Ethernet 18, 19, 42, 44, 47, 534  
Ethernet-адрес 541

Evolution 508—510  
ext3 210

## F

Fast Ethernet 534  
FAT12 288  
FAT16 288  
FAT32 210, 288, 429  
File Transfer Protocol (FTP) Service 346, 534  
Firestarter 128, 140  
Firewall 130  
FOIRL 532

## G

Gaim 516

## H

Hamachi 167  
HTA 456  
HTML 535  
HTML-страница 542  
Hub 535, 539

## I

ICMP 166  
ICQ 512, 513, 516  
IDS 61  
IKE 61  
Interface 535  
Internet Information Services (IIS) 346, 353  
IPv4 19  
IPv6 19  
IPX/SPX 540  
IP-адрес 19, 30—33, 47, 77, 99, 101, 102, 104—  
106, 117  
◇ выделенный 477  
◇ динамический 482  
IP-фильтр 402, 408, 409, 421  
ISDN 535

## L

LAN 535  
LINKLOCAL 95, 96, 535  
Linux 42—44, 49, 51, 53—57, 89—92,  
210—214, 487—490  
◇ файловая система 289

Linux Mint 70  
LMHOSTS 373, 375  
LogMeIn 486, 487  
LogMeIn Hamachi 167  
LPT-порт 16

## M

MAC 535  
MAC-адрес 535, 541  
Media-сервер 382  
Mirrored Arrays 336

## N

NAT 170  
NDIS 535  
NeoRouter 169  
NeoRouter Configuration Explorer 170  
NetBEUI 535, 540  
NetBIOS 375, 535  
NetBIOS-имя 370, 375  
NetBIOS-имя домена 429  
NTFS 210, 287—290  
◇ том 429  
NTFS5 252, 287

## O

OpenVPN 164—166  
◇ клиент 165  
◇ сервер 165  
Oracle VirtualBox 325  
Organizational Unit (OU) 438

## P

Partition Magic 253  
PCMCIA-порт 15  
Pidgin 516  
POP3 402, 403  
POP3-клиент 402, 403, 412  
POP3-сервер 397, 402, 404, 409, 412, 419, 421  
PowerChute Pluss 237  
PrimalScript 453  
Proxy Server 535

## Q

Q\_Chat 517  
QIP Infium 513

**R**

RAID 336  
Rambler-ICQ 512  
Rasdial 119, 120  
RDN 549  
Remote Storage 225  
Rootkit 139

**S**

SIP 515  
SIPNET 513, 514  
Skype 512  
◇ для Linux 515  
◇ для Windows 512  
SMS 512  
SMTP 402, 403, 409, 410, 421, 422  
SMTP-клиент 402, 411  
SMTP-подключение 420  
SMTP-сервер 397, 402, 404, 405, 407, 409, 411,  
412, 418—422  
SPI 61  
Splitter 161  
StarGazer 496  
SUN VirtualBox 325  
Switch 27, 538  
System Restore 225

**T**

TCP/IP 19, 95, 96, 532, 536, 540  
◇ привязка 79  
Teamviewer 490  
Telnet 188, 536  
Telphin 514  
Throughput 536  
TKIP 60

**U**

URL 61  
USB 59, 61, 63, 66, 67  
UTP 536

**V**

VideoLAN 524  
Virtual Appliances 308  
Virtual Server Migration Toolkit (VSMT) 295  
VLC Media Player 386, 524  
VMware Player 294, 302, 303, 306, 307, 309, 310  
VMware Server 302, 307, 309—311, 313  
VMware Server Console 316, 319—323  
VMware Workstation 29  
VPN 60, 164—166  
VRDP 327

**W**

WAN 536  
WebHop 482  
Web-интерфейс 398  
Web-камера 384, 518, 521  
Web-сервер 353, 376, 377  
◇ настройка 353  
Web-страница 358, 542  
◇ создание 383  
WEP (Wireless Encryption Protocol) 60  
Wi-Fi 58, 59, 537  
Windows 27  
Windows 2000 Server 353  
Windows 7 27  
Windows Live Mail 506  
Windows Live Messenger 511, 512  
Windows Media 9 Series 382, 383, 518  
Windows Vista 27, 36, 37, 48, 49, 51, 55, 57  
Windows XP 27, 29, 30, 33, 35, 210  
WINIPCFG 96  
WINS 537  
WINS-сервер 370  
Wireless 67—69

**X**

XML 211

**Z**

ZeRAT 469, 470

**А**

- Автоматическое назначение личных IP-адресов 96
- Адаптер 541
  - ◇ сетевой 541
  - ◇ беспроводный 59
- Архивирование 220

**Б**

- Бесперебойное питание 236
- Беспроводная сеть 537
- Беспроводный адаптер 59
  - ◇ D-Link DWL-G122 USB 59, 63
- Брандмауэр 35, 130
  - ◇ настройка в Windows 131
  - ◇ настройка для Windows Comodo 137

**В**

- Виртуальная локальная сеть 536
- Виртуальная машина:
  - ◇ Oracle VirtualBox 325
  - ◇ SUN VirtualBox 325
- Виртуальный компьютер 29, 309, 310, 312, 316, 323, 324, 333
- Витая пара 149, 537
- Время входа в сеть 446, 447
- Выделенная линия 187
  - ◇ настройка связи 187

**Д**

- Демилитаризованная зона 110
- Дерево 549
  - ◇ доменов 550
- Домен 80, 550
  - ◇ верхнего уровня 376
  - ◇ широковещательной рассылки 533
- Доступность принтера 89
- Драйвер 86, 538

**Ж**

- Журнальный файл 211

**З**

- Зеркалирование 336

**И**

- Идентификация компьютера в сети 81
- Имя компьютера в Linux 81
- Интернет 21
- Интерфейс 538
- Источник бесперебойного питания (ИБП) 236, 239—241, 260

**К**

- Кадр информации 19
- Картридер 15
- Каталог 546
- Клиент для сетей Microsoft 38, 40
- Коаксиальный кабель 538
- Кодировщик Windows Media 9 Series 520
- Команда:
  - ◇ hostname 184
  - ◇ ipconfig 184
  - ◇ nbtstat 184
  - ◇ netstat 183, 184
  - ◇ netsh diag connect iphost 473
  - ◇ pathping 185
  - ◇ ping 35, 36, 184
  - ◇ put 352
  - ◇ Rasdial 119
  - ◇ route 180, 184
  - ◇ runas 447
  - ◇ shutdown 476
  - ◇ tracert 183, 185
  - ◇ xcopy 452
- Коммутатор 27, 36, 538
- Коммутируемое соединение 110
- Компьютеры одноранговой сети 78
- Коннектор 539
- Коннектор RJ-45 26
- Консоль 263
- Контейнер 548
- Контроллер:
  - ◇ домена 82, 427, 428
  - ◇ удаленного доступа 79
- Концентратор 538, 539

**Л**

- Лес 550
- Локальная вычислительная сеть (ЛВС) 18
- Локальные политики домена 435
- Локатор Windows 38

**М**

- Маршрутизатор 60, 63, 64, 66, 99, 104, 106, 110, 539
  - ◇ DI-824VUP+ 60, 61
- Маршрутизация 175
  - ◇ настройка 180
- Маска 20, 21
  - ◇ подсети 21
- Мастер:
  - ◇ настройки сервера 377
  - ◇ настройки сети 77
  - ◇ создания области 361—363
- Модем 58, 98, 104, 106, 110—114, 120, 126, 128, 539
  - ◇ D-Link DFM-562E 58, 59
  - ◇ аналоговый 58
- Модемное соединение 125
- Монтирование разделов 211
- Мост 533
- Мост/маршрутизатор 533

**Н**

- Непрерывное поддерево 549
- Неэкранированная витая пара 536
- Нуль-модемный кабель 16

**О**

- Общий:
  - ◇ доступ 48, 49, 51, 52, 91, 92
  - ◇ принтер 86
- Объект 548
- Одноранговая сеть 539
  - ◇ компьютеры 78
- Операционная система (ОС):
  - ◇ Windows 98 17
  - ◇ для рабочей станции 284
  - ◇ для сервера 247
  - ◇ сетевая 541
  - ◇ установка на сервер 250
- Организационные единицы 438
- Относительное уникальное имя объекта 549

**П**

- Пакет 540
  - ◇ данных 19
- Параметры безопасности 435
  - ◇ домена 435, 436

- Патчкорд 36
- Перекрестный кабель 27
- Планировщик задач 119
- Подключение к рабочему столу 479
- Подразделение 263
- Политика паролей 435
- Политики учетных записей 435
- Порт 540
  - ◇ программный 540
  - ◇ физический 540
- Почтовый:
  - ◇ клиент ZeRAT 469, 470
  - ◇ протокол 402
  - ◇ сервер 394, 402
    - CourierMS 469, 470
    - встроенный в Windows Server 2003 469
- Принтер 86
- Принт-сервер 66
- Программа:
  - ◇ Acronis True Image 220
  - ◇ AnVir Task Manager 145
  - ◇ Avast! 143
  - ◇ Backup 225
  - ◇ Clam AntiVirus 143
  - ◇ Comodo Firewall Pro 137
  - ◇ Firestarter 128
  - ◇ Hamachi 167
  - ◇ HiperTerminal 159
  - ◇ Lap2Desk 16, 17
  - ◇ NeoRouter 169
  - ◇ NeoRouter Configuration Explorer 170
  - ◇ OpenVPN 163, 164
  - ◇ Remote Storage 225
  - ◇ ServerOK 160
  - ◇ System Restore 225
  - ◇ VMware Workstation 29
- Производительность 536
- Пропускная способность 536
- Пространство имен 548
- Протокол 540
  - ◇ NetBEUI 79
  - ◇ Интернета 39
  - ◇ Интернета версии 4 40
- Профиль служб терминалов 441, 443

**Р**

- Рабочая группа 80, 82
  - ◇ имя 80
- Рабочая станция 284
- Разводка кабеля 26

Расширения масок подсети 21  
Резервирование 364, 365  
Резервное копирование 220  
Роль сервера 429  
Руткит 139

## С

Сегмент сети 540  
Сервер 96, 247, 539, 540  
◇ DHCP 359  
◇ DNS 375  
◇ media 382  
◇ Web 353  
◇ WINS 370  
◇ локальное управление 465  
◇ настройка 337  
◇ почтовый 394  
◇ удаленного доступа 541  
◇ файловый 335  
◇ электронной почты 402  
Сетевая операционная система 541  
Сетевая плата 541  
Сетевое подключение 30, 38  
Сетевой:  
◇ адаптер 541  
◇ кабель 541  
◇ мост 175  
◇ принтер 89  
◇ профиль 443  
Сеть:  
◇ беспроводная 537  
◇ виртуальная 536  
◇ компьютерная 538  
◇ одноранговая 539  
Скрипты 451  
Служба каталогов 547  
Соединение компьютеров:  
◇ в Linux 210  
◇ в MS-DOS 198  
Сохраненные запросы 437  
Сплиттер 161  
Средства связи 499

Статическое:  
◇ отображение 374  
◇ сопоставление 373  
Сценарии 451, 453, 456, 460

## Т

Точка доступа к радиосети 58  
Трафик 491

## У

Узел 149, 551  
Уникальное имя 549  
Утилита Firestarter 140  
Учетные записи 433, 437, 440, 443  
◇ задание времени входа в сеть 446  
◇ локальные 443  
◇ поиск в AD 437

## Ф

Файервол 130  
◇ настройка в Mandriva Linux 135  
Файловая система 287  
◇ NTFS5 252  
Факсимильные сообщения 500  
Флэш-накопители 15  
Формат HTA 456

## Х

Хаб 539

## Ш

Широковещательная рассылка 533  
Шлюз 98, 99, 106, 107, 118  
◇ в Интернет 98

## Э

Электронная подпись 500  
Электронная почта 505