Самоучитель

Александр Поляк-Брагинский

Linux и Windows в домашней сети

Малая домашняя сеть с Windows и Linux

Удаленная работа на компьютере

Подключение сети к Интернету

Виртуальные компьютеры в малой сети

Средства для общения в сети

Безопасность

bhv

Александр Поляк-Брагинский

Linux и Windows
в домашней сети

Санкт-Петербург
«БХВ-Петербург»
2008

УДК 681.3.06
ББК 32.973.26-018.2
П54

Поляк-Брагинский А. В.

П54 Linux и Windows в домашней сети. — СПб.: БХВ-Петербург, 2008. — 336 с.: ил. — (Самоучитель)

ISBN 978-5-9775-0257-3

Книга представляет собой практическое руководство по созданию простой локальной вычислительной сети для дома или небольшого офиса на основе компьютеров под управлением Windows и Linux. Обсуждаются вопросы маршрутизации, удаленной работы на компьютерах, совместного использования ресурсов, создания смешанной сети. Представлено описание программ для организации общения в сети. Рассмотрено применение виртуальных компьютеров в сети.

Для опытных пользователей

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Натальи Смирновой*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 27.06.08.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 27,09.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

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

ISBN 978-5-9775-0257-3

Оглавление

Предисловие

Вы держите в руках книгу о создании маленькой компьютерной сети на основе Windows и Linux. Это не научный труд, а описание возможностей эффективного использования своих компьютеров в домашней сети. Не секрет, что теперь во многих семьях не один компьютер. Техника и программное обеспечение развиваются, и не всегда удается модернизировать старый компьютер для работы с новыми операционными системами. Но старый компьютер еще исправно работает. Так зачем же избавляться от него, когда можно применить с пользой, организовав небольшую сеть? Компьютер, не дотягивающий по своим параметрам до требований Windows Vista, вполне может работать под управлением Linux одной из последних версий. Иногда и новые компьютеры приобретаются для каждого ребенка в семье, есть уже компьютеры у родителей. Так почему бы не заставить эти машины работать совместно?

Для кого эта книга

Конечно, для вас! Для тех, кто хотел бы настроить маленькую домашнюю сеть с выходом в Интернет, используя имеющиеся компьютеры под управлением Windows и Linux, для тех, кто ценит возможности коллективной работы на компьютере. Для тех, кто хочет получить доступ к своим компьютерам из Интернета с компьютера друга или со своего рабочего компьютера, иметь доступ к своему компьютеру на работе, или к компьютеру друга. А может быть вы и ваши родственники живете далеко друг от друга. Разве вас не интересует возможность совместной работы, помощи друг другу? А может быть, у вас есть ноутбук, с которым вы путешествуете далеко от дома, а на домашнем компьютере установлены именно те программы, которые потребовались именно сейчас, когда до дома сотни или тысячи километров. Возможно, вы дома, а на рабочем компьютере хранится крайне необходимый документ...

Новые компьютеры все чаще продаются с предустановленной ОС Windows Vista, но развивается, становится все более популярной операционная система с открытым кодом — Linux. Наверняка, вы уже работали в среде Windows XP. Эта ОС есть практически в каждом доме и на каждом предприятии, где есть компьютеры, и в настоящее время наиболее приспособлена для организации сети. Но время идет... Обостряется конкуренция среди разработчиков ОС, появляются новые версии Linux, работа в которых стала не сложнее, чем в привычных Windows. Вы можете освоить незнакомые ранее системы, использовать их преимущества перед предшественницами, использовать эти системы на своем компьютере и в своей сети, сделать работу на компьютере более интересной, воспользоваться простыми технологиями, которые вы раньше считали слишком сложными.

Ну, вот уже слышу голос скептика: "Жил без сети и не тужил. Зачем она мне?" Тогда и вы, уважаемый скептик, прочтите несколько страниц этой книги. Она вас заинтересует. Вы увидите перспективы, ранее не замеченные вами. Новые знания позволят подняться на новую высоту, увидеть горизонты, к которым будет стремиться ваша маленькая сеть из двух или более компьютеров. Ощутите свободу в своей сети, свободу работы на своем компьютере, свободу обмена информацией с другими компьютерами, с вашими друзьями и родственниками.

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.

Приступая к новой книге, необходимо быть уверенным в своих силах. В этом мне помогли медики. Всем медработникам, которые помогли мне сохранить и приумножить силы и работоспособность, моя благодарность.

Друзья и семья, которые поддерживали в трудные минуты, тоже содействовали появлению этой книги. Если бы не эта поддержка, книга могла не появиться.

Редакторы стоят на рубеже подготовки книги к печати. Им приходится "причесывать" текст, находить не совсем логичные с точки зрения читателя фразы, обнаруживать 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.

Введение

Зачем нам малая домашняя сеть?

Кое-что об этом сказано уже в предисловии. Если вы еще не увидели повода для организации малой сети у себя дома, прочтите следующие строки. Попробуем более подробно оценить преимущества сетевой работы по сравнению с работой на отдельно стоящем компьютере, не имеющем возможности использовать ресурсы сети.

Повышение эффективности работы на компьютере

Доступ к Интернету теперь есть у многих. Гигабайты информации скачиваются из этой глобальной сети и оседают в локальных хранилищах, занимая место на жестких дисках. Если вы все же решили экономить дисковое пространство, то вам приходится переносить с компьютера на компьютер необходимые файлы с помощью дискет, флэш-дисков, USB-винчестеров, CD-R- или DVD-R-дисков. То и дело не читается диск на компьютере — получателе информации. Тратится время и расшатываются нервы. Возникает необходимость приобретения новых носителей информации только для переноса данных с компьютера на компьютер. Но есть более удобный вариант. Если один из компьютеров снабдить достаточно емким винчестером, то на нем можно хранить все необходимые файлы. Другие могут получить доступ к ним через сеть, в которую объединены компьютеры. В любой момент можно скопировать файл или запустить его прямо из сетевого каталога. Файлы занимают место в специально выделенном хранилище и используются по мере необходимости всеми пользователями сети. Новые файлы так же помещаются в это хранилище. Вы не хотите, чтобы к некоторым файлам имели доступ отдельные пользователи сети? Нет ничего проще. Ограничьте права доступа к файлам или отдельным каталогам.

Программное обеспечение, которое вам необходимо, зачастую не бесплатно. Нередко лицензионное соглашение ограничивает число инсталляций программы. Если вы хотите использовать такую программу на втором или треть-

ем компьютере, придется покупать дополнительную лицензию. В сети возможен другой путь для использования программы. Получите доступ к рабочему столу компьютера с установленной программой с другой машины. При этом возможно получение доступа к компьютеру с Windows с компьютера с установленной ОС Linux. Вы можете, используя бесплатную операционную систему, подключаться к компьютеру с установленными коммерческими программами и работать с ними.

Не секрет, что скачивание из Интернета больших файлов занимает некоторое время и ресурсы компьютера. Поручите эту работу удаленному компьютеру, продолжая без помех работать на своей рабочей машине.

Коллективная работа и развлечения

Иногда работа в какой-либо программе требует участия второго человека. Возможно, что это создание текста, компьютерной программы или графического произведения, и совет товарища или его помощь были бы более чем желательны. Но работать на одном компьютере в таких случаях может быть неудобно. Работая с одним документом на разных компьютерах, можно избежать необходимости присутствия товарища не только около вашего компьютера, но даже в вашей квартире. Вы можете находиться далеко друг от друга, но выполнять совместную работу. То же самое можно сказать и об играх по сети. Чтобы играть в одну и ту же игру, не обязательно быть рядом. Сеть объединит вас, когда вы находитесь на значительном расстоянии друг от друга.

Возможность удаленной работы

Эту возможность я использую очень часто. Зачем носить с собой или даже копировать через сеть файлы, если всегда есть доступ к компьютеру, на котором они находятся? Файл, содержащий информацию этого введения, находится за сорок километров от меня. Я с помощью не самого современного ноутбука подключен к рабочему компьютеру и пишу эти строки... Завершенную работу я отправлю по электронной почте, которая тоже настроена на рабочем компьютере. То есть мне не нужно настраивать для текущей работы компьютеры, около которых я нахожусь в данный момент. Важно лишь получить дистанционный доступ к рабочему компьютеру. Вариантов организа-

ции такого доступа множество, но самое важное звено — наличие сети, которая связывает два компьютера. Это может быть и локальная сеть, и Интернет, как в моем случае.

Общее подключение к Интернету

Подключить один компьютер к Интернету не сложно. Если же у вас не один компьютер, то, предоставив возможность выхода в Интернет с каждого из них, вы сможете избежать семейных споров за место у компьютера. Каждый сможет путешествовать в Интернете совершенно независимо, даже если подключение только одно. Не имея хотя бы самой простой сети, решить эту задачу невозможно. Практически не имеет значения, какой вариант подключения к Интернету вы используете. Обычный модем или ADSL-модем, или подключение через районную (городскую, домовую) сеть. В каждом случае потребуется учесть особенности подключения, но сделать его общим всегда возможно.

Безопасная работа в Интернете

Эта возможность в наше время может быть особенно полезной. Трояны, черви и прочие компьютерные вирусы распространены настолько, что беззащитный компьютер под управлением Windows не проработает и дня, если он активно используется для прогулок в Интернете. Антивирусные программы, конечно, помогают защититься от этой нечисти. Но нет идеальной антивирусной программы. Кроме того, эти программы нередко мешают работать с совершенно безобидными файлами. При этом пользователи отключают антивирусы на время, а потом забывают вовремя включить. Источников заражения множество: это и электронная почта, и вредоносные сайты, и принесенные кем-то непроверенные файлы, — всего не перечислишь. Серьезная защита каждого компьютера — дело совсем непростое. Тем не менее, во многих случаях может помочь сеть. Достаточно иметь один хорошо защищенный компьютер, а еще лучше, если это компьютер под управлением Linux с общим доступом к рабочим столам (в Linux их может быть несколько), и значительная часть путей заражения вирусами будет перекрыта. ОС Linux практически не подвержена заражению большинством современных вирусов.

Представляет интерес тот факт, что на современных компьютерах можно запускать виртуальные машины с виртуальными компьютерами. Находясь на одной физической машине, можно создать сеть, в которой будет работать защищенный виртуальный компьютер.

Надежность хранения важной информации

Сколько раз я слышал жалобы на то, что кто-то удалил важные файлы с компьютера, к которому имеют доступ несколько человек. Даже если вы сможете определить виновника пропажи, восстановить файлы часто бывает невозможно. При этом файлы могут быть удалены из лучших побуждений. В них был обнаружен вирус, который не поддавался лечению, и антивирусная программа предложила их удалить. Но у меня хранится несколько файлов, которые мне крайне необходимы. Они практически всеми антивирусными программами определяются как зараженные. Конечно, работа с такими файлами требует осмотрительности, но потеря их для меня крайне нежелательна. Где выход? Снова положение спасает сеть. В сетевом хранилище, где распределены права на каталоги, к моим файлам имею доступ только я. Другие пользователи имеют свои личные каталоги, к которым, возможно, нет доступа у меня. Все персональные файлы надежно хранятся, а их случайная утрата практически исключена.

Возможность оказания и получения помощи через сеть

Эта возможность может быть использована как специалистами, так и родителями или друзьями. Находясь в сети, всегда можно обратиться к другому ее пользователю за помощью. Достаточно получить доступ к вашему рабочему столу, чтобы иметь возможность не просто словами, а на реальном примере показать, как правильно выполнить то или иное действие в какой-либо программе, где найти нужные настройки в вашей системе, просто научить пользоваться тем или иным программным инструментом. Имея дополнительно возможность текстового или голосового общения, можно провести полноценный урок работы на компьютере.

Другие возможности

Уже перечисленного выше, надеюсь, достаточно, чтобы заинтересовать вас и побудить к организации домашней сети. Но есть еще некоторые возможности, которые могут стать дополнительным стимулом в освоении прогрессивных технологий. Компьютерная сеть — это дополнительные каналы общения. Вы можете организовать каналы голосовой связи в дополнение к телефонной или при отсутствии таковой. Можно передавать и видеоинформацию, транслировать фильмы и радиопередачи (в Интернете много теле- и радиостанций!). Вы можете создать свою радио- или телевизионную студию, организовать вещание в вашу сеть и даже в Интернет. Создав локальный Web-сайт, вы можете выставлять свои фото- и видеоработы... Думаю, что нет смысла продолжать перечислять преимущества, которые даст вам ваша маленькая сеть. Следует, видимо, только добавить что сеть, о которой мы говорим, скорее, не совсем локальная. Это смешанная сеть. Как внутри локальной сети, так и для связи с ее компьютерами извне предполагается наличие разнородных операционных систем. Для организаций и предприятий такая сеть чаще всего неприемлема ввиду сложности ее обслуживания. Но в нашем случае нет никакого регламента для использования той или иной операционной системы или оборудования. Мы ориентируемся на то, что каждый волен выбирать то, что ему больше по душе, значит, и сеть наша весьма демократична. Ее пользователями могут быть владельцы любых распространенных компьютеров и операционных систем.

Как читать эту книгу

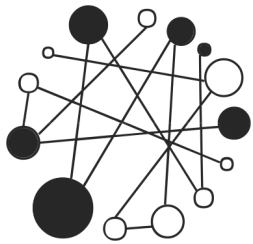
Книга почти не содержит теоретического материала. Все, что в ней описано, действительно работает, опробовано или применяется в настоящее время автором. Поэтому лучше прочитать книгу от начала до конца последовательно. Изложение построено от простого к сложному. Каждый следующий этап создания сети, реализация новой функциональности основаны на предыдущем опыте. Теоретические сведения, имеющиеся в книге, напрямую связаны с практикой создания сети, по возможности постарайтесь вникнуть в них. Теории совсем не много, но она поможет в дальнейшем освоении практического материала.

Предварительные замечания

Для того чтобы изложение было по возможности лаконичным, автор упускает отдельные замечания, связанные с повторением одних и тех же действий или выполнением определенных условий. Возможно, что при повторении примеров вы обнаружите какие-либо сообщения системы, которые не упомянуты. Но вы не окажетесь в затруднительном положении. Так, например, производя установку и настройку программ в Linux, вы неоднократно увидите требование системы ввести пароль администратора. Это совсем не трудно, а включение этого действия в описание только удлинит его, будет отвлекать от основной идеи. В Windows Vista ситуация аналогичная. Но автор рекомендует на время проведения сложных настроек отключить контроль учетных записей пользователей. Есть ситуации, когда Windows Vista не требует ввести пароль администратора и не подчиняется вашим действиям, если контроль учетных записей включен. Отключить контроль учетных записей не сложно. В Панели управления найдите апплет Учетные записи пользователей и откройте его. В открывшемся окне есть пункт меню **Включение и отключение контроля учетных записей** (UAC). После завершения настроек можно опять включить контроль учетных записей. Совсем отключать эту функцию не стоит — дополнительное средство обеспечения безопасности компьютера при работе в Интернете, с файлами сомнительного происхождения и при доступе к компьютеру неопытных пользователей не повредит.

Не старайтесь искать в инструкциях, приведенных в книге, строгих рецептов выполнения поставленных задач. Примеры в книге рассчитаны на творческое применение. Нет двух одинаковых людей, нет двух одинаковых сетей. В каждом конкретном случае возможны свои решения. Для того чтобы решить конкретную задачу, и приведены примеры, которые можно модифицировать и комбинировать.

Глава 1



Создаем сеть

Создание большой сети под силу лишь группе опытных специалистов, а в одиночку большую сеть не создать, каким бы опытом и знаниями мы не обладали. Но сеть в вашей квартире не настолько велика, чтобы приглашать специалистов для ее создания. Не боги горшки обжигают... Все начинается с малого: два компьютера, соединенные между собой кабелем, — это уже сеть. С этого мы и начнем. Вы все-таки не знаете с чего начать? Тогда для тех, кто совершенно не знаком с основами сетестроения, небольшой ликбез.

Все гениальное просто! Сеть — одно из гениальных изобретений прошлого века. Множество талантливых инженеров работали над созданием и совершенствованием локальных вычислительных сетей. Работы начались еще в 1961 г., но сеть, которая интересует нас, появилась лишь в 1973 г. Боб Меткалф предложил фирме Xerox создать Ehternet. Первая Ethernet-сеть, созданная Бобом Меткалфом и Дэвидом Боггсом в исследовательском центре PARC (Palo Alto Research Centre) фирмы Xerox, работала со скоростью 2,944 Мбит/с и соединяла друг с другом два компьютера.

> ***Примечание***
>
> Если вы хотите подробнее узнать об истории создания локальных сетей, зайдите в виртуальный компьютерный музей по адресу в Интернете: **http://www.computer-museum.ru/frgnhist/lan.htm**.

Это именно то, что нам нужно! Наша маленькая ЛВС (локальная вычислительная сеть) тоже для начала объединит всего два компьютера, и работать она будет по правилам сетей Ethernet. В 1980 г. был опубликован первый стандарт для таких сетей. Постепенно стандарты и сетевое оборудование совершенствовались, обслуживание сетей упрощалось. Теперь рядовому пользователю маленькой ЛВС нет необходимости знать все существующие стандарты, описывающие множество параметров сети, правил их построения,

принципов работы. Сеть стала обычным явлением в нашей жизни, как и радио, телевидение, телефонная связь... Для того чтобы снять любительский фильм, не требуется знание стандартов из области цифровой записи информации или физических основ магнитной записи. Вот и мы, если и будем упоминать специальные термины, то только потому, что без них не обойтись. В каждой области человеческой деятельности существует свой профессиональный язык. Нередко не обходится без жаргонных выражений. Такой язык упрощает общение профессионалов. Мы не профессионалы в области создания и эксплуатации вычислительных сетей, но нам придется иногда обращаться к специальной литературе, где эти термины применяются. Придется иногда консультироваться у специалистов, язык которых должен быть нам понятен, как и наш язык им.

Итак, для начала немного теории.

Как работает сеть?

У вас, скорее всего, есть телефон... Компьютер имеет многократно более сложное устройство, чем телефон, но для первого знакомства с сетью вполне подойдет упрощенное описание работы телефонов в телефонной сети. Эти привычные всем устройства могут иметь различную функциональность. Иногда в них встраивают диктофон для записи разговоров, записную книжку для записи телефонных номеров, часы... Некоторые возможности этих устройств могут быть использованы без подключения к телефонной сети. Но основное назначение телефона — работа в телефонной сети, соединение удаленных друг от друга абонентов этой сети, передача голоса на расстоянии. Стоит нам набрать номер абонента, и через несколько мгновений два телефонных аппарата окажутся соединенными между собой, мы сможем общаться с собеседником на другом конце провода. Для того чтобы это произошло, электрические сигналы в телефонной сети вырабатываются и распределяются по определенным правилам, а управляют этими сигналами АТС (автоматические телефонные станции). В современной телефонной сети правила обработки сигналов очень сложны. Но, возможно, вы помните детскую игрушку из двух телефонных трубок, соединенных проводом. Эта простейшая телефонная сеть тоже вполне работоспособна. Аналогично и в компьютерной сети. Большие сети, состоящие из множества компьютеров, управляются сложными электронными устройствами, такими как маршрутизаторы, коммутаторы, серверы. Электрические сигналы в компьютерной сети претерпевают сложнейшую обработку по правилам, которые называют *протоколами*.

Но вполне возможно соединить два компьютера специальным кабелем, и мы получим простейшую сеть. Сигналы в этой сети будут обрабатываться самими компьютерами по протоколам, которые предусмотрены разработчиками компьютеров и программного обеспечения. Ведь компьютер сам по себе не сможет работать, и не только в сети. Необходимы компьютерные программы. Самые важные для работы компьютеров программы — операционные системы. Эти программы обеспечивают общение человека с компьютером, переводя понятные человеку символы на язык машины и обратно. Для того чтобы передать компьютеру команды и понять ответ компьютера, существуют интерфейсы. Интерфейс — очень широкое понятие. Достаточно сказать, что к интерфейсу относят и изображение на экране компьютерного монитора, и клавиатуру для ввода символов и команд, и манипулятор "мышь" (часто называют просто "мышка") для управления визуальными элементами интерфейса на экране монитора. Интерфейсы нужны не только для общения человека и компьютера, но и для общения компьютера с различными периферийными устройствами. Поэтому в литературе вы можете встретить и такое понятие, как *интерфейсный кабель*. Простой пример такого кабеля — кабель, соединяющий компьютер с принтером, который необходим для вывода в печатном виде текстов и изображений из памяти компьютера.

Среда передачи данных и топология

Современная компьютерная сеть, как и телефонная, может быть построена не только на кабельных соединениях. Сотовый телефон, например, не требует кабеля для подключения к телефонной сети, и компьютеры могут объединяться по радиоканалу. Сейчас активно распространяются беспроводные технологии и в компьютерных сетях. Да и кабели могут быть не только с электропроводящими жилами, но и с оптическими волокнами. Возможно, что вы уже слышали об оптоволоконных линиях, соединяющих дома и целые городские районы в оптоволоконную сеть для подключения пользователей персональных компьютеров к глобальной сети Интернет, передачи цифрового телевидения, обеспечения работы IP-телефонии. Новые технологии активно вторгаются в нашу жизнь. Но среда передачи сигналов в нашей первой сети будет традиционной. Мы будем объединять компьютеры в сеть с помощью витой пары. Это кабель, состоящий из четырех пар свитых между собой медных изолированных проводников, заключенных в полимерную оболочку (рис. 1.1).

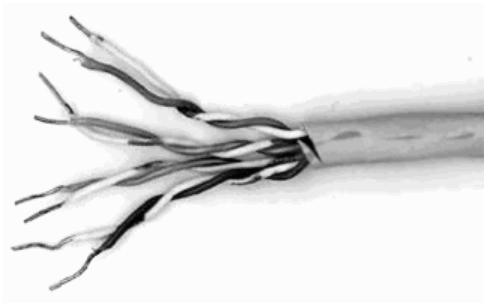


Рис. 1.1. Кабель типа "витая пара"

Такая конструкция кабеля часто применяется и в телефонных сетях. Но компьютерная сеть требует особого качества кабеля. Обычно для построения компьютерной сети применяется кабель не ниже пятой категории. На оболочке такого кабеля можно увидеть маркировку UTP 5 или UTP 5e. Применение кабеля категории ниже пятой может привести к сбоям в работе сети, особенно при значительных расстояниях между компьютерами. Но в любом случае одно из условий нормальной работы сети — расстояние между ее узлами не более 80 метров. Узел сети это любой ее компьютер или другое сетевое устройство, например, сетевой принтер, которое включено в сеть.

Концы кабеля обжимаются коннекторами (разъемами) типа RJ-45 (рис. 1.2).

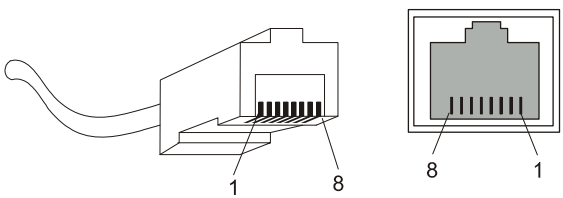


Рис. 1.2. Коннектор RJ-45 и гнездо для него

Предварительно освобожденные от оболочки и выровненные по длине проводники вводят в коннектор и обжимают специальным инструментом — обжимкой. Подробное руководство по обжиму кабеля вы можете найти по адресу в Интернете:
http://www.xnets.ru/plugins/content/content.php?content.44.

Жилы кабеля должны подходить к контактам коннектора по определенной схеме. Так, для простого объединения в сеть двух компьютеров необходим перекрестный (Crossover) кабель. Это значит, что в разъемах на концах кабеля проводники будут расположены не одинаково. Схема подключения коннекторов к кабелю в этом случае показана в табл. 1.1.

Таблица 1.1. *Схема обжима перекрестного кабеля*

Коннектор 1	**Номер контакта**	**Коннектор 2**
Бело-зеленый	1	Бело-оранжевый
Зеленый	2	Оранжевый
Бело-оранжевый	3	Бело-зеленый
Синий	4	Синий
Бело-синий	5	Бело-синий
Оранжевый	6	Зеленый
Бело-коричневый	7	Бело-коричневый
Коричневый	8	Коричневый

Необходимо соблюдать распределение жил кабеля в соответствии с их цветом. Обычно для работы сети используются 1—2 и 3—6 контакты. К этим парам контактов должны подходить витые пары проводников. Другие контакты обычно не используются, но соблюдение порядка их обжима позволит получить наилучшее качество готового кабеля.

Рис. 1.3. Типичный коммутатор для домашней сети

Перекрестным кабелем можно соединить только два компьютера. Для обеспечения возможности объединения более двух компьютеров в сеть следует использовать дополнительное устройство — *коммутатор* (рис. 1.3). Коммутаторы имеют несколько гнезд для подключения сетевых устройств, а кабель для соединения компьютера с коммутатором должен быть обычным не перекрестным.

В этом случае схема обжима кабеля будет такой, как в табл. 1.2 или 1.3. Оба способа могут применяться на равных правах, но лучше выбрать один из них для постоянного применения.

Таблица 1.2. *Схема обжима кабеля по стандарту T568A*

Коннектор 1	**Номер контакта**	**Коннектор 2**
Бело-зеленый	1	Бело-зеленый
Зеленый	2	Зеленый
Бело-оранжевый	3	Бело-оранжевый
Синий	4	Синий
Бело-синий	5	Бело-синий
Оранжевый	6	Оранжевый
Бело-коричневый	7	Бело-коричневый
Коричневый	8	Коричневый

Таблица 1.3. *Схема обжима кабеля по стандарту T568B*

Коннектор 1	**Номер контакта**	**Коннектор 2**
Бело-оранжевый	1	Бело-оранжевый
Оранжевый	2	Оранжевый
Бело-зеленый	3	Бело-зеленый
Синий	4	Синий
Бело-синий	5	Бело-синий
Зеленый	6	Зеленый

Таблица 1.3 *(окончание)*

Коннектор 1	Номер контакта	Коннектор 2
Бело-коричневый	7	Бело-коричневый
Коричневый	8	Коричневый

Подключая компьютеры и другие устройства к коммутатору, мы невольно создадим одну из распространенных топологических схем локальной сети. Эта схема называется "звезда". В центре этой звезды находится коммутатор, а все сетевые устройства — на концах ее лучей. Современные сети могут иметь сложную топологическую структуру, но чаще всего применяется именно такая топология. Ранее применялась еще шинная топология, когда последовательно коаксиальным кабелем соединялись несколько узлов. Кабель типа "витая пара" не позволяет использовать такую топологию, но нам она и не потребуется. Топология "звезда" более гибка, позволяет подключать и отключать устройства, не вызывая перебоев в работе сети. 10BASE-T, 100BASE-T — такие наименования технологий, применяемых в нашей сети, можно встретить в литературе. Ethernet 10/100/1000 — это наименование порта (точки подключения, гнезда), который, скорее всего, имеется в вашем сетевом адаптере (сетевой карте) — устройстве, необходимом для подключения компьютера к сети.

Правила работы сети — сетевые протоколы

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 Мбит/с 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 10 Мбит/с, что вполне нас устроит.

Но в любом случае правила, по которым будет работать сеть, одни и те же. Сетевое оборудование будет использовать 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.

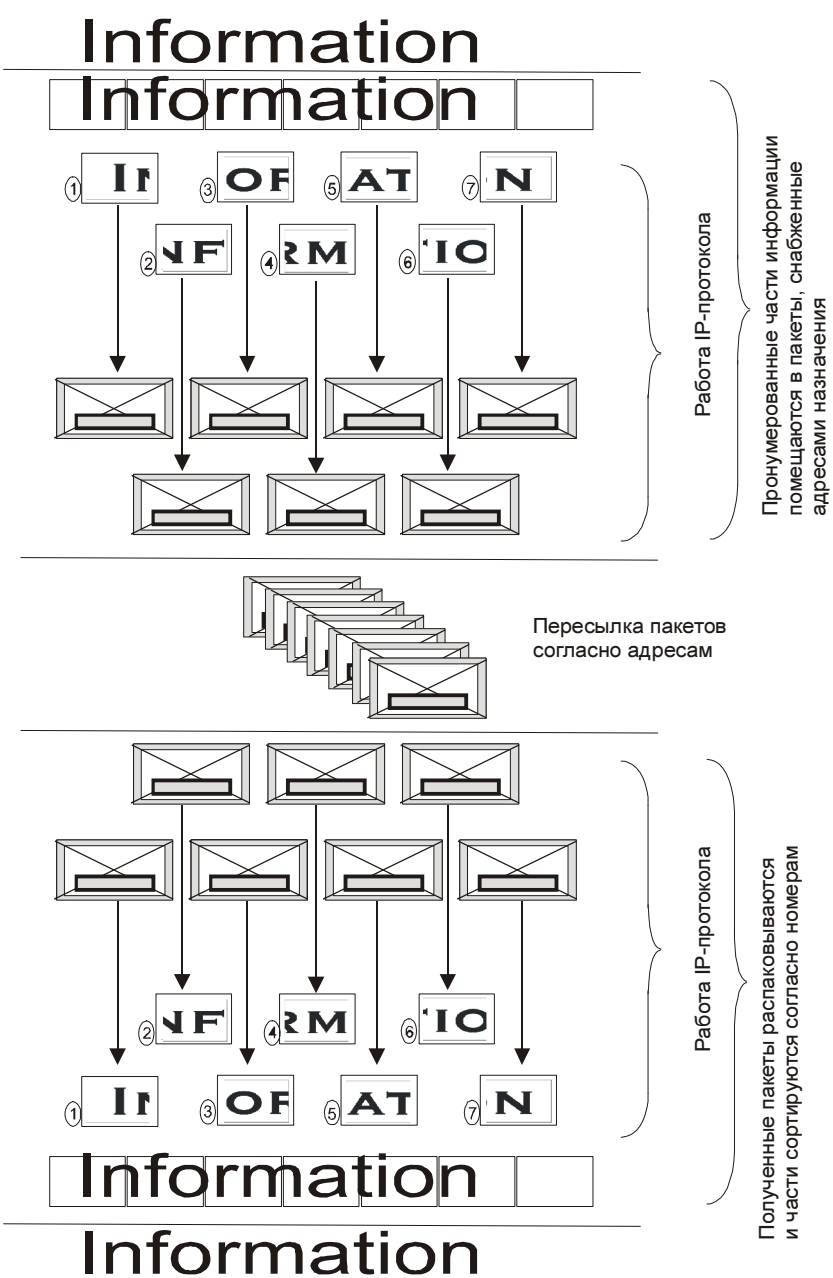


Рис. 1.4. Графическое представление работы TCP/IP

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 (правилам общения компьютеров 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 сеть должна работать по общим правилам. Понять суть работы этих правил проще всего, посмотрев на графическое представление работы TCP/IP (рис. 1.4).

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.

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

Протокол IP нумерует пакеты информации 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. 1.4).

Таблица 1.4. *Диапазоны адресов для классов сетей*

Класс сети	Маска подсети	Диапазон	Зарезервированные адреса
A	255.0.0.0	01.0.0.0—126.0.0.0	С 10.0.0.0 по 10.255.255.255 С 127.0.0.0 по 127.255.255.255
B	255.255.0.0	128.0.0.0— 191.255.0.0	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 указывает на биты, предназначенные для задания адреса сети, в остальных полях адреса должен располагаться адрес компьютера. Каждому классу сети соответствует свой диапазон применяемых и неприменяемых в Интернете (зарезервированных) адресов.

Структура адреса становится более понятной при представлении в двоичном коде. Например, маска 255.255.255.0 в двоичном коде выглядит так: 11111111.11111111.11111111.0. Все поля адреса сети заняты единицами. Адрес 198.168.55.1 в двоичном коде выглядит так: 11000110.10101000.110111.1. По таблице можно определить, что это адрес сети класса "С", а адрес компьютера (узла) выражен младшей единицей. Чем ниже класс сети, тем больше адресов сети может существовать и тем меньше компьютеров может находиться в такой сети. Каждый компьютер в сети имеет свой уникальный адрес, назначенный администратором сети или полученный автоматически. Именно с такими адресами и работает протокол IP. 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 выделить 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 64 516 узлов. Для общего применения такие значения адресов не рекомендованы, но в закрытых сетях их можно использовать, как и адреса 10.0.0/24. Расширение (табл. 1.5), таким образом, позволяет более точно указать назначение адреса, независимо от принятых договоренностей о применении диапазонов адресов.

Таблица 1.5. *Расширение масок подсети от 24 до 32*

Маска подсети 255.255.255.0 /24 (11111111.11111111.11111111.00000000)			
1 подсеть			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.255		
Маска подсети 255.255.255.128/25 (11111111.11111111.11111111.10000000)			
2 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.127	x.x.x.128	x.x.x.255
Маска подсети 255.255.255.192/26 (11111111.11111111.11111111.11000000)			
4 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.63	x.x.x.128	x.x.x.191
x.x.x.64	x.x.x.127	x.x.x.192	x.x.x.255

Таблица 1.5 *(продолжение)*

Маска подсети 255.255.255.224/27 (11111111.11111111.11111111.11100000)			
8 подсетей			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.31	x.x.x.128	x.x.x.159
x.x.x.32	x.x.x.63	x.x.x.160	x.x.x.191
x.x.x.64	x.x.x.95	x.x.x.192	x.x.x.223
x.x.x.96	x.x.x.127	x.x.x.224	x.x.x.255
Маска подсети 255.255.255.240/28 (11111111.11111111.11111111.11110000)			
16 подсетей			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.15	x.x.x.128	x.x.x.143
x.x.x.16	x.x.x.31	x.x.x.144	x.x.x.159
x.x.x.32	x.x.x.47	x.x.x.160	x.x.x.175
x.x.x.48	x.x.x.63	x.x.x.176	x.x.x.191
x.x.x.64	x.x.x.79	x.x.x.192	x.x.x.207
x.x.x.80	x.x.x.95	x.x.x.208	x.x.x.223
x.x.x.96	x.x.x.111	x.x.x.224	x.x.x.239
x.x.x.112	x.x.x.127	x.x.x.240	x.x.x.255
Маска подсети 255.255.255.248/29 (11111111.11111111.11111111.11111000)			
32 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.7	x.x.x.128	x.x.x.135
x.x.x.8	x.x.x.15	x.x.x.136	x.x.x.143
x.x.x.16	x.x.x.23	x.x.x.144	x.x.x.151
x.x.x.24	x.x.x.31	x.x.x.152	x.x.x.159

Таблица 1.5 *(продолжение)*

Маска подсети 255.255.255.248/29 (11111111.11111111.11111111.11111000)			
32 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.32	x.x.x.39	x.x.x.160	x.x.x.167
x.x.x.40	x.x.x.47	x.x.x.168	x.x.x.175
x.x.x.48	x.x.x.55	x.x.x.176	x.x.x.183
x.x.x.56	x.x.x.63	x.x.x.184	x.x.x.191
x.x.x.64	x.x.x.71	x.x.x.192	x.x.x.199
x.x.x.72	x.x.x.79	x.x.x.200	x.x.x.207
x.x.x.80	x.x.x.87	x.x.x.208	x.x.x.215
x.x.x.88	x.x.x.95	x.x.x.216	x.x.x.223
x.x.x.96	x.x.x.103	x.x.x.224	x.x.x.231
x.x.x.104	x.x.x.111	x.x.x.232	x.x.x.239
x.x.x.112	x.x.x.119	x.x.x.240	x.x.x.247
x.x.x.120	x.x.x.127	x.x.x.248	x.x.x.255
Маска подсети 255.255.255.252/30 (11111111.11111111.11111111.11111100)			
64 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.3	x.x.x.128	x.x.x.131
x.x.x.4	x.x.x.7	x.x.x.132	x.x.x.135
x.x.x.8	x.x.x.11	x.x.x.136	x.x.x.139
x.x.x.12	x.x.x.15	x.x.x.140	x.x.x.143
x.x.x.16	x.x.x.19	x.x.x.144	x.x.x.147
x.x.x.20	x.x.x.23	x.x.x.148	x.x.x.151
x.x.x.24	x.x.x.27	x.x.x.152	x.x.x.155

Таблица 1.5 *(продолжение)*

Маска подсети 255.255.255.252/30 (11111111.11111111.11111111.11111100)			
64 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.28	x.x.x.31	x.x.x.156	x.x.x.159
x.x.x.32	x.x.x.35	x.x.x.160	x.x.x.163
x.x.x.36	x.x.x.39	x.x.x.164	x.x.x.167
x.x.x.40	x.x.x.43	x.x.x.168	x.x.x.171
x.x.x.44	x.x.x.47	x.x.x.172	x.x.x.175
x.x.x.48	x.x.x.51	x.x.x.176	x.x.x.179
x.x.x.52	x.x.x.55	x.x.x.180	x.x.x.183
x.x.x.56	x.x.x.59	x.x.x.184	x.x.x.187
x.x.x.60	x.x.x.63	x.x.x.188	x.x.x.191
x.x.x.64	x.x.x.67	x.x.x.192	x.x.x.195
x.x.x.68	x.x.x.71	x.x.x.196	x.x.x.199
x.x.x.72	x.x.x.75	x.x.x.200	x.x.x.203
x.x.x.76	x.x.x.79	x.x.x.204	x.x.x.207
x.x.x.80	x.x.x.83	x.x.x.208	x.x.x.211
x.x.x.84	x.x.x.87	x.x.x.212	x.x.x.215
x.x.x.88	x.x.x.91	x.x.x.216	x.x.x.219
x.x.x.92	x.x.x.95	x.x.x.220	x.x.x.223
x.x.x.96	x.x.x.99	x.x.x.224	x.x.x.227
x.x.x.100	x.x.x.103	x.x.x.228	x.x.x.231
x.x.x.104	x.x.x.107	x.x.x.232	x.x.x.235
x.x.x.108	x.x.x.111	x.x.x.236	x.x.x.239
x.x.x.112	x.x.x.115	x.x.x.240	x.x.x.243

Таблица 1.5 *(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.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. 1.6 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 1.6. *Связь между расширением маски подсети, двоичной записью маски и побайтовой записью*

Расширение	**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
/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

Таблица 1.6 *(продолжение)*

Расширение	Маска подсети в двоичном представлении	Побайтовое представление	Число узлов	Класс
/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

Таблица 1.6 *(окончание)*

Расширение	Маска подсети в двоичном представлении	Побайтовое представление	Число узлов	Класс
/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).

```
11000000 Bin = 128*1 + 64*1 + 32*0 + 16*0 + 8*0 + 4*0 + 2*0 + 1*0
             = 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0
             = 128 + 64
             = 192
```

В Интернете и в больших сетях практически не применяются числовые адреса для поиска узлов или сайтов. Просто не удобно запоминать эти адреса. Поэтому была разработана система доменных имен — DNS.

Отображение символьных адресов на IP-адреса: служба DNS

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. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров на IP-адрес.

В Интернете и во многих локальных сетях существуют DNS-серверы, на которых регистрируются доменные имена и записываются соответствия их IP-адресам. Сами DNS-серверы не имеют символьных адресов и их IP-адреса указываются при настройке подключения к Интернету.

Автоматизация процесса назначения IP-адресов узлам сети. Протокол DHCP

Как уже было сказано, IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети, и поэтому должны полагаться на администраторов.

Протокол *Dynamic Host Configuration Protocol* (DHCP, протокол динамической настройки конфигурации хоста) был разработан для того, чтобы освободить администратора от этих проблем. Основной работой DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра, именуемого "продолжительность аренды" (lease duration), который определяет, как долго компьютер может использо-

вать назначенный IP-адрес, перед тем как снова запросить его у сервера DHCP в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Протокол DHCP использует модель "клиент-сервер". Во время старта системы компьютер-клиент DHCP, находящийся в состоянии "инициализация", посылает сообщение `discover` (исследовать), которое широковещательно распространяется по локальной сети и передается всем DHCP-серверам частной интрасети. Каждый DHCP-сервер, получивший это сообщение, отвечает на него сообщением `offer` (предложение), которое содержит IP-адрес и конфигурационную информацию.

Компьютер-клиент DHCP переходит в состояние "выбор" и собирает конфигурационные предложения от DHCP-серверов. Затем он выбирает одно из этих предложений, переходит в состояние "запрос" и отправляет сообщение `request` (запрос) тому DHCP-серверу, чье предложение было выбрано.

Выбранный DHCP-сервер посылает сообщение `DHCP-acknowledgment` (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, DHCP-сервер отправляет параметры сетевой конфигурации. После того как клиент получит это подтверждение, он переходит в состояние "связь", находясь в котором, он может принимать участие в работе сети TCP/IP. Компьютеры-клиенты, которые имеют локальные диски, сохраняют полученный адрес для использования при последующих стартах системы. При приближении момента истечения срока аренды адреса компьютер пытается обновить параметры аренды у DHCP-сервера, а если этот IP-адрес не может быть выделен снова, то ему возвращается другой IP-адрес.

В протоколе DHCP описывается несколько типов сообщений, которые используются для обнаружения и выбора DHCP-серверов, запросов информации о конфигурации, продления и досрочного прекращения лицензии на IP-адрес. Все эти операции направлены на то, чтобы освободить администратора сети от утомительных рутинных операций конфигурирования сети.

Однако использование DHCP создает и некоторые проблемы. Во-первых, это проблема согласования информационной адресной базы в службах DHCP и

DNS. Как известно, DNS служит для преобразования символьных имен в IP-адреса. Если IP-адреса будут динамически изменяться сервером DHCP, то эти изменения необходимо также динамически вносить в базу данных сервера DNS. Хотя протокол динамического взаимодействия между службами DNS и DHCP реализован некоторыми фирмами (так называемая служба Dynamic DNS), стандарт на него пока не принят.

Во-вторых, нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов. Аналогичные проблемы возникают и при конфигурировании фильтров-маршрутизаторов, которые оперируют IP-адресами.

Наконец, централизация процедуры назначения адресов снижает надежность системы: при отказе DHCP-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации. Негативные последствия такого отказа могут быть уменьшены путем использования в сети нескольких серверов DHCP, каждый из которых имеет свой пул IP-адресов.

> ***Примечание***
>
> Вполне возможно, что ваш компьютер содержит несколько операционных систем, и каждая из них позволяет работать в сети. В каждой из установленных операционных систем вы можете назначить компьютеру различные символьные имена. Сервер DHCP, ориентируясь на аппаратный (MAC) адрес сетевого адаптера, каждый раз при перезагрузке будет выдавать один и тот же IP-адрес, несмотря на изменение символьного имени компьютера.

Со временем протокол IP претерпевал множество модификаций, которые существенно улучшили многие его параметры. Однако быстрота и перспективы дальнейшего роста сети поставили перед IP-протоколом, который используется в настоящее время, ряд серьезных проблем:

- истощение адресного пространства;
- неограниченный рост маршрутных таблиц;
- отсутствие встроенных механизмов обеспечения "качества обслуживания";
- отсутствие встроенных механизмов автоконфигурации хостов;
- отсутствие встроенных средств безопасности;
- неэффективность механизмов поддержки мобильных устройств.

Для устранения перечисленных недостатков IP-протокола Проблемная группа проектирования Интернета (IETF, Internet Engineering Task Force) разработала спецификации IP-протокола следующего поколения, известного как IPng, или IPv6. Внедрение протокола IPv6 является одновременно и насущной задачей, и долгосрочной перспективой для сетевых администраторов и операторов сетей общего пользования. С одной стороны, продукты, поддерживающие IPv6, уже появились на рынке, с другой стороны, доработка и усовершенствование IPv6, вероятно, будут продолжаться. Несмотря на то, что в основе IPv6 лежат необходимые доработки прежней версии протокола IP (IPv4), IPv6 следует воспринимать как новый протокол, который станет прочным фундаментом сетей в будущем.

Приняты три формы представления адресов IPv6 в текстовом виде.

1. Предпочтительная форма x:x:x:x:x:x:x:x, где знаки "x" — шестнадцатеричные значения восьми 16-битных частей адреса. Нет необходимости писать ведущие нули в каждом отдельном поле, однако в каждом поле должна быть, по меньшей мере, одна цифра. Например,

   3FFE:2403:0:0:280:C8FF:FE4B:F7A8

   FF01:0:0:0:0:0:0:101

   0:0:0:0:0:0:0:1

   0:0:0:0:0:0:0:0

2. Для облегчения записи адресов, содержащих длинные последовательности нулевых битов, принят специальный синтаксис сжатия нулей. Обозначение "::" указывает на наличие нескольких 16-битных групп нулей. Это обозначение может присутствовать в адресе только один раз. Оно используется также для сжатия ведущих и/или концевых нулей в адресе. Например,

   3FFE:2403::280:C8FF:FE4B:F7A8

   FF01::101

   ::1

   ::

3. Альтернативной формой, которая иногда более удобна при работе в смешанной среде узлов IPv4 и IPv6, является x:x:x:x:x:x:d.d.d.d, где знаки "x" — шестнадцатеричные значения шести старших 16-битных частей адреса, а "d" — десятичные значения четырех младших октетов адреса (стандартное представление IPv4).

Например,

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

или в сжатой форме:

::13.1.68.3

::FFFF:129.144.52.38

Специалисты предупреждают, что с вводом IPv6 медлить нельзя, высока вероятность того, что адреса закончатся до того, как будет введен IPv6. Существующие свободные IP-адреса начнут интенсивно раздаваться с ростом количества беспроводных устройств с доступом в Интернет, каждое из которых должно иметь свой IP-адрес. Уже теперь заметен значительный рост популярности мобильных средств связи со встроенными интернет-возможностями. Последние версии Windows содержат новый протокол, но широкого применения пока он не получил. Существенной практики работы с этим протоколом у обычных пользователей ПК еще нет. При необходимости использования этого протокола в вашей сети пока лучше ориентироваться на автоматические настройки. Впрочем, дома вряд ли можно увидеть явные выгоды от применения IPv6.

Возможно, что теоретические сведения, которые представлены выше, не очень просты для восприятия сходу. Но в дальнейшем, когда вы столкнетесь с вопросами настройки IP-протокола, они помогут вам выполнять эти настройки осознанно.

Операционные системы для работы в сети, установка и настройка

Что ж, пока теории хватит. Все теоретические сведения, которые потребуются в дальнейшем, мы будем рассматривать по ходу изложения. Если вы уже можете соединить два компьютера перекрестным кабелем или с помощью двух отрезков кабеля посредством коммутатора, можно приступать к настройке сети. Все настройки необходимо выполнять на узлах сети. Узлами нашей сети могут быть компьютеры, ADSL-модемы для подключения сети к Интернету и маршрутизаторы. Начнем с компьютеров. Компьютер не может работать сам по себе без программного обеспечения. Прежде всего, необходимо установить операционную систему (ОС), в которой и будут произведе-

ны основные настройки для работы в сети. Мы рассмотрим установку и настройку наиболее распространенных у домашних пользователей ОС. Даже если на ваших компьютерах ОС были предустановлены изготовителями, процедуру установки необходимо знать, чтобы впоследствии при возникновении необходимости иметь возможность самостоятельно установить систему или переустановить. Если вы считаете, что для выполнения этой процедуры всегда можно пригласить специалиста, — ваше дело. Но цена этой работы сейчас несколько сотен рублей, не считая цены за вызов специалиста. Настройка системы для работы в вашей сети обойдется еще в несколько сотен рублей...

Думаю, что я вас убедил в необходимости освоения этих процедур.

Windows Vista

Пожалуй, наиболее распространенной на новых компьютерах в последнее время стала операционная система Windows Vista.

Возможно, что компьютер, купленный вами, уже содержит предустановленную операционную систему Windows Vista. Если у вас еще нет компьютера, то по возможности приобретайте его именно в таком виде. Тем не менее, возможно, что вы будете использовать компьютер, на котором уже была установлена другая операционная система, которую вы решили заменить на Windows Vista. В таком случае необходимо ознакомиться с процедурой установки этой операционной системы.

Перед установкой системы необходимо убедиться, что компьютер, на который вы собрались установить ее, подходит для этого. Если ваш компьютер собран в этом году, то, скорее всего, проблем с установкой не возникнет. Совершенно не будет проблем, если вы приобрели готовый компьютер и на нем есть наклейка с надписью "Windows Vista Capable" (совместимо с Windows Vista), Works with Windows Vista или Certified for Windows Vista (рис. 1.5).

В других случаях перед установкой можно проверить совместимость вашего "железа" с новой операционной системой. В значительной степени и сама устанавливаемая система может подстраиваться под аппаратную часть. Если какие-либо параметры компьютера не дотягивают до идеала, то система сама решит, как распределить память, а возможно, и какие части системы не следует устанавливать вообще. Правда, недостаточный объем оперативной памяти (менее 512 Мбайт) не позволит произвести установку системы. Еще до начала установки убедитесь, что вы держите в руках официальный дистрибу-

тив системы. Возможно, что к вам попал слегка переработанный любителями тестовый дистрибутив. Тестовых версий было довольно много, все они содержали те или иные ошибки и отличия. В интерфейсе системы были изменения от версии к версии во время тестирования. Конечно, если вы официально приобрели этот дистрибутив, то вам не грозят проблемы, связанные с использованием нефинального дистрибутива.

Рис. 1.5. Сертифицировано для Windows Vista

Примечание

Windows Vista требует активации через Интернет до истечения тестового периода 30 дней.

Вариант функциональности установленной системы зависит от Product Key (ключ продукта), который представляет собой пять групп по пять алфавитно-цифровых символов, но дистрибутив системы (установочный диск) содержит все необходимое для всех версий Vista.

Эти символы должны быть введены на одном из этапов установки. В зависимости от того, к какой версии системы относится ключ, вы в результате установки можете получить следующие варианты системы.

Windows Vista Starter

Самая недорогая и доступная версия для бытовых ПК и пользователей начального уровня. Базовый набор возможностей Windows Vista Starter несколько урезан, хотя и близок к Home Basic, главное, что сохраняется со-

вместимость со всеми современными приложениями и устройствами. Фактически это операционная система для начинающих, делающих первые шаги в освоении ПК.

Windows Vista Home Basic

Это простой и доступный вариант начального уровня, преимущественно для домашних пользователей. Обладает всеми ключевыми характеристиками ОС нового поколения: безопасностью, поддержкой расширенного родительского контроля, базовым интерфейсом пользователя, новыми функциями поиска и систематизации данных, улучшенной работой в сети.

Windows Vista Home Premium

Основной вариант Windows Vista для домашних пользователей настольных и мобильных ПК. Помимо возможностей Vista Home Basic в этом выпуске поддерживается 3-мерный интерфейс пользователя Windows Aero, функциональность Windows Media Center, ряд дополнительных возможностей по работе с мультимедийными данными вроде редактирования и записи DVD. Наряду с этим реализована возможность работы системы в виде Windows Tablet PC, поддерживаются дополнительные возможности повышения мобильности вроде функции синхронизации двух ПК.

Windows Vista Business

Основная аппаратная платформа для настольных и мобильных ПК корпоративного класса. Vista Business подходит для малого, среднего бизнеса и крупных предприятий, содержит все функции Vista Home Basic (кроме ряда развлекательных) и имеет ряд специфических особенностей. Так, Vista Business поддерживает интерфейс Windows Aero, возможности Windows Tablet PC, ряд функций повышения мобильности, плюс исключительно корпоративные возможности вроде подключения к домену, поддержку групповой политики, шифрование файловой системы, поддержку факсов и сканеров и пр.

Windows Vista Enterprise

Расширенный вариант Vista для корпоративных ПК и ноутбуков, исключительно для клиентов программы Microsoft Software Assurance. То есть до-

машним пользователям этот выпуск доступен не будет. В дополнение к возможностям Vista Business эта версия обладает средствами шифрования диска Windows BitLocker, поддерживает все существующие языки интерфейса, функцию Virtual PC Express, которая не входит ни в одну другую версию, и подсистему для приложений на основе UNIX (SUA). Словом, система с учетом специфики работы крупных предприятий и организаций со сложной инфраструктурой.

Windows Vista Ultimate

Исчерпывающе полный вариант Vista для пользователей настольных и мобильных ПК класса "персоналка" или "малый офис", наряду с полным набором возможностей версий Home Premium и Enterprise. Windows Vista Ultimate содержит все необходимое для одинаково комфортной работы дома, в поездках и в офисе.

В табл. 1.7 подробно показаны функциональные возможности различных выпусков системы. Возможности, отсутствующие в выпуске, отмечены словом "Нет", выделенным жирным шрифтом. Это позволит вам оперативно просмотреть таблицу при оценке возможностей приобретаемой системы. Назначение функций до прочтения книги и некоторого периода собственной практической работы вам может быть не совсем понятно. Большинство домашних пользователей вообще никогда не столкнется с необходимостью применения многих возможностей системы.

Таблица 1.7. *Функциональные возможности выпусков Vista*

Функциональные возможности	Home Basic	Home Premium	Business	Enterprise	Ultimate
Контроль учетных записей пользователей	Да	Да	Да	Да	Да
Центр безопасности Windows	Да	Да	Да	Да	Да
Защитник Windows	Да	Да	Да	Да	Да
Брандмауэр Windows	Да	Да	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Защищенный режим Internet Explorer 7	Да	Да	Да	Да	Да
Исправление параметров безопасности в Internet Explorer 7	Да	Да	Да	Да	Да
Фильтр фишинга в Internet Explorer 7	Да	Да	Да	Да	Да
Фильтр фишинга в Windows Mail	Да	Да	Да	Да	Да
Служба Windows Update	Да	Да	Да	Да	Да
Родительский контроль	Да	Да	**Нет**	**Нет**	Да
Уменьшение числа перезагрузок, зависаний и сбоев	Да	Да	Да	Да	Да
Ограничение полномочий служб	Да	Да	Да	Да	Да
Автоматическая настройка производительности и диагностика оборудования	Да	Да	Да	Да	Да
Стек TCP/IP нового поколения	Да	Да	Да	Да	Да
Поддержка IPv6 и IPv4	Да	Да	Да	Да	Да
Windows ReadyDrive	Да	Да	Да	Да	Да
Windows Display Driver Model (WDDM)	Да	Да	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Средство переноса данных Windows	Да	Да	Да	Да	Да
Поддержка 64-разрядных процессоров	Да	Да	Да	Да	Да
Быстрая загрузка, быстрое выключение и переход в спящий режим	Да	Да	Да	Да	Да
Максимальный поддерживаемый объем памяти (32-разрядная система), Гбайт	4	4	4	4	4
Максимальный поддерживаемый объем памяти (64-разрядная система), Гбайт	8	16	128	128	128
Поддержка двух процессоров (двух процессорных разъемов)	**Нет**	**Нет**	Да	Да	Да
Резервное копирование и восстановление файлов и папок пользователя	**Нет**	**Нет**	Да	Да	Да
Резервное копирование файлов пользователя по сети	**Нет**	**Нет**	Да	Да	Да
Windows ShadowCopy (теневая копия системы)	**Нет**	**Нет**	Да	Да	Да
Резервное копирование и восстановление на основе образа системы	**Нет**	**Нет**	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Шифрование файловой системы	**Нет**	**Нет**	Да	Да	Да
Средства распространения приложений для управляемых сетей	**Нет**	**Нет**	Да	Да	Да
QoS на основе политик для сетевых подключений	**Нет**	**Нет**	Да	Да	Да
Клиент службы управления правами Windows (RMS)	**Нет**	**Нет**	Да	Да	Да
Управляемая установка драйверов устройств	**Нет**	**Нет**	Да	Да	Да
Агент клиента NAP	**Нет**	**Нет**	Да	Да	Да
Подключаемая архитектура проверки подлинности при входе в систему	**Нет**	**Нет**	Да	Да	Да
Встроенные средства управления смарт-картами	**Нет**	**Нет**	Да	Да	Да
Средство шифрования диска Windows BitLocker	**Нет**	**Нет**	**Нет**	Да	Да
Поддержка одновременной установки нескольких языков интерфейса пользователя	**Нет**	**Нет**	**Нет**	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Возможность выбора языков интерфейса пользователя для всех стран мира (36 языков)	**Нет**	**Нет**	**Нет**	Да	Да
Подсистема для приложений на основе UNIX	**Нет**	**Нет**	**Нет**	Да	Да
Virtual PC Express	**Нет**	**Нет**	**Нет**	Да	**Нет**
Программа обновления Windows Anytime Upgrade	Да	Да	Да	**Нет**	**Нет**
Дополнения для Windows Ultimate	**Нет**	**Нет**	**Нет**	**Нет**	Да
Упрощенный интерфейс пользователя Windows Vista	Да	Да	Да	Да	Да
Интерфейс пользователя Windows Aero с элементами Glass ("стекло"), Windows Flip, Windows Flip 3D, масштабируемыми миниатюрами на панели задач, динамическими окнами и более плавным отображением рабочего стола	**Нет**	Да	Да	Да	Да
Средство быстрого поиска по всей операционной системе	Да	Да	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Автоматическая систематизация содержимого на основе свойств и меток файла	Да	Да	Да	Да	Да
Internet Explorer 7 с поддержкой вкладок, быстрыми вкладками и встроенным поиском	Да	Да	Да	Да	Да
Internet Explorer 7 с поддержкой RSS-каналов	Да	Да	Да	Да	Да
Поддержка приложений нового поколения, основанных на технологии WinFX	Да	Да	Да	Да	Да
Windows SuperFetch	Да	Да	Да	Да	Да
Windows ReadyBoost	Да	Да	Да	Да	Да
Ввод и вывод с низким приоритетом	Да	Да	Да	Да	Да
Автоматическая дефрагментация жесткого диска	Да	Да	Да	Да	Да
Windows Mail	Да	Да	Да	Да	Да
Календарь Windows	Да	Да	Да	Да	Да
Боковая панель Windows	Да	Да	Да	Да	Да
Фотоальбом Windows	Да	Да	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Средство быстрого поиска по всей операционной системе	Да	Да	Да	Да	Да
Тематические слайд-шоу	**Нет**	Да	**Нет**	**Нет**	Да
Windows Media 11	Да	Да	Да	Да	Да
Windows Media Center (музыка, фото, видео, ТВ, записанные ТВ-программы, интерактивные развлечения)	**Нет**	Да	**Нет**	**Нет**	Да
Windows Media Center (просмотр и запись ТВ высокой четкости)	**Нет**	Да	**Нет**	**Нет**	Да
Windows Media Center, поддержка CableCard	**Нет**	Да	**Нет**	**Нет**	Да
Поддержка Media Center Extender, в том числе Xbox 360	**Нет**	Да	**Нет**	**Нет**	Да
Windows Movie Maker	Да	Да	**Нет**	**Нет**	Да
Windows Movie Maker HD	**Нет**	Да	**Нет**	**Нет**	Да
Windows DVD Maker	**Нет**	Да	**Нет**	**Нет**	Да
Проводник игр	Да	Да	Да	Да	Да
Обновленные игры	Да	Да	Да	Да	Да
Новые дополнительные игры	**Нет**	Да	Возможно	Возможно	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Поддержка универсальных игровых устройств	Да	Да	Возможно	Возможно	Да
Распознавание речи	Да	Да	Да	Да	Да
Специальные возможности и центр специальных возможностей	Да	Да	Да	Да	Да
Центр начальной настройки Windows	Да	Да	Да	Да	Да
Поддержка документов в формате XPS	Да	Да	Да	Да	Да
Ресурсы для малых предприятий	**Нет**	**Нет**	Да	**Нет**	Да
Факсы и сканеры Windows	**Нет**	**Нет**	Да	Возможно	Возможно
Сетевой центр	Да	Да	Да	Да	Да
Диагностика сети и устранение неисправностей	Да	Да	Да	Да	Да
Улучшенная поддержка беспроводных сетевых соединений	Да	Да	Да	Да	Да
Обеспечение поддержки беспроводной сети	**Нет**	**Нет**	Да	Да	Да
Улучшенная поддержка одноранговых сетей	Да	Да	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Улучшенная поддержка VPN	Да	Да	Да	Да	Да
Улучшенное управление питанием	Да	Да	Да	Да	Да
Количество одновременных подключений по протоколу SMB в одноранговой сети	5	5	10	10	10
Windows HotStart	Да	Да	Да	Да	Да
Центр мобильных устройств Windows	Частично	Частично	Да	Да	Да
Центр синхронизации	Да	Да	Да	Да	Да
Windows Tablet PC со встроенной поддержкой рукописного ввода/цифровых чернил	**Нет**	Да	Да	Да	Да
Поддержка сенсорного экрана Windows Tablet PC	**Нет**	Да	Да	Да	Да
Улучшенная поддержка распознавания рукописного ввода Windows Tablet PC	**Нет**	Да	Да	Да	Да
Повышенное удобство использования и навигации Windows Tablet PC	**Нет**	Да	Да	Да	Да
Windows SideShow	**Нет**	Да	Да	Да	Да

Таблица 1.7 *(продолжение)*

Функциональные возможности	**Home Basic**	**Home Premium**	**Business**	**Enterprise**	**Ultimate**
Программа совместной работы Windows	Только просмотр	Да	Да	Да	Да
Улучшенное совместное использование файлов и папок	Да	Да	Да	Да	Да
Синхронизация двух ПК	**Нет**	Да	Да	Да	Да
Сетевое отображение	**Нет**	Да	Да	Да	Да
Настройки отображения	**Нет**	Да	Да	Да	Да
Средство удаленного управления рабочим столом	Только клиент	Только клиент	Клиент и сервер	Клиент и сервер	Клиент и сервер
Присоединение к домену Windows Small Business Server	**Нет**	**Нет**	Да	Да	Да
Присоединение к домену Windows Server	**Нет**	**Нет**	Да	Да	Да
Поддержка групповой политики	**Нет**	**Нет**	Да	Да	Да
Поддержка автономных файлов и папок	**Нет**	**Нет**	Да	Да	Да
Кэширование на стороне клиента	**Нет**	**Нет**	Да	Да	Да
Перемещаемые профили пользователей	**Нет**	**Нет**	Да	Да	Да
Перенаправление папок	**Нет**	**Нет**	Да	Да	Да

Таблица 1.7 *(окончание)*

Функциональные возможности	Home Basic	Home Premium	Business	Enterprise	Ultimate
Централизованное управление питанием при помощи групповой политики	**Нет**	**Нет**	Да	Да	Да
Сервер IIS	**Нет**	**Нет**	Возможно	Возможно	Возможно

Возможно, что не все функции, перечисленные в этом обширном списке, в основе которого информация с сайта Microsoft, вам потребуются. Постепенно, осваивая систему, вы встретитесь с необходимостью применения той или иной функции, и сможете оценить возможности выпуска Windows Vista, установленного на вашем компьютере.

Версии выпусков системы отличаются не только функциональностью, но и вариантом локализации. Windows Vista создана так, что сама операционная система не зависит от языка пользователя. Вся текстовая информация, включая меню, заголовки окон и справку Windows, представлена на языке применяемого пакета локализации. В Россию поставляется преимущественно версия системы, локализованная для России, т. е. русскоязычная. В связи с тем, что законы Соединенных Штатов не позволяют распространять отдельные программы и технологии в другие страны, в локализованной для России версии есть определенные ограничения, например, снижен возможный уровень шифрования информации на дисках, пока не работает система распознавания речи на русском языке. Тем не менее, именно такая версия системы предназначена для продаж в России. При этом цена русской версии несколько ниже, чем цена версии для Соединенных Штатов. Поэтому мы будем рассматривать именно русскую локализацию системы. Только процедура установки будет описана для англоязычной версии, поскольку на момент написания книги автору был доступен такой вариант дистрибутива.

Мы не будем в книге рассматривать интерфейс пользователя Windows Aero с элементами Glass ("стекло"), Windows Flip 3D, масштабируемыми миниатюрами на панели задач, динамическими окнами и более плавным отображением рабочего стола. Если возможности вашего компьютера позволяют его использовать, вы сами увидите его красоту. Полиграфические возможности

книги не позволяют передать изображения этого интерфейса достаточно достоверно. Приведем лишь одно изображение (рис. 1.6) нового интерфейса в момент выбора необходимого из множества открытых окон (используем Windows Flip 3D).

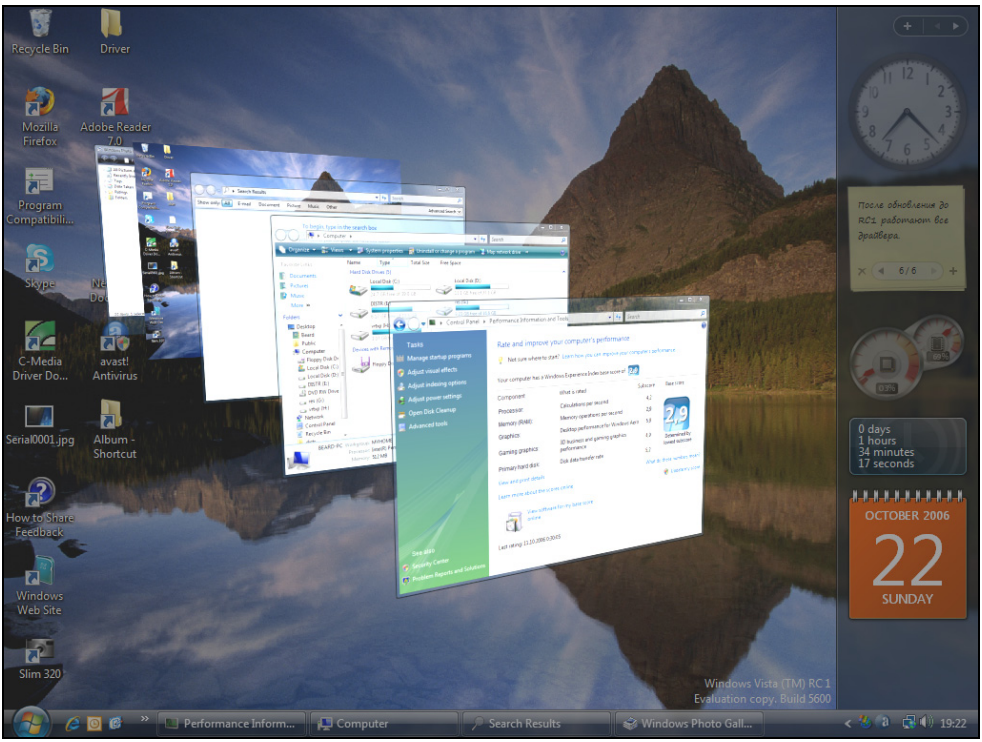


Рис. 1.6. Интерфейс пользователя Windows Aero

Объемный вид полупрозрачных окон позволяет оперативно найти необходимое окно и, переместив его на передний план, развернуть. Этот режим, если установлен интерфейс Windows Aero, доступен при нажатии комбинации клавиш <Win>+<Tab>. Удерживая клавишу <Win> и нажимая клавишу <Tab>, можно перемещать окна в стопке.

Это невольное заглядывание далеко вперед, в тот момент, когда вы уже освоились с системой, потребовалось нам только для того, чтобы вы представляли возможности этого интерфейса. Для большей читаемости иллюстраций мы применим более простой и лаконичный интерфейс.

Но до того как вы увидите какой-либо интерфейс Windows Vista, систему требуется установить. Этим мы сейчас и займемся. Если у вас Windows Vista уже установлена, то ознакомление с этой процедурой вам пригодится в будущем.

Просто вставьте диск

Да, если вы только что приобрели компьютер, то обычно этого достаточно, чтобы началась установка операционной системы. Следует, правда, уточнить, какой диск и куда следует вставлять. Дистрибутив Windows Vista распространяется на DVD-дисках. Диски загрузочные. Следовательно, компьютер должен иметь дисковод, который может читать DVD-диски. Для большинства современных компьютеров это обычная составляющая. Если вы решили использовать старый компьютер, несколько модернизировав его, то обратите внимание на эту деталь. Кроме того, в отдельных случаях, если компьютер не имеет наклейки о совместимости с Vista, может потребоваться обновление BIOS (базовой системы ввода/вывода) для повышения стабильности работы системы. Вот здесь следует быть максимально осторожным. Версию BIOS для обновления всегда можно найти на сайтах производителей материнских плат. Обязательно сохраните резервную копию BIOS вашей старой версии. Если что-нибудь не заладится при установке Vista на ваш не очень новый компьютер, его можно продолжать использовать под управлением Windows XP. Но вероятна такая ситуация, когда Windows XP не будет устанавливаться после обновления BIOS. Причем уже установленная система будет продолжать работать. Если вы не устанавливали Windows Vista, как вторую систему, и Windows XP необходимо установить заново, то придется вернуть BIOS той версии, что была ранее установлена. При этом нужно иметь программу для перезаписи BIOS, которая будет работать с загрузочной дискеты.

Если вы сами не уверены, что сможете произвести процедуры обновления BIOS без ошибок, то лучше доверьте эту работу опытным пользователям ПК, объяснив им для чего это необходимо выполнить. Начинать обновление BIOS есть повод только в том случае, если вы обнаружили, что Windows Vista работает нестабильно, без всякой видимой причины появляется синий экран с указанием на неизвестную ошибку системы, а после перезагрузки в журналах системы не обнаруживается никакой информации о сбое, которая помогла бы выявить его причину. Но будем надеяться, что у вас не возникнет необходимости в таких сложных для начинающих пользователей действиях.

Далее описан процесс установки Windows Vista с универсального дистрибутива, в котором установка проходит на английском языке. Применив дистрибутив, специально локализованный для России, вы увидите процесс установки на русском языке, и практически никаких решений во время установки вам принимать не придется. Если же предполагается использование дистрибутива английской версии, а затем самостоятельная локализация с помощью языкового пакета, то вы встретитесь с процессом установки, описанным далее.

После вставки диска и начала загрузки с него появятся надпись "Windows is loading files..." ("Идет загрузка файлов...") и индикатор выполнения в виде белой полосы.

> ***Примечание***
>
> Требуется нажать любую клавишу для начала загрузки с DVD-диска, если есть другие варианты загрузки, когда на вашем компьютере установлена иная версия операционной системы. Конечно, в BIOS SETUP должна быть задана загрузка с CD или DVD.

Следует просто подождать, пока завершится загрузка файлов, о чем и сообщает надпись на экране.

Если установка не началась

Возможно, что загрузка с вставленного диска не начинается вовсе. В этом случае следует просто поправить установки в BIOS SETUP (настройки BIOS). Для этого в начале загрузки компьютера необходимо нажать клавишу <Del> или <F2>. Это наиболее часто встречающиеся способы входа в BIOS SETUP. После входа в программу настройки BIOS найдите вкладку или раздел **Boot**. В нем, в зависимости от версии BIOS, тем или иным способом должен быть указан порядок загрузки. Это может быть список дисков, в котором можно изменить порядок следования записей, а может быть одно поле, в котором перечислены варианты загрузки одной строкой. В большинстве случаев порядок записей в списке или выбор строки в поле выполняется клавишами <+> или <-> на цифровой части клавиатуры. Обычно, чтобы выбор был возможен, требуется выделить элемент списка или поле, "встав" на него, перемещаясь по экрану с помощью клавиш со стрелками или клавишей <Tab>. Первым в списке или в строке должен быть дисковод компакт-дисков. Он может обозначаться как CD, CD-ROM, CD-ROM Drive. Вероятно, возможны и другие варианты, но всегда понятно, о каком диске идет речь. После уста-

новки правильного порядка загрузки нажмите последовательно клавиши <Esc>, <F10> и <Enter>. Компьютер перезагрузится и, если в дисководе находится установочный диск Windows Vista, попытается с него загрузиться. При исправном дисководе и диске начнется загрузка и установка системы.

Во время установки

Программа установки системы продумана очень хорошо. Возможны два варианта установки системы: установка с нуля или обновление системы, если у вас уже была установлена более ранняя или менее функциональная ее версия. Причем обновление возможно, если запустить программу установки уже из-под загруженной Windows Vista.

Рис. 1.7. Окно **Install Windows**: выбор языковых параметров

Если, загрузившись с DVD-диска, выполнить установку поверх ранее установленной версии Windows Vista, то программа установки сохранит все

документы и файлы ранее установленной системы. Это предотвратит потерю важной для вас информации, если вы забыли сохранить ее на другом носителе.

Установка с чистого листа всегда более надежна. В систему не смогут проникнуть ошибки из ранее установленной системы, но программы, которые были установлены, придется инсталлировать снова. Мы предполагаем, что на вашем компьютере Windows Vista еще не устанавливалась, соответственно установка проводится с нуля на новый винчестер.

После загрузки файлов начнет работу программа установки.

На этом этапе (рис. 1.7) следует выбрать языковые параметры системы. Если вы живете в России, то выбирайте формат времени и чисел (**Time and currency format**) **Russian** и параметры клавиатуры или метод ввода (**Keyboard or input method**) **Russian**.

Рис. 1.8. Окно **Install Windows**: начало установки

После нажатия кнопки **Install now** (Установить сейчас) начнется собственно установка системы (рис. 1.8).

Для того чтобы была возможна активация системы после установки, необходимо ввести ключ продукта (Product key) (дефисы при вводе ключа подставляются автоматически). Если вы не уверены в необходимости автоматической активации системы после установки, снимите флажок (рис. 1.9) **Automatically activate Windows when I'm online** (Автоматически активировать Windows, когда я подключен к Интернету). Дело в том, что число активаций ограничено, и если вам не понравится работа системы на данном компьютере, вы сможете ее переустановить на другую машину. Для оценки необходимости переустановки или активации у вас будет 30 дней.

Для удобства ввода ключа продукта предусмотрена экранная клавиатура (рис. 1.10).

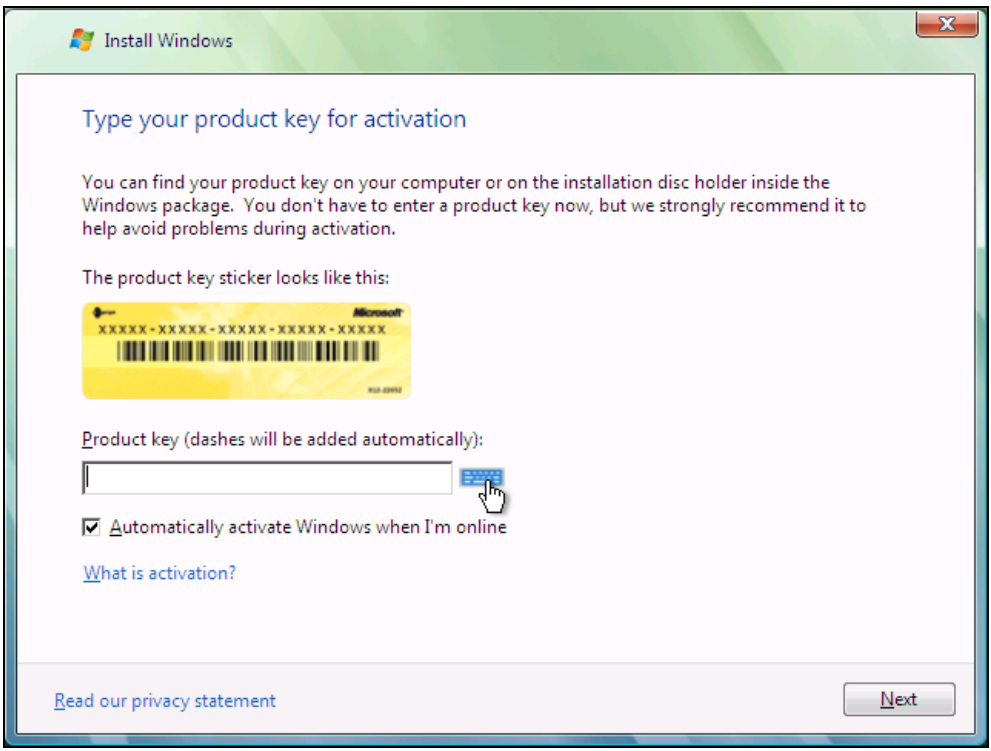


Рис. 1.9. Окно **Install Windows**: ввод ключа продукта

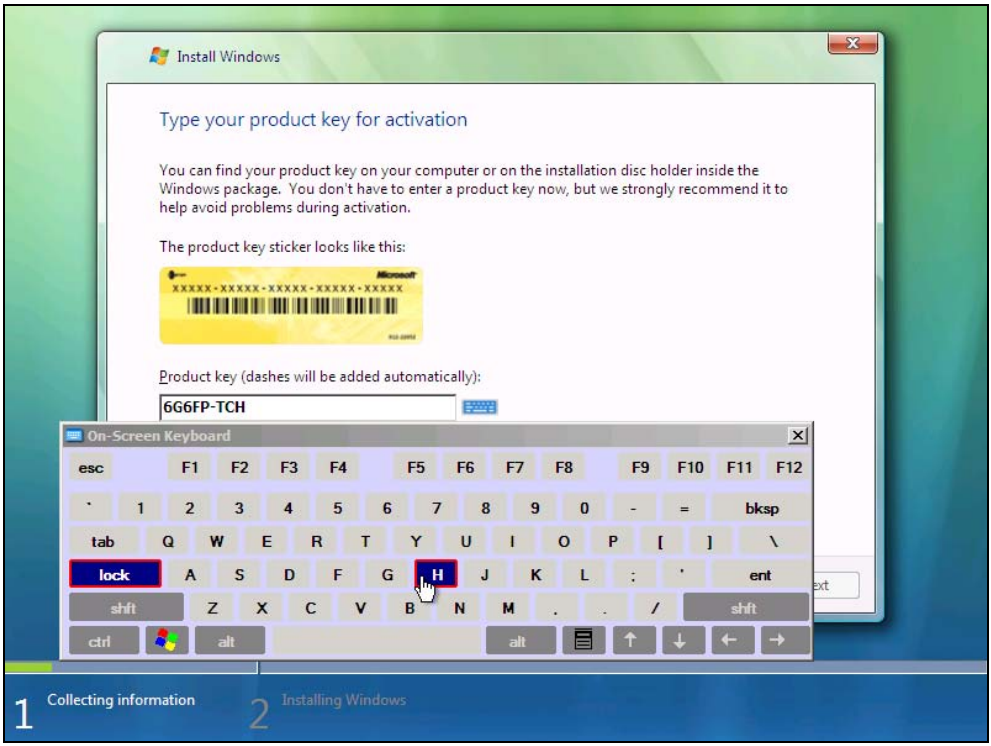


Рис. 1.10. Окно **Install Windows** и экранная клавиатура

Если вы не введете ключ продукта, то программа установки попросит вас подтвердить, что вы согласны переустановить систему после приобретения. Но взамен вы получите возможность ознакомиться с любой версией системы. Дистрибутив содержит все версии, и вы сможете выбрать интересующую вас для ознакомления. Период ознакомления, конечно, 30 дней. Возможность ознакомиться с любой версией Windows Vista может быть полезной для принятия решения о необходимости приобретения более полнофункциональной версии, чем вы уже имеете.

После ввода ключа продукта программа установки предложит прочитать и принять лицензионное соглашение. В следующем окне вы будете предупреждены, что при желании обновить систему вы должны начать установку из-под Windows. После выбора продолжения установки потребуется указать диск, на который будет установлена система.

Если жесткий диск был отформатирован заранее, то начнется копирование файлов, в противном случае диск будет подготовлен и отформатирован перед началом копирования файлов, но процесс будет идти скрыто от вас.

Все дальнейшие действия программа выполнит самостоятельно, информируя вас о состоянии процесса установки выделением строк с описанием текущего процесса установки и отображая индикатор выполнения установки в нижней части экрана (рис. 1.11).

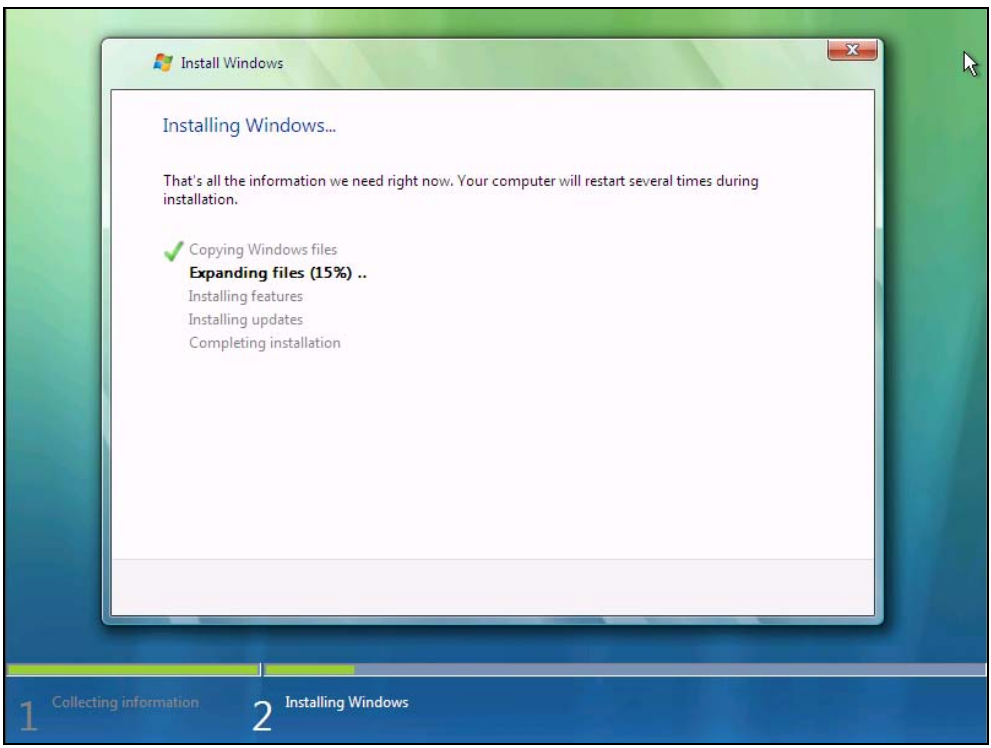


Рис. 1.11. Окно **Install Windows** и отображение хода установки Windows

Установка может продлиться довольно долго. Если есть подключение к Интернету, которое система сможет использовать в процессе установки, то автоматически будут установлены и самые необходимые обновления.

После завершения установки компьютер будет автоматически перезагружен.

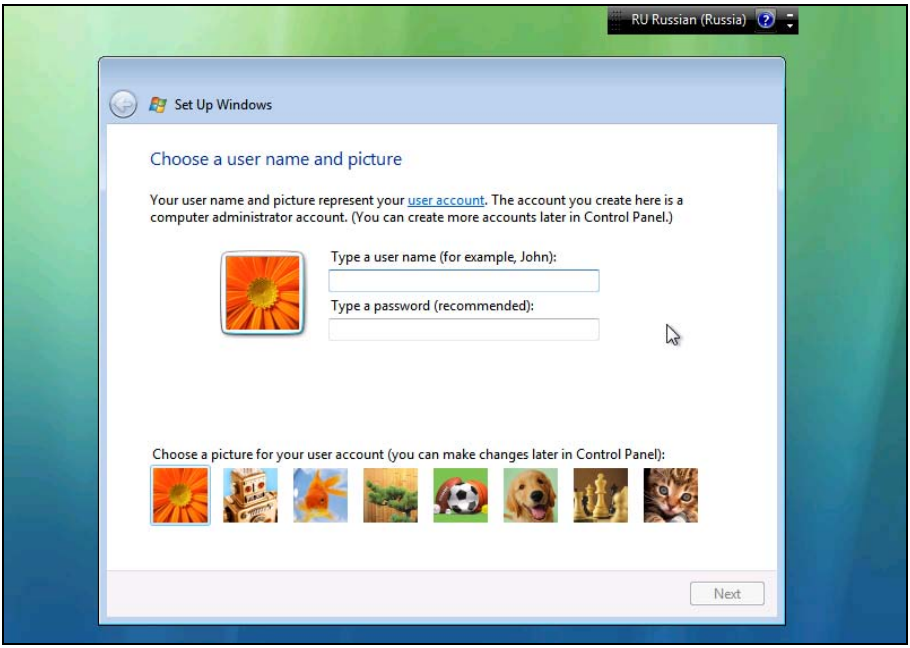


Рис. 1.12. Окно **Set Up Windows**: выбор имени пользователя и пиктограммы

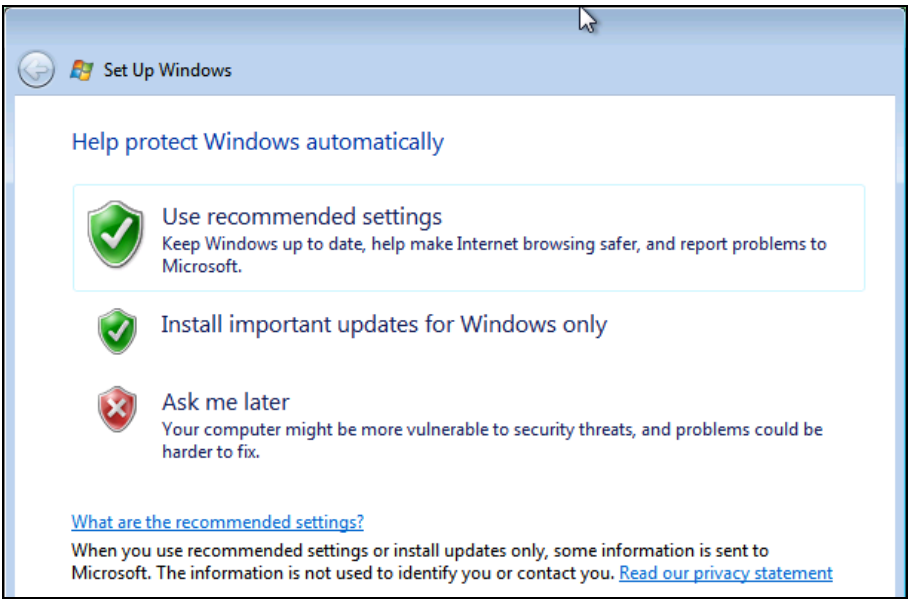


Рис. 1.13. Окно **Set Up Windows**: настройка защиты Windows

Теперь останется выбрать имя пользователя, ввести придуманный для него пароль и выбрать пиктограмму (рис. 1.12). Для ввода имени и пароля латиницей достаточно нажать комбинацию клавиш <Alt>+<Shift>.

Нажав кнопку **Next**, мы попадем в окно настройки защиты Windows (рис. 1.13). Для начинающих лучше выбрать вариант, предложенный системой — **Use recommended setting** (Использовать рекомендуемые установки).

До полного завершения установки остается совсем немного. В следующем окне (рис. 1.14) устанавливаем правильные значения даты, времени и часовой пояс.

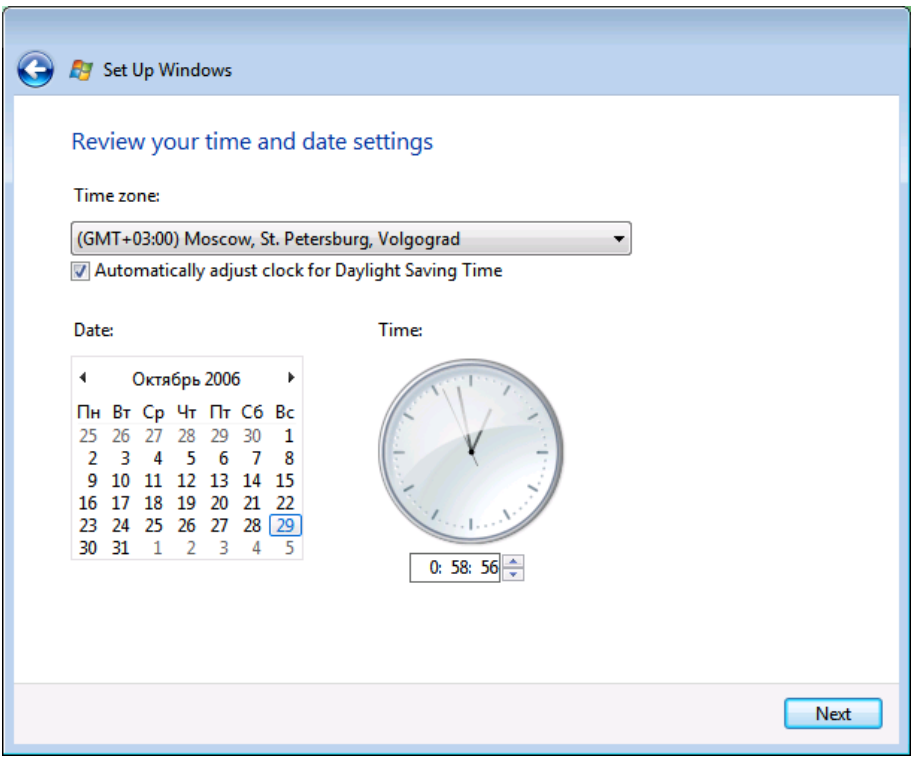


Рис. 1.14. Окно **Set Up Windows**: проверка установки даты и времени

В разделе **Select your computer's current location** (Выбор расположения вашего компьютера) окна **Set Up Windows** (Установка Windows) следует указать, в какой сети находится компьютер. Это окно появится только в том случае, если компьютер действительно подключен к сети. Скорее всего, ваш

компьютер находится в домашней сети, это и выберем. И, наконец, долгожданный раздел **Thank you** (Спасибо) после полного завершения установки (рис. 1.16).

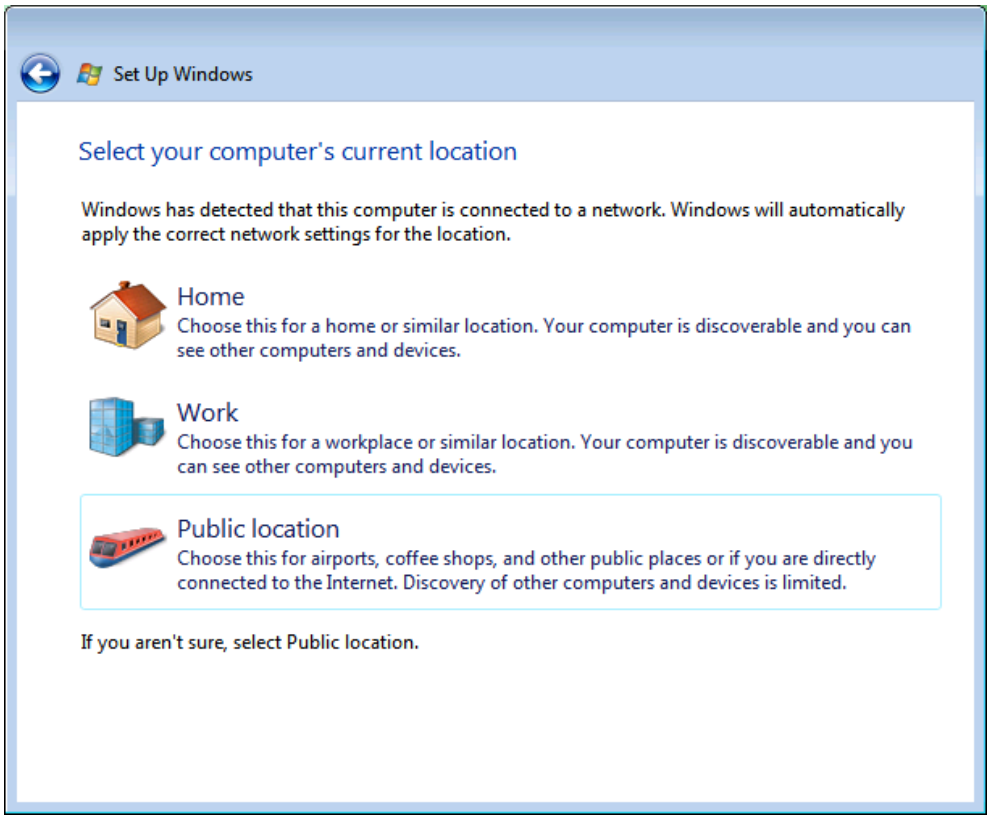


Рис. 1.15. Окно **Set Up Windows**: выбор расположения вашего компьютера

Осталось нажать кнопку **Start** (Пуск) для первой загрузки установленной системы.

Весь процесс установки у вас может занять от часа до трех часов (зависит от параметров компьютера). Но после загрузки системы при наличии подключения к Интернету тут же будет предложено загрузить и установить последние обновления. Для Windows обновления никогда не были лишними. Если подключение к Интернету позволяет загрузить предложенный объем информации, то согласитесь и обновите систему.

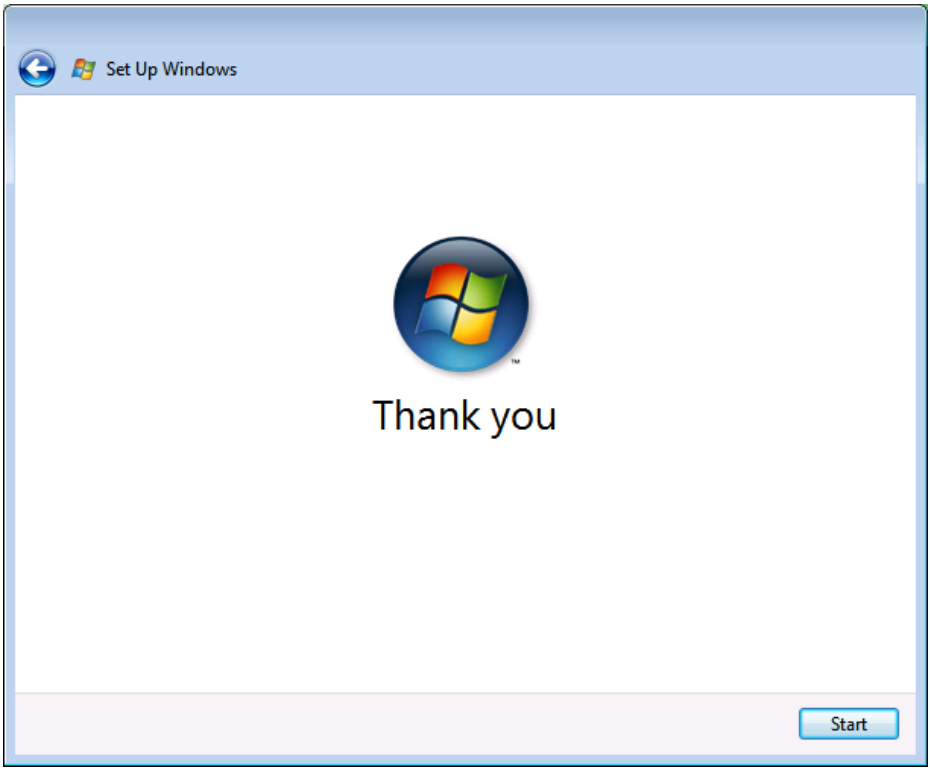


Рис. 1.16. Окно **Set Up Windows**, раздел **Thank you**

Если подключение к Интернету не настроено, вы можете выполнить обновления позднее, отказавшись пока от их загрузки. На экране появится окно центра настройки компьютера. Но это уже не установка системы, а начало работы в ней. О работе в установленной системе поговорим в следующих главах. Да и я, пожалуй, переберусь с виртуального компьютера на реальный. А пока я меняю компьютер, полюбуйтесь красотами интерфейса Windows Vista. Ведь все следующие главы будут содержать иллюстрации, снятые с более аскетичного интерфейса, на который и вам, видимо, придется временно перейти. Немного освоившись в системе, вы можете снова переключиться на понравившийся вам вариант интерфейса, но в книге о нем мы говорить не будем.

Единственное, о чем еще следует сказать, — это о локализации.

Для локализации английской версии системы для России требуется языковый пакет.

После установки системы следует в **Control Panel** (Панель управления) найти апплет **Regional and Language Options** (Язык и региональные стандарты). В нем на вкладке **Keyboard and Languages** (Языки клавиатуры) найти кнопку **Install/Uninstall Languages** (Установить или удалить язык). Далее потребуется только указать расположение пакета русификации и подождать завершения его установки.

После перезагрузки в поле **Choose Display Language** на вкладке **Keyboard and Languages** (Языки клавиатуры) следует выбрать язык **русский**. Теперь достаточно выйти и снова войти в систему, и язык системы будет изменен.

Если вы использовали русскую версию дистрибутива, то изменить язык системы на английский, вероятнее всего, не получится. Языковый пакет для английского языка по информации, предоставленной сотрудниками Microsoft, не существует. Он просто сразу встроен в английскую версию.

Далее в книге будет рассматриваться только русская версия Windows Vista.

Настройка рабочих станций для работы в сети

Пожалуй, вся предыдущая информация была лишь прелюдией к описанию самых важных в нашем случае настроек. Следует, правда, помнить, что настройки, которые будут сейчас описаны, лишь предварительные. Множество вариантов режимов работы компьютера в сети требует 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. Более того, суть производимых действий одна и та же, независимо от применяемой операционной системы. Поняв принцип работы компьютера в сети на примере одной-двух операционных систем, вы будете в состоянии настроить машину под управлением любой ОС.

Что же необходимо выполнить для того, чтобы Windows Vista заработала в вашей сети?

> ***Примечание***
>
> Описание настроек приведено для классического интерфейса Windows. Если вы не знаете, как привести вашу систему к такому интерфейсу, воспользуйтесь встроенной справкой.

1. Подключите компьютер к сети.

2. Нажмите кнопку **Пуск**.
3. Выберите **Настройка | Панель управления**.
4. В открывшемся окне **Панель управления** (рис. 1.17) найдите значок **Центр управления сетями и общим доступом** (на рисунке нижний ряд в центре).

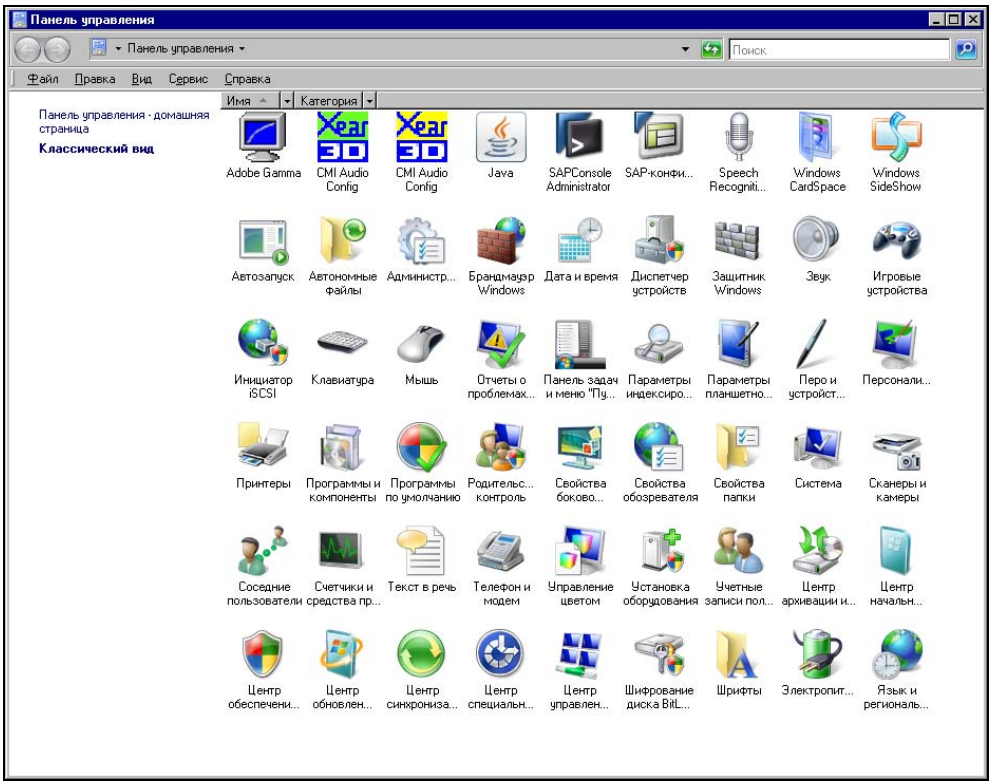


Рис. 1.17. Окно **Панель управления**

5. Двойным щелчком (если у вас не настроено иное поведение мыши) по этому значку откройте одноименное окно (рис. 1.18).
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**.

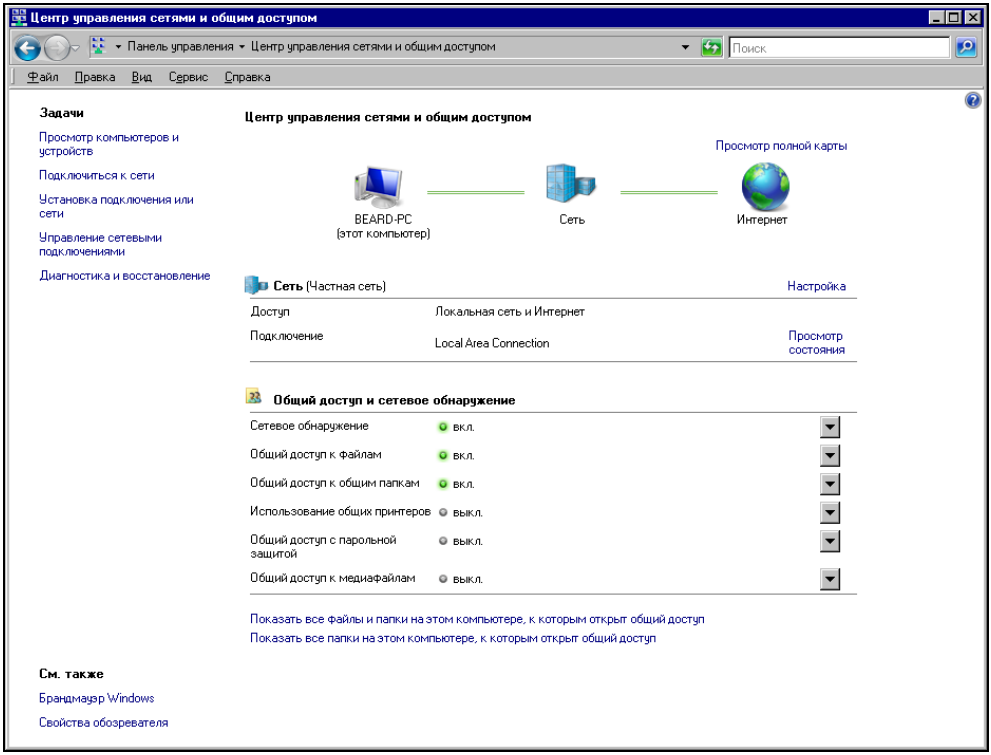


Рис. 1.18. Окно **Центр управления сетями и общим доступом**

7. В открывшемся окне **Сетевые подключения** (рис. 1.19) 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. 1.20) 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** в выпадающем списке **Поставщик службы имен** выберите **Локатор Windows** (рис. 1.21).

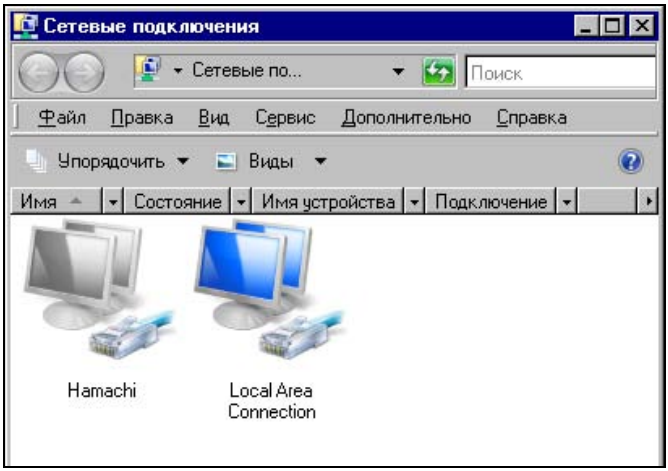


Рис. 1.19. Окно **Сетевые подключения**

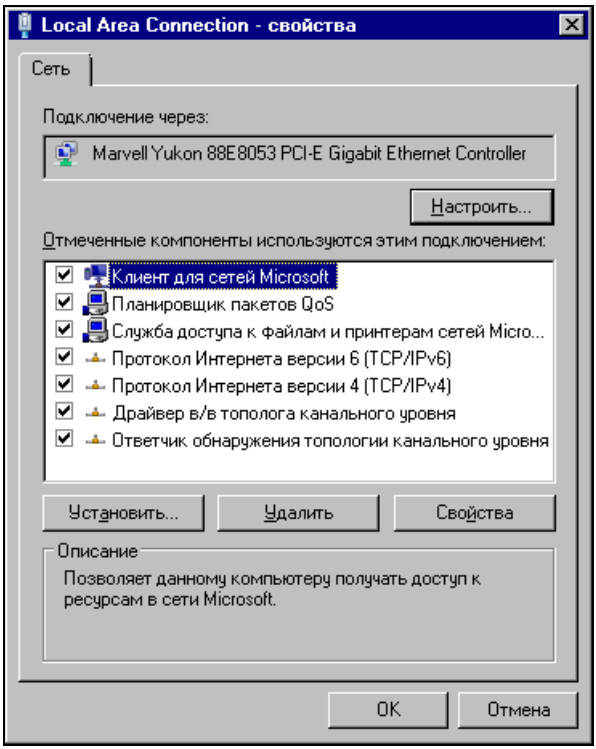


Рис. 1.20. Окно **Local Area Connection - свойства**

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.

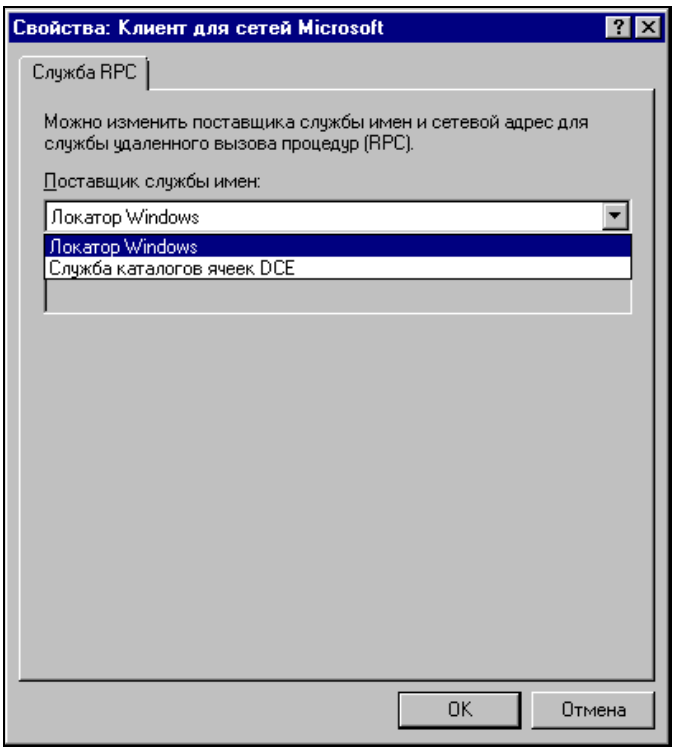


Рис. 1.21. Окно **Свойства: Клиент для сетей Microsoft**

10. Если вы не видите у себя компонент **Служба доступа к файлам и принтерам сетей Microsoft**, 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)**. Нажмите кнопку **Свойства**.

На рис. 1.22 приведены параметры настройки для конкретной сети, в которой работает мой компьютер. Ваши настройки могут быть иными. 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 ад-

реса 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 "C" (с 192.168.0.0 по 192.168.255.0) или из диапазона зарезервированных адресов сетей класса "A" кроме адресов с 127.0.0.0 по 127.255.255.255. При этом маска подсети назначается в зависимости от числа компьютеров и других узлов в вашей сети.

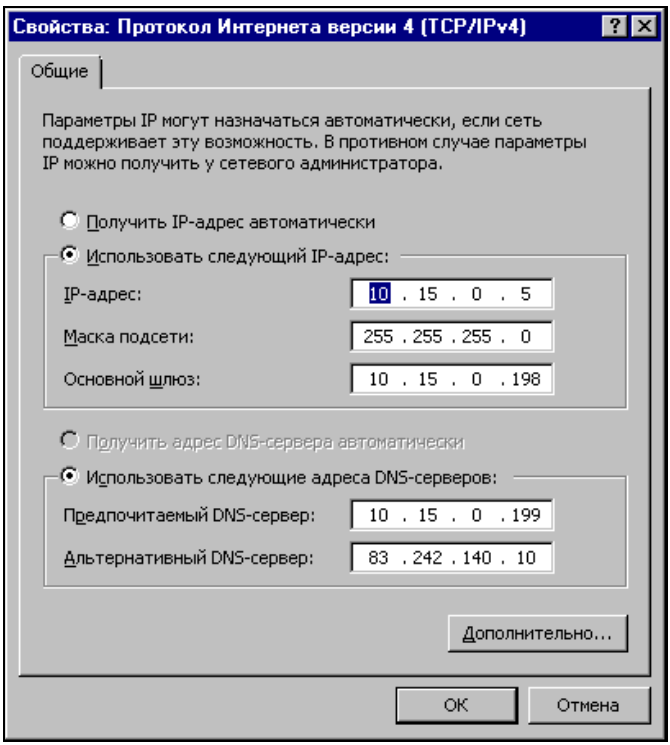


Рис. 1.22. Окно **Свойства: Протокол Интернета версии 4 (TCP/IPv4)**

Предположим, что вы планируете приобрести пять компьютеров для всех членов семьи. Сами 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 табл. 1.5, можно найти маску

255.255.255.240/28, применив которую, можно создать 16 подсетей с 16 адресами в каждой. Если вы выбрали сеть класса "C", 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 "A" 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 октетах 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-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 ранее ADSL-модем, например.

Linux

В последнее время интерес к Linux у пользователей ПК растет. 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 могут содержаться более совершенные драйверы устройств и некоторые дополнительные возможности, такие как бесплатная поддержка от разработчиков, например.

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.

Установка и первоначальная настройка

В качестве примера для установки Linux рассмотрим одну из новейших версий Mandriva Linux 2008. Начинается установка Linux, как и установка Windows, со вставки диска с дистрибутивом в дисковод и загрузки с него компьютера.

По умолчанию установка проходит в графическом режиме. Экран программы установки в левой части содержит перечень пунктов установки, по мере выполнения которой отображаются экраны, в которых можно выбрать необходимые опции. Первый экран, который представлен на рис. 1.23, — **Language choice** (Выбор языка). Дистрибутивы Linux в отличие от Windows обычно содержат в себе сразу множество системных языков. Независимо от языка, на котором вы говорите, дистрибутив системы один, и нет необходимости скачивать дополнительные языковые пакеты. Выбираем из списка необходимый язык (в данном случае русский) и нажимаем кнопку **Next** (Далее). Теперь все диалоги с пользователем программа установки будет вести на понятном ему языке.

На следующем экране (рис. 1.24) вы сможете прочитать лицензионное соглашение, которое следует принять после прочтения, отметив соответствующую опцию. Если мы согласны с лицензией и хотим продолжить установку системы, нажимаем кнопку **Далее**.

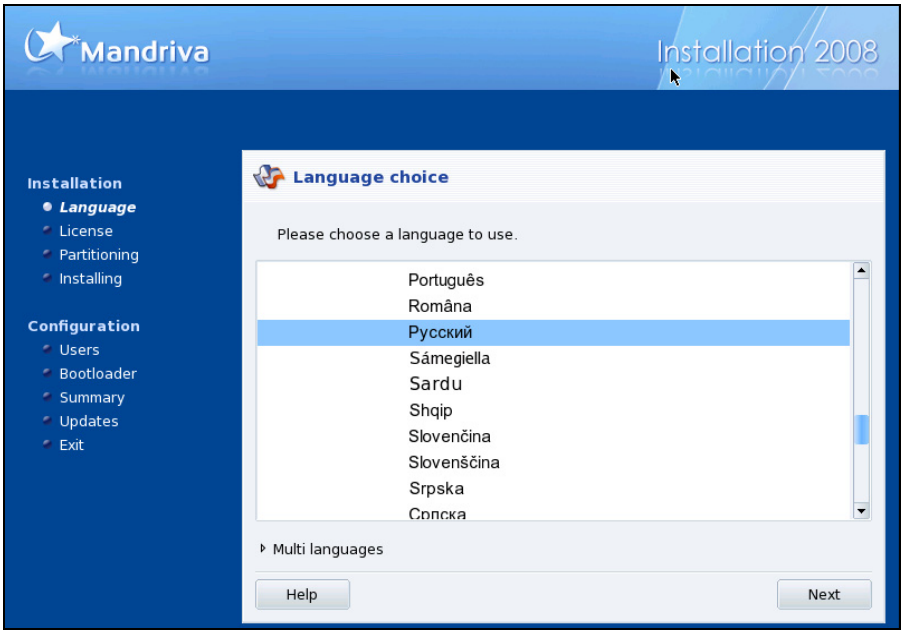


Рис. 1.23. Установка Linux, экран **Language choice**

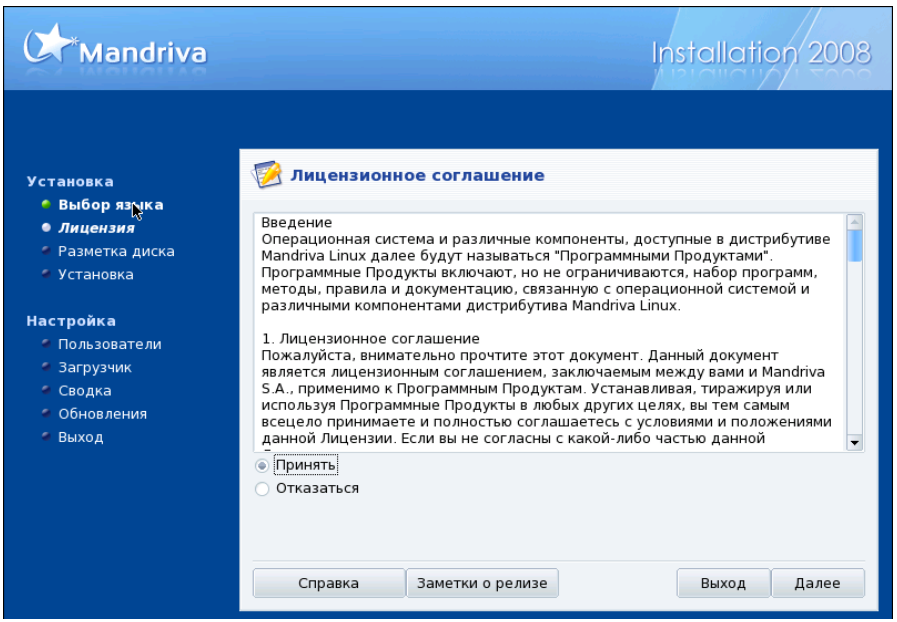


Рис. 1.24. Установка Linux, экран **Лицензионное соглашение**

В зависимости от аппаратной конфигурации вашего компьютера программа установки может задавать вопросы, которые могут показаться неожиданными. Рассматриваемый нами дистрибутив не содержит в себе некоторых драйверов контроллеров жестких дисков. Определив, что на диск с интерфейсом SCSI, установленный в данном компьютере, установку выполнить невозможно, программа в окне **Поиск жесткого диска** просит предложить ей другой диск (рис. 1.25).

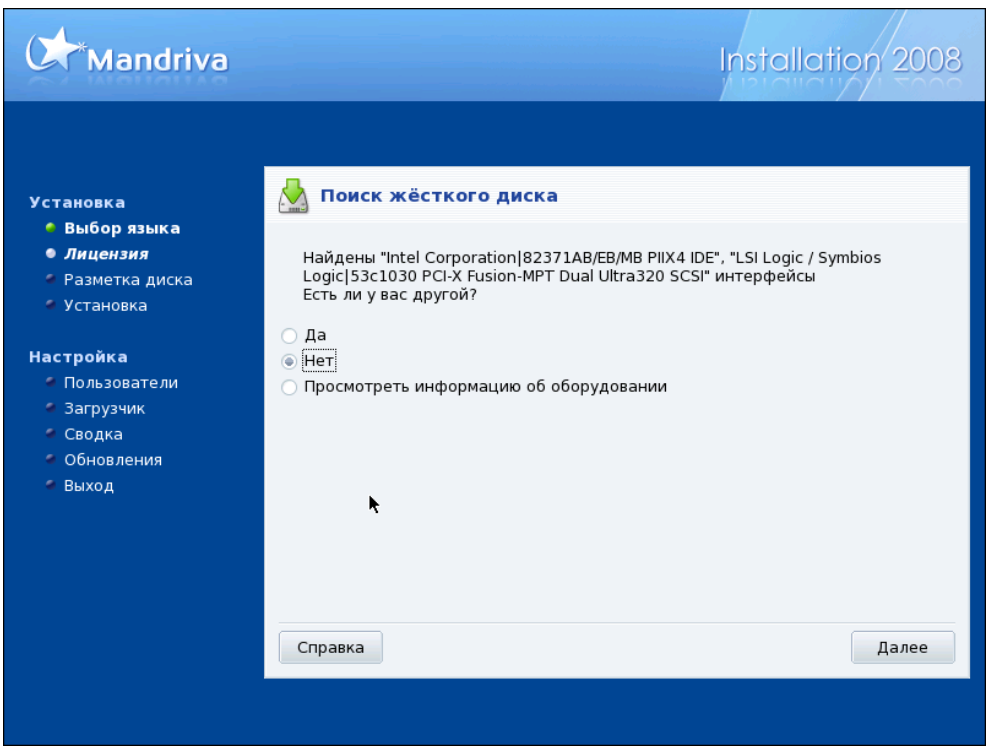


Рис. 1.25. Установка Linux, экран **Поиск жесткого диска**

На компьютере, на который производилась установка, другого диска не было. Пришлось прекратить установку, установить обычный винчестер и начать процедуру заново. Скорее всего, вы не столкнетесь с такой ситуацией, поскольку практически все диски, которые устанавливаются в современные компьютеры, поддерживаются программой установки. А рассматриваемая ситуация создана намеренно, чтобы показать, как программа установки реагирует на нештатные ситуации. Далее рассматривается обычный ход уста-

новки системы. Если установка уже была запущена, но система не установилась окончательно по каким-либо причинам, вы можете увидеть экран с меню выбора дальнейших действий пользователя (рис. 1.26). Программа установки считает, что система уже установлена, и предлагает выбрать дальнейшее действие. В случае проблем с загрузкой уже установленной операционки, например, возможен запуск аварийной системы для поиска и устранения проблем.

Рис. 1.26. Установка Linux, экран выбора действий пользователем

Нас интересует установка системы, поэтому мы выбираем пункт **Install Mandriva Linux 2008 on your system** (Установка Mandriva Linux 2008 на вашу систему). На следующем экране вы увидите отображение процесса загрузки программы установки в оперативную память компьютера (рис. 1.27). Жесткий диск при этом доступен для любых преобразований, на нем в процессе установки не сохраняются никакие компоненты программы установки.

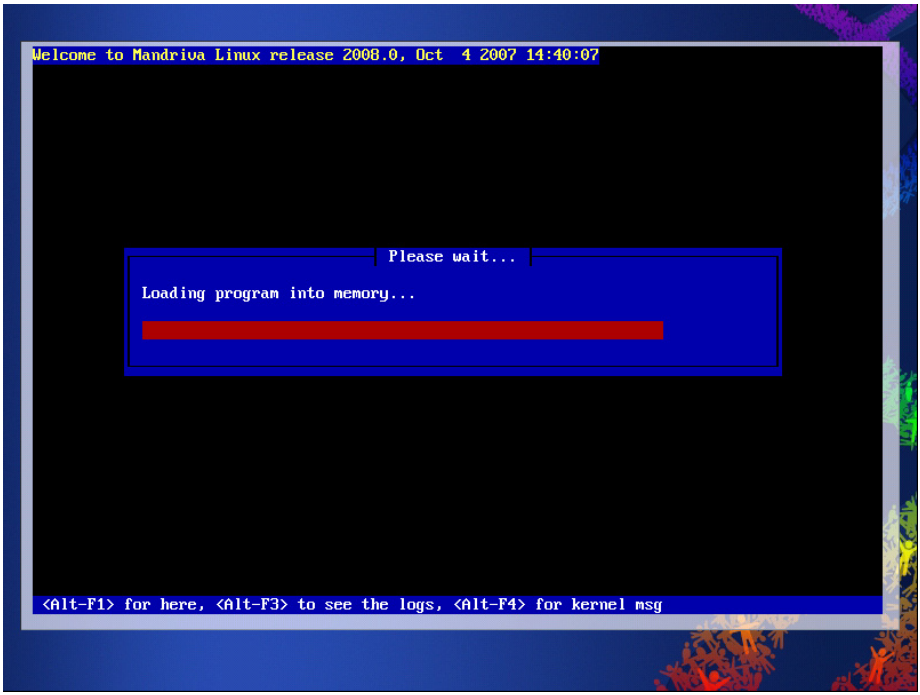


Рис. 1.27. Установка Linux,
экран загрузки программы установки в оперативную память

Винчестер у нас теперь вполне подходящий для установки системы, поэтому после выбора языка установки и принятия лицензии программа попросит нас выбрать раскладку клавиатуры (рис. 1.28). Обратите внимание, что это не язык ввода, а раскладка, расположение символов на клавиатуре. В Linux предусмотрена возможность применения клавиатур с множеством раскладок. Этот список можно развернуть, щелкнув по стрелке пункта **Больше**, но для большинства читателей этой книги достаточно того короткого списка, который открыт по умолчанию.

Выбрав желаемую раскладку, нажимаем кнопку **Далее**. Теперь можно определиться с удобным сочетанием клавиш для переключения между раскладками (рис. 1.29). Это необходимо для изменения языка ввода. Латинская раскладка всегда присутствует по умолчанию, именно она используется для ввода латиницы и англоязычных символов. Рекомендовать какое-либо сочетание не имеет смысла, каждый может выбрать наиболее удобный вариант самостоятельно. Тем более что изменить эту настройку можно и после установки системы.

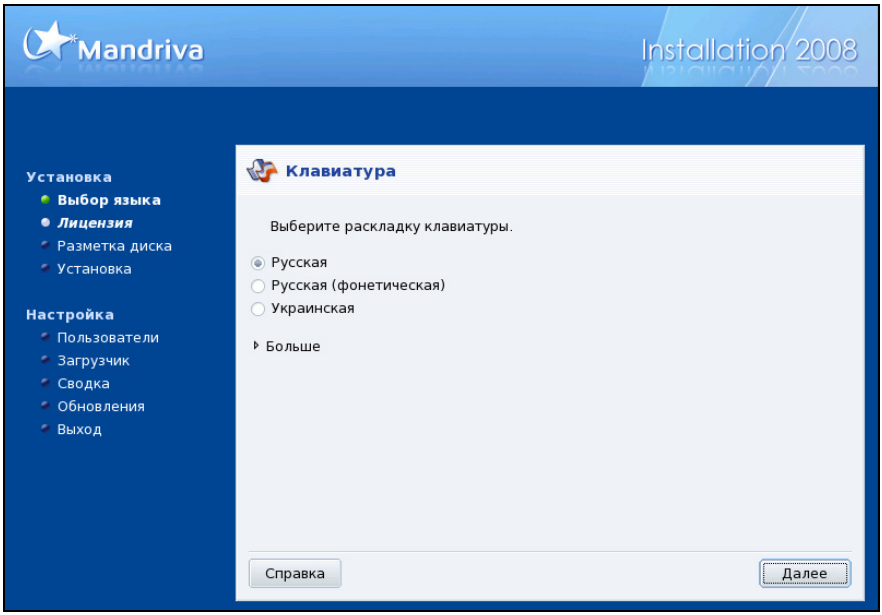


Рис. 1.28. Установка Linux, экран **Клавиатура** (выбор раскладки клавиатуры)

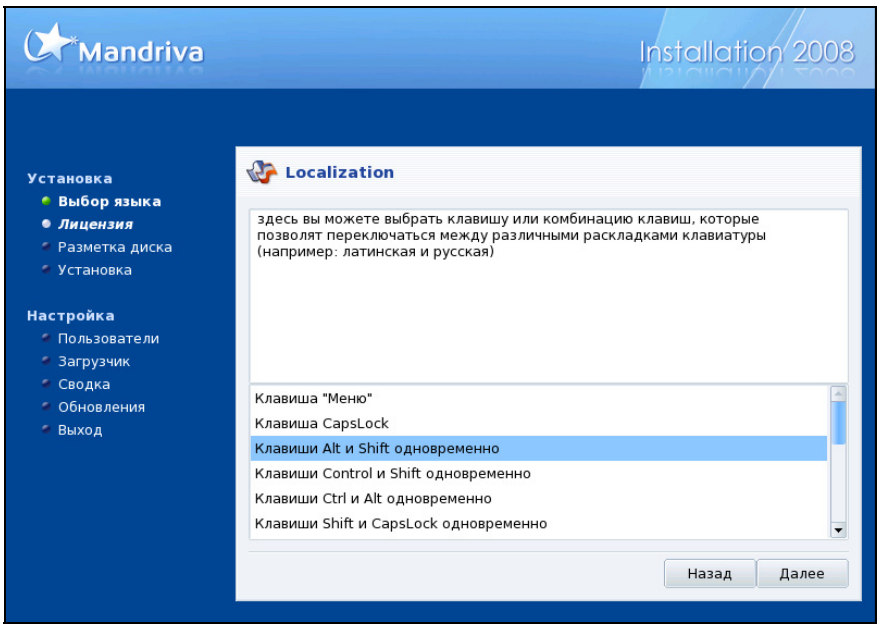


Рис. 1.29. Установка Linux, экран **Localizacion**

Любая операционная система для установки требует определенным образом подготовить диск. Устанавливая Linux, вы можете выполнить разметку диска самостоятельно или поручить это программе установки (рис. 1.30). Второй вариант предпочтительнее в подавляющем большинстве случаев. Даже если на вашем диске уже установлена другая операционная система, но есть свободное место, Linux установится на него. Обе системы при этом будут работоспособны, и вы сможете выбрать загрузку той, которая вам потребуется.

Некоторое время потребуется на форматирование созданных разделов на жестком диске (рис. 1.31).

Далее начинается собственно установка операционной системы. Дистрибутив Linux может содержать в своем составе несколько интерфейсов пользователя (рис. 1.32). В данном случае предлагается выбрать один из двух наиболее популярных. Возможно, что опытные пользователи Linux не согласятся со мной, но, на мой взгляд, есть смысл выбрать GNOME Desktop. Этот интерфейс несколько проще, чем KDE, ориентироваться в нем будет легче. Функциональность же системы от интерфейса не зависит. Программы, которые разрабатывались для KDE, вполне смогут работать и в среде GNOME.

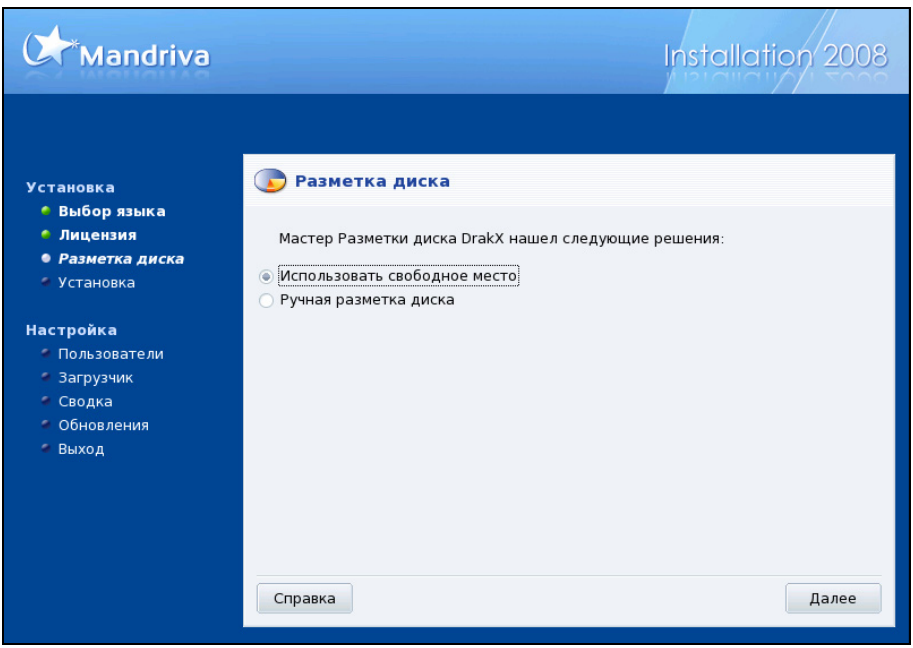


Рис. 1.30. Установка Linux, экран **Разметка диска**

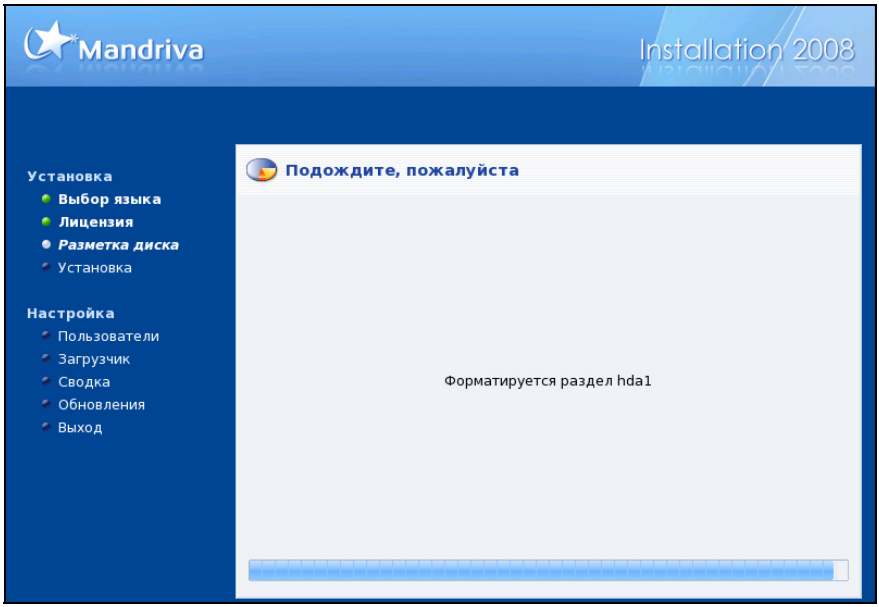


Рис. 1.31. Установка Linux, экран форматирования диска

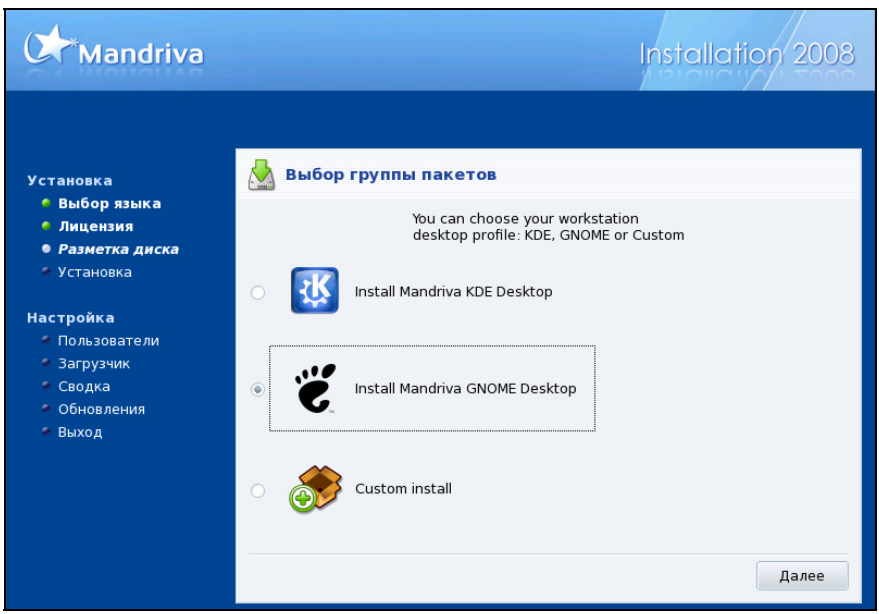


Рис. 1.32. Установка Linux, экран **Выбор группы пакетов**

Рис. 1.33. Установка Linux, экран с индикатором хода установки

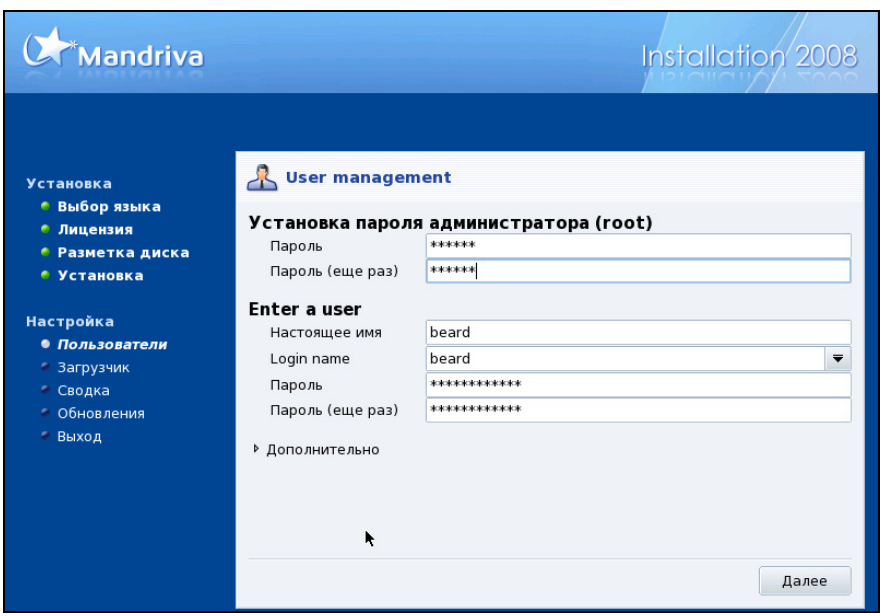


Рис. 1.34. Установка Linux,
экран **User management** управления учетными записями пользователей

Установка может занять продолжительное время (рис. 1.33). На компьютере автора потребовалось более часа самостоятельной работы программы. Перед завершением установки потребуется информация об учетной записи пользователя и пароль администратора системы, который в Linux имеет имя root (рис. 1.34). Под учетной записью этого пользователя обычно работать нельзя, но при выполнении операций, которые связаны с риском для "здоровья" системы, необходимо вводить пароль администратора.

После внесения сведений об учетных данных пользователей останется выбрать тип монитора и указать его основное разрешение. Если вы не знаете тип своего монитора или предполагаете использовать другой после установки системы, то можно выбрать **Обычный** монитор и параметры, с которыми могут работать любые современные мониторы, например, как на рис. 1.35, **1024×768 @ 60 Hz**.

Можно было бы на этом завершить настройки и насладиться первой загрузкой Linux Mandriva, но программа установки предоставляет возможность выполнить еще несколько настроек (рис. 1.36). Можно воспользоваться этим предложением и сразу настроить сеть и Интернет. Для этого, конечно, следует знать параметры сети и подключения к Интернету.

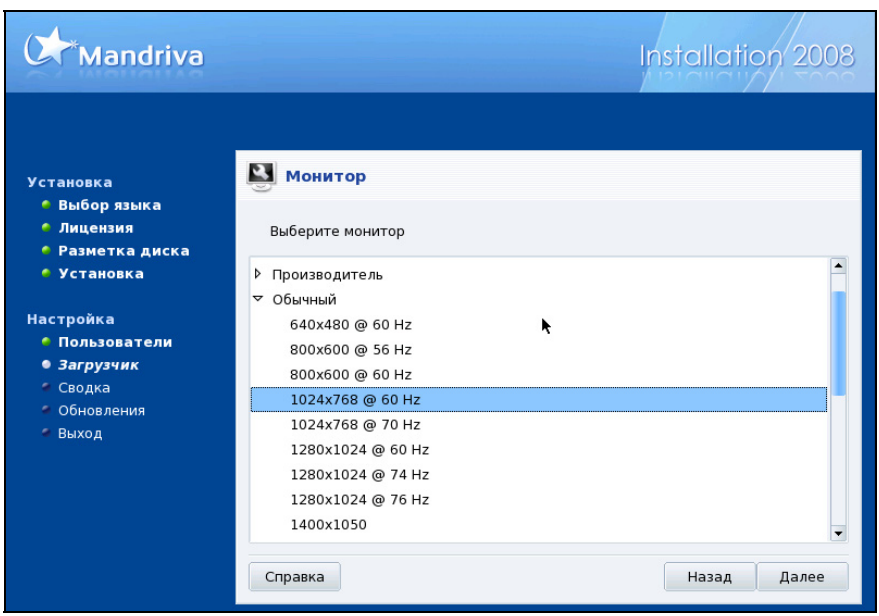


Рис. 1.35. Установка Linux, экран **Монитор**

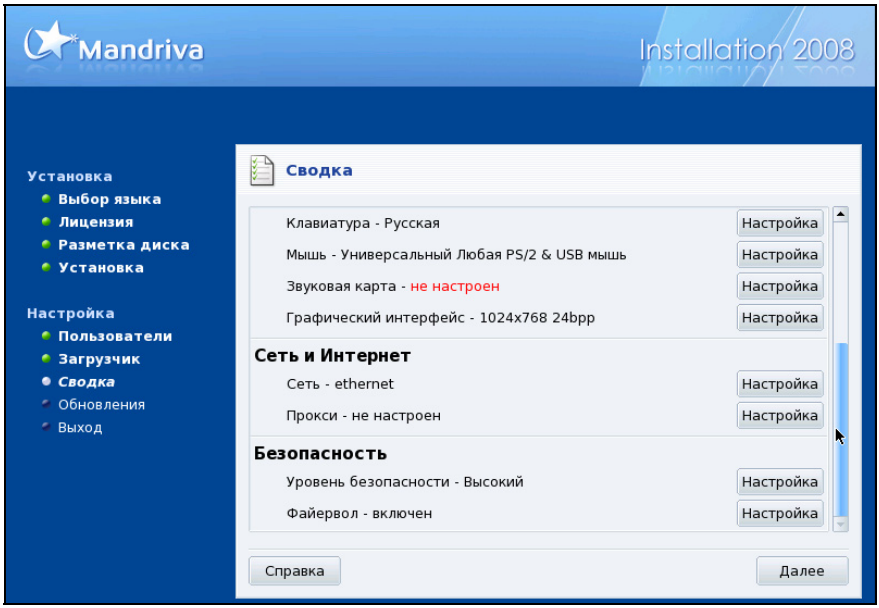


Рис. 1.36. Установка Linux, экран **Сводка**

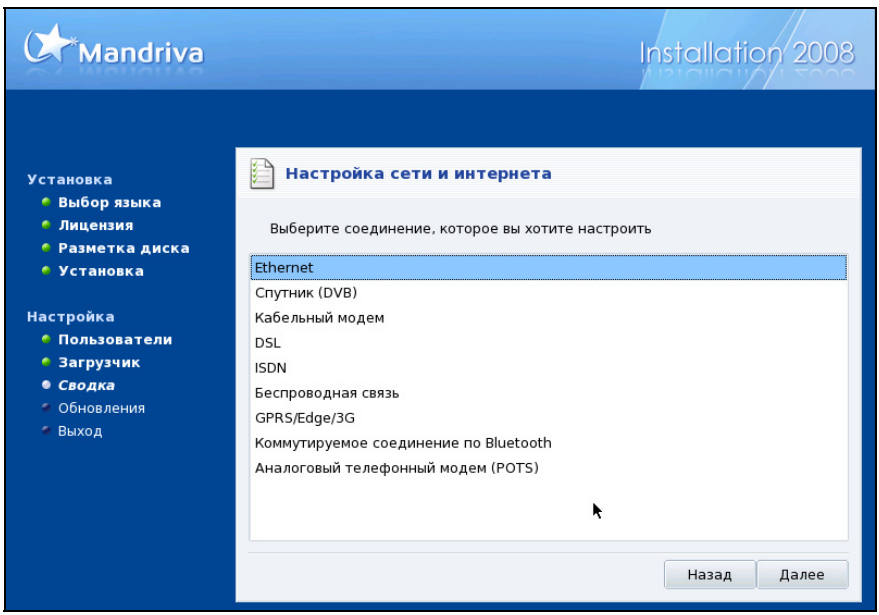


Рис. 1.37. Установка Linux, экран **Настройка сети и интернета** (выбор соединения)

В данном примере предполагается, что уже существует локальная сеть Ethernet со шлюзом в Интернет. Нажимаем кнопку **Настройка**, на следующем экране (рис. 1.37) выбираем Ethernet, нажимаем кнопку **Далее**, и на появившемся экране (рис. 1.38) выбираем ручную настройку, нажимаем кнопку **Далее** и вводим необходимые параметры сети и локального компьютера на экране (рис. 1.39).

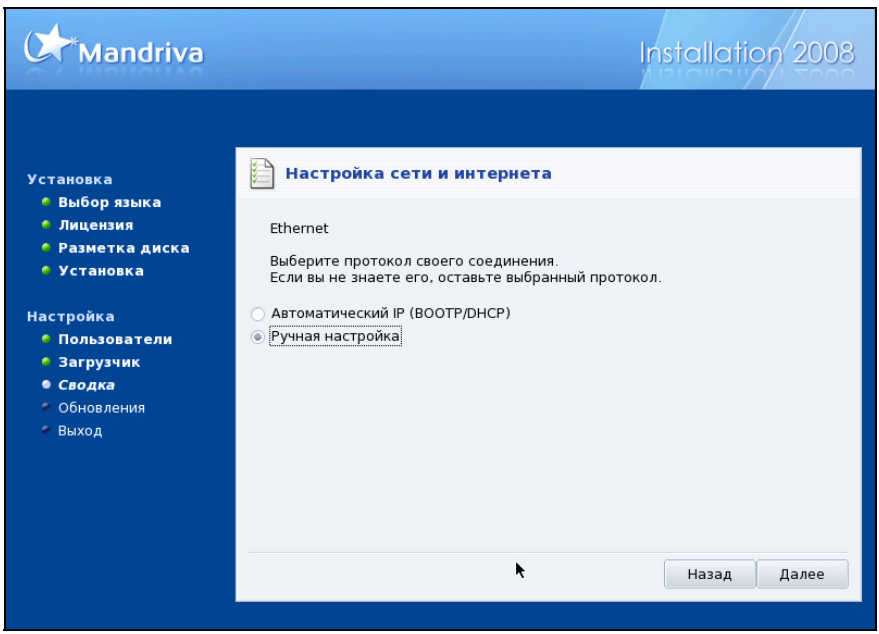


Рис. 1.38. Установка Linux, экран **Настройка сети и интернета** (Ethernet)

По завершении настроек программа установки предложит загрузить обновленные пакеты системы и программ (рис. 1.40). Автор рекомендует отложить обновление до момента, когда система загрузится после установки. Средства Linux позволяют в этом случае выбрать необходимые пакеты. Обновление в процессе установки тоже может быть выборочным, но выбрать нужные для обновления пакеты начинающему пользователю Linux будет непросто.

Позднее мы рассмотрим работу в Mandriva Linux, а пока обратимся к настройке рабочей станции под управлением другой версии Linux — ASPLinux для работы в сети. Ознакомившись с несколькими версиями Linux, вы поймете, что работать можно в любой из них одинаково комфортно.

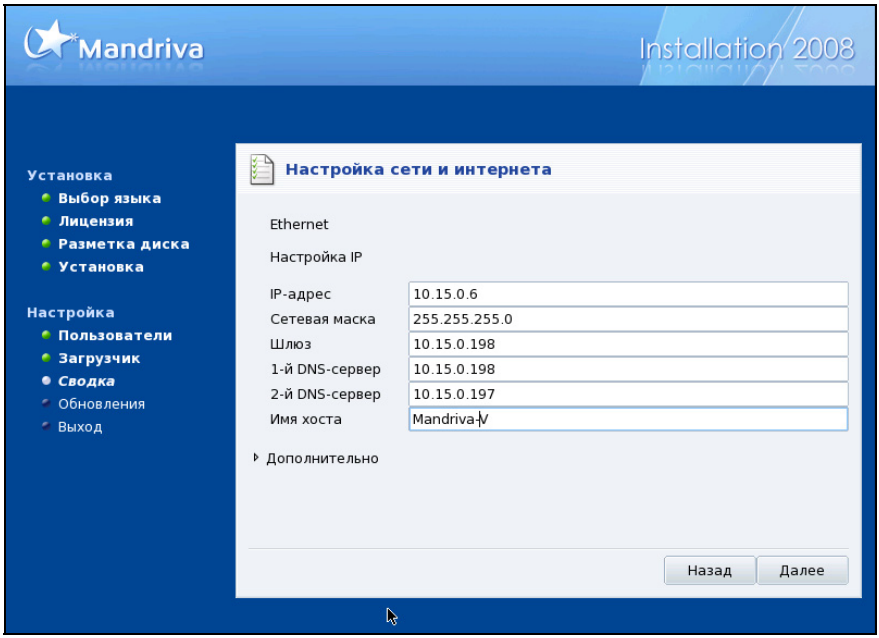


Рис. 1.39. Установка Linux, экран **Настройка сети и интернета** (Ethernet, настройка IP)

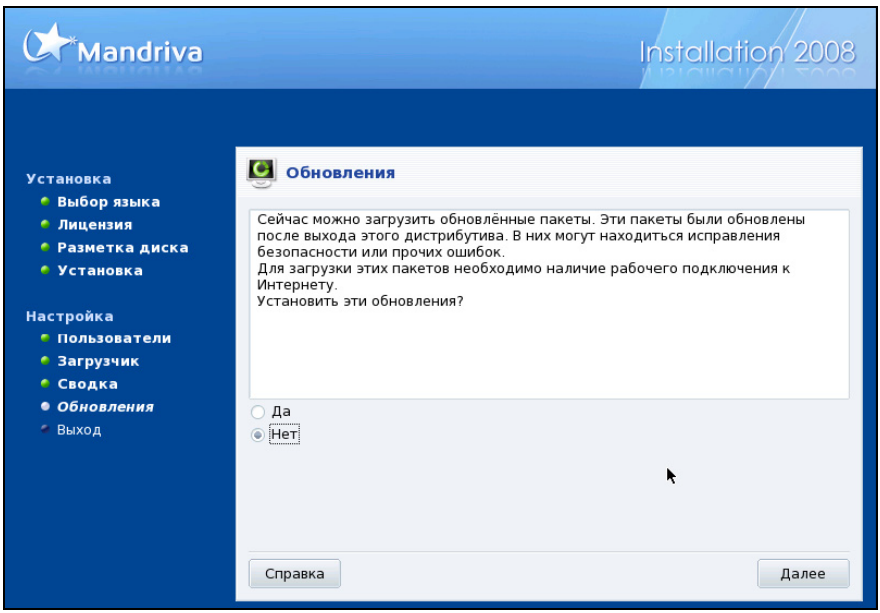


Рис. 1.40. Установка Linux, экран **Обновления**

Настройка рабочих станций

Версий Linux больше, чем версий Windows. Каждая из них обладает определенными преимуществами или недостатками по сравнению с другими. Каждый пользователь может выбрать наиболее подходящую для него версию, установить ее в необходимой конфигурации. Если Windows в серверной редакции и в редакции для рабочей станции — это разные дистрибутивы, то в Linux это может быть один дистрибутив, а как вы его будете устанавливать — это ваше дело. Вот и ASPLinux можно устанавливать в необходимом вам объеме. Установив систему как рабочую станцию, необходимо будет указать параметры сети, в которой эта рабочая станция будет работать.

Практически все возможные настройки системы Linux доступны из командной строки, но пользователям Windows привычнее работать с графическим интерфейсом, в котором и рассмотрим настройку рабочей станции Linux для работы в сети Windows. На рассматриваемой рабочей станции установлена ОС ASPLinux 11.2, имеющая весьма широкое распространение у российских пользователей.

1. Подключите компьютер к сети.
2. Нажмите кнопку **Система** (рис. 1.41).
3. Выберите **Администрирование | Сеть**.
4. В открывшемся окне **Запрос** (рис. 1.42) введите пароль администратора системы. Откроется окно **Настройка сети** (рис. 1.43).
5. На вкладке **Оборудование** этого окна вы должны увидеть ваш сетевой адаптер, который определился 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 пи помощи dhcp**.
9. Согласитесь с предложением системы сохранить настройки.

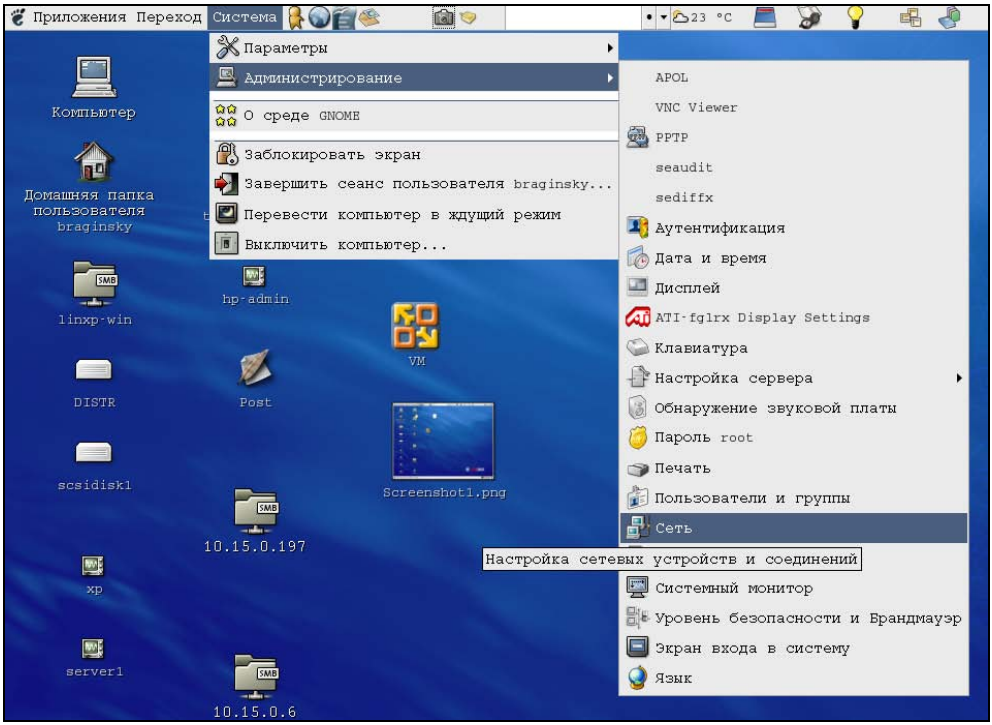


Рис. 1.41. Рабочий стол ASPLinux 11.2 (фрагмент).
Выбор меню **Система | Администрирование | Сеть**

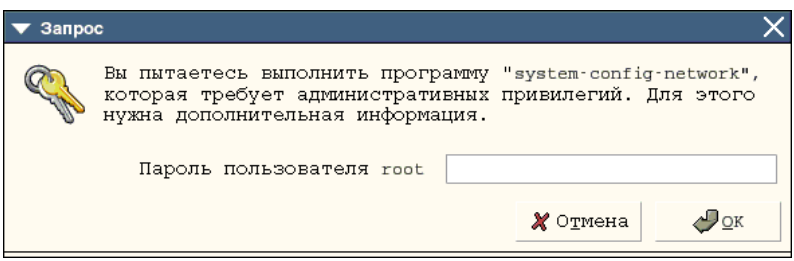


Рис. 1.42. Окно **Запрос**. Ввод пароля администратора

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.

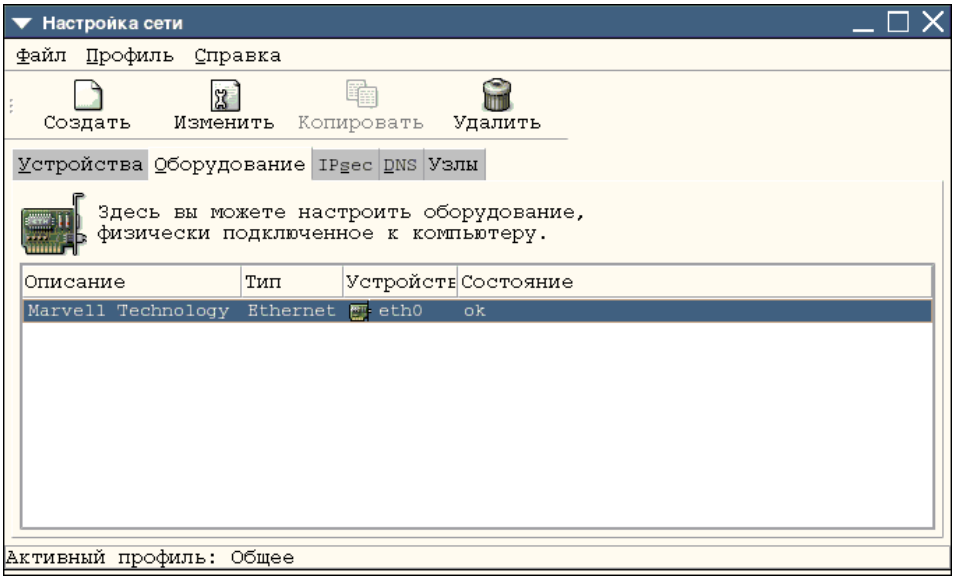


Рис. 1.43. Окно **Настройка сети**

Для подключения к сетевым каталогам достаточно в меню **Файл** любого локального каталога выбрать пункт **Соединиться с сервером** и указать в окне **Соединение с сервером** в качестве типа 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.

Общие файлы и принтеры

Настроив свои компьютеры для работы в сети, вы сможете совместно использовать файлы и принтеры. Для просмотра сохраненного видео, например, не потребуется делать копию фильма и переносить ее на другой компьютер. Достаточно открыть имеющийся файл из общего сетевого каталога. Аналогично, для печати документов с разных компьютеров нет необходимости подключать принтер к каждому компьютеру. Достаточно иметь один общий принтер. Настройка компьютеров для работы с общими файлами и принтерами для Windows и Linux отличается. Но рассмотрим все по порядку.

Настраиваем общий доступ к файлам и папкам в Windows Vista

Откройте из Панели управления окно **Центр управления сетями и общим доступом**, в котором найдите задачу **Просмотр компьютеров и устройств**. Откроется окно **Сеть** (рис. 1.44).

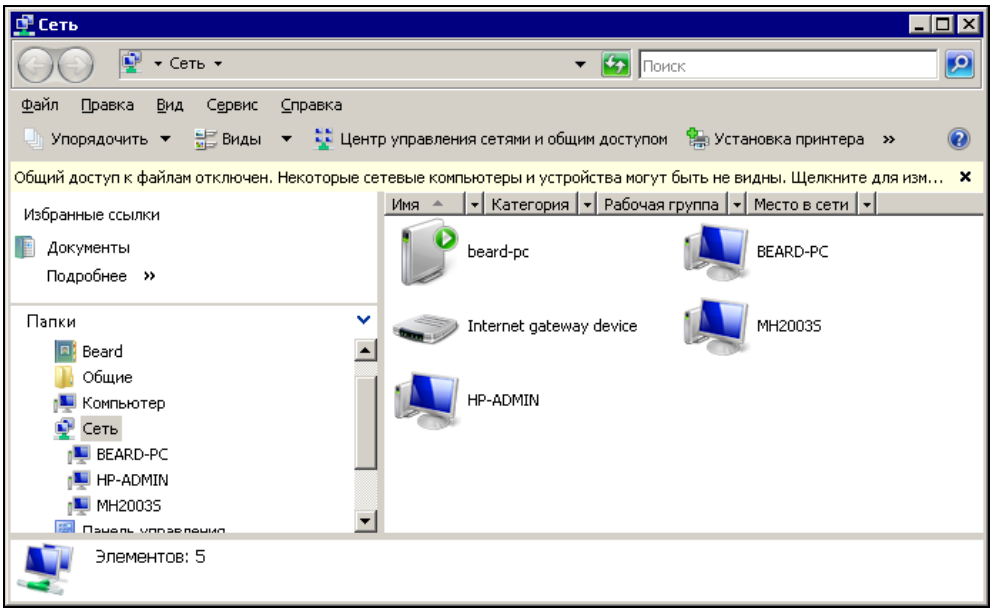


Рис. 1.44. Окно **Сеть**

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.

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. 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. Тоже 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 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 1, которая впоследствии переименована в Beard. Вы можете исполь-

зовать любые имена для своих учетных записей, заменяя ими те, что использовал автор.

Создадим для учетной записи Beard каталог с общим доступом.

Откроем папку пользователя **Пуск | Документы | Beard** (рис. 1.45).

Создадим вложенную папку Share, откроем окно ее свойств и перейдем на вкладку **Доступ** (рис. 1.46).

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

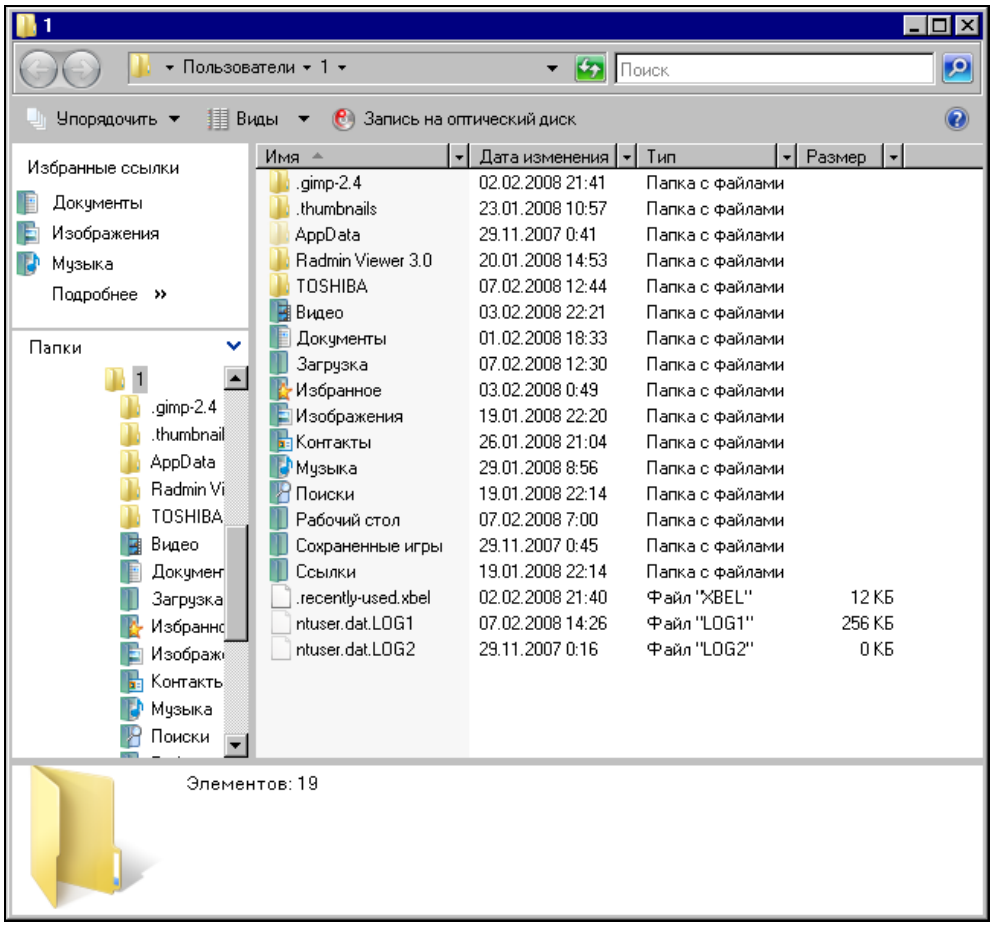


Рис. 1.45. Окно **1** (папка текущей учетной записи)

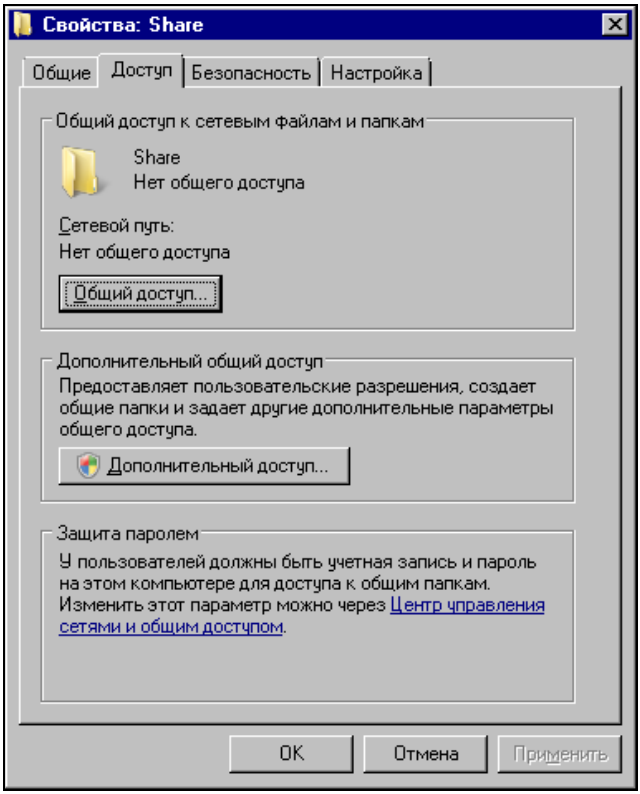


Рис. 1.46. Окно **Свойства: Share**

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. 1.47).

Теперь воспользуемся кнопкой **Дополнительный доступ** (см. рис. 1.46). Нажав на нее, мы вызовем окно **Дополнительный общий доступ** (рис. 1.48). Только что мы обеспечили доступ локальных пользователей к папке, теперь обеспечим доступ по сети. Нажмем кнопку **Разрешения**.

В открывшемся окне **Разрешения для Share** (рис. 1.49) 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. 1.50).

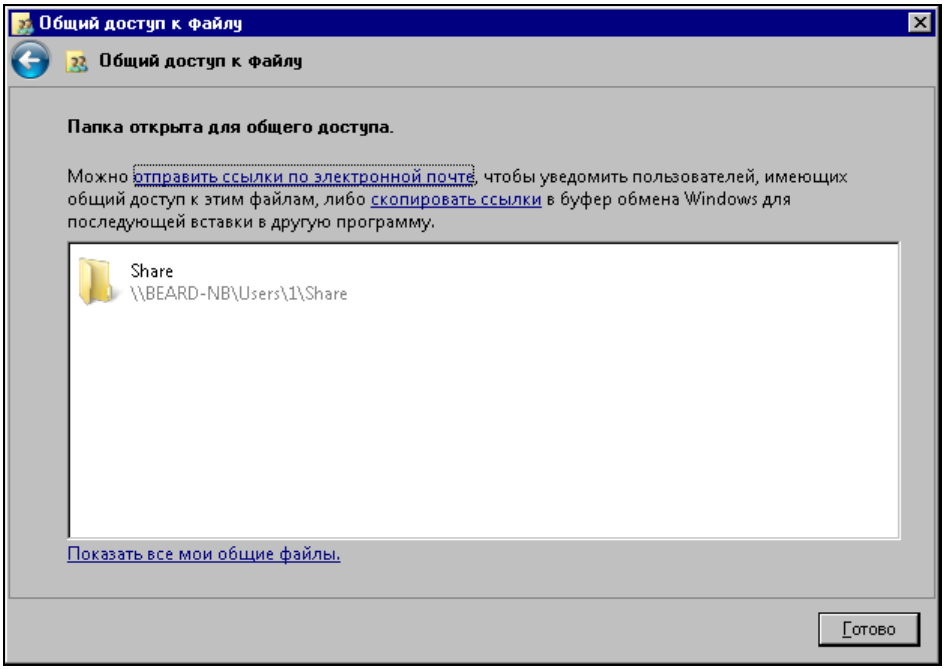


Рис. 1.47. Окно **Общий доступ к файлу**. Сообщение об открытии общего доступа

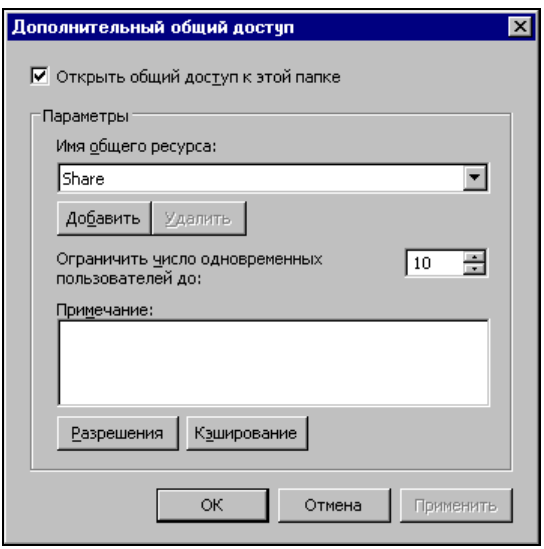


Рис. 1.48. Окно **Дополнительный общий доступ**

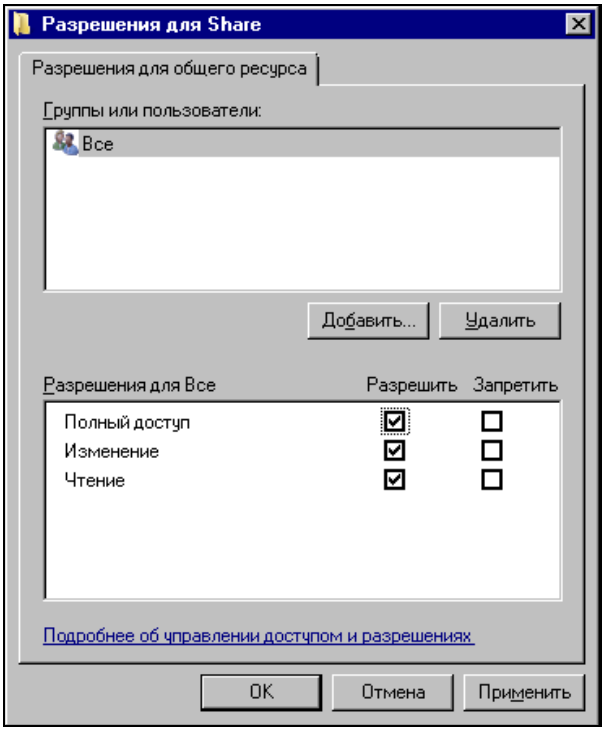


Рис. 1.49. Окно **Разрешения для Share**

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. 1.51).

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

Напоминаем, 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 обслуживание | 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.

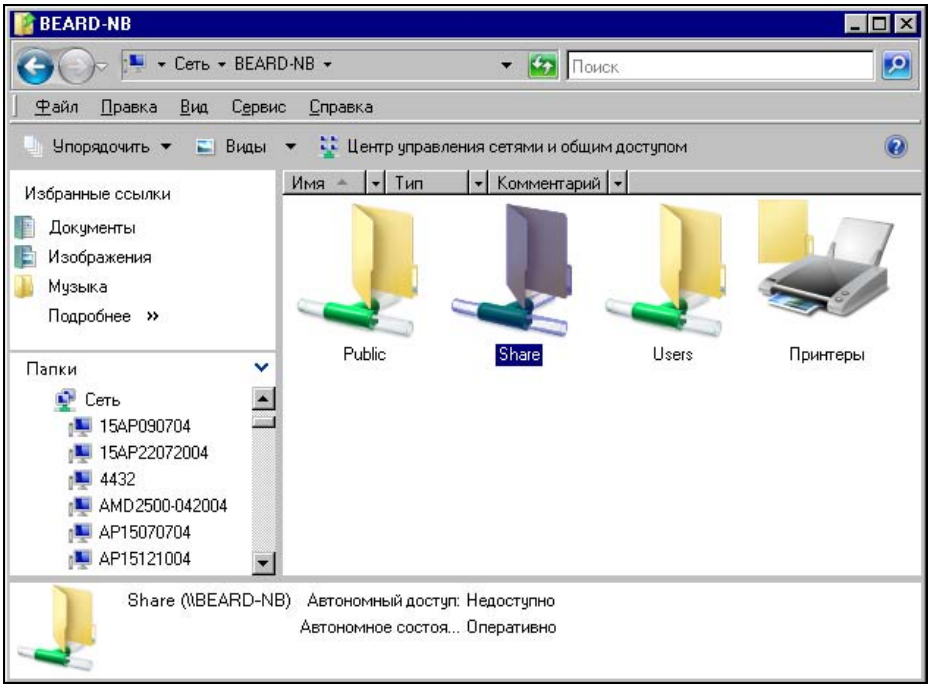


Рис. 1.50. Окно **BEARD-NB**.
Общие ресурсы, видимые через сеть с другого компьютера

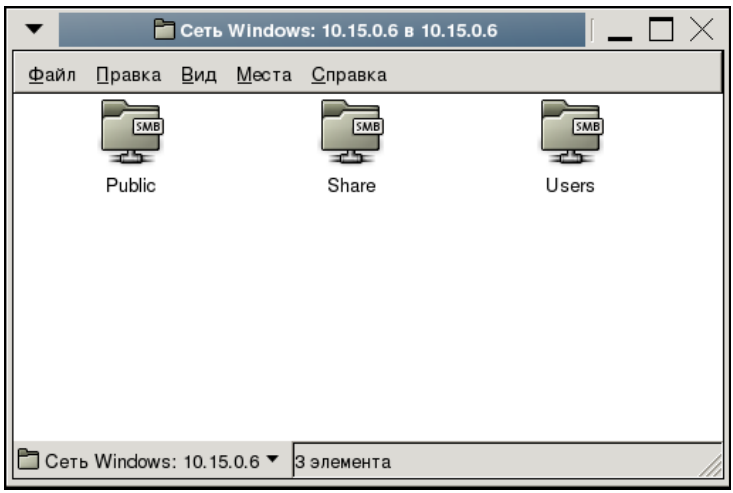


Рис. 1.51. Доступные по сети ресурсы на компьютере с IP 10.15.0.6
при подключении из Linux

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 ASPLinux 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**.

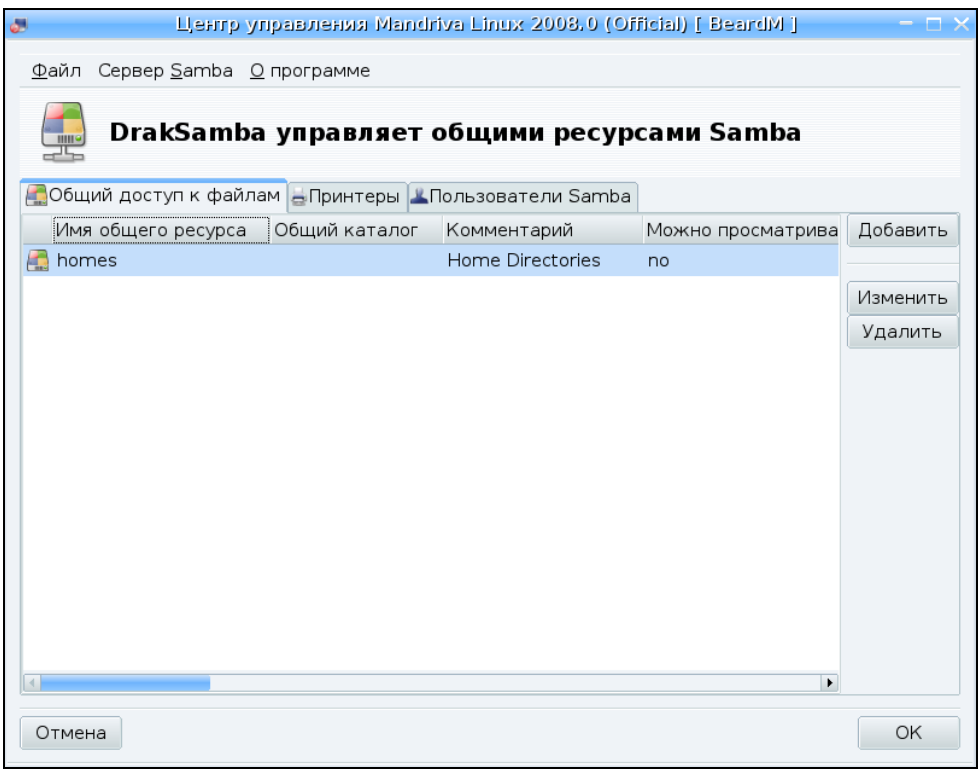


Рис. 1.52. Окно **Центр управления Mandriva Linux 2008.0**

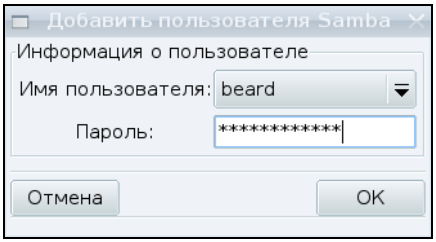


Рис. 1.53. Окно **Добавить пользователя Samba**

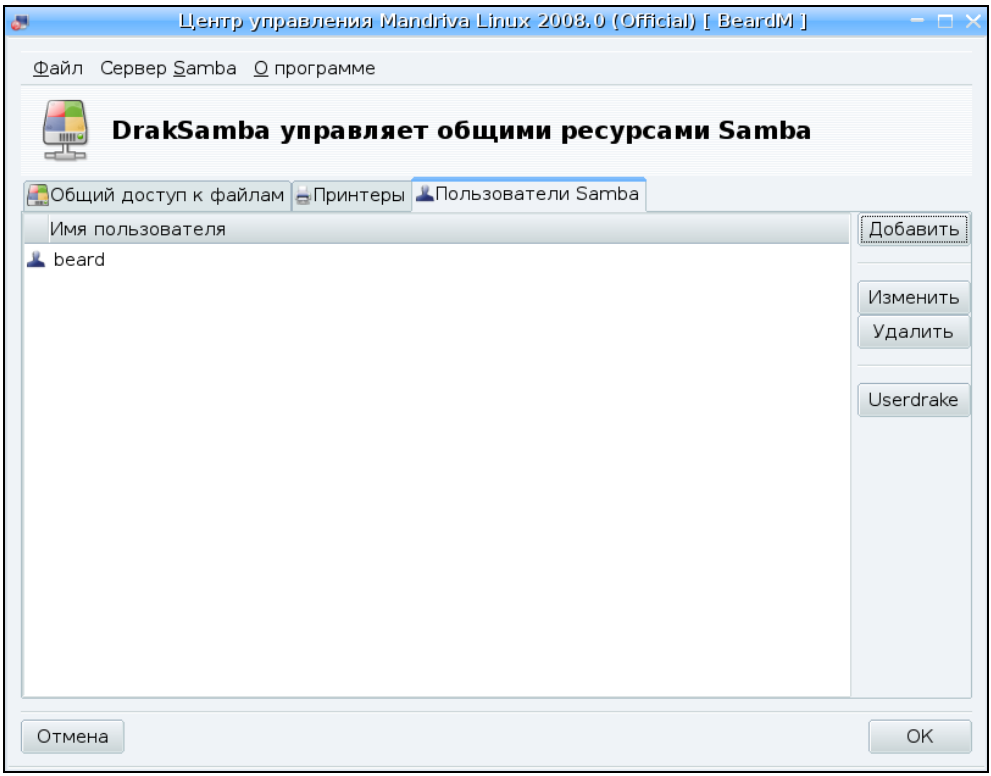


Рис. 1.54. Окно **Центр управления Mandriva Linux 2008.0**, вкладка **Пользователи Samba**

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.

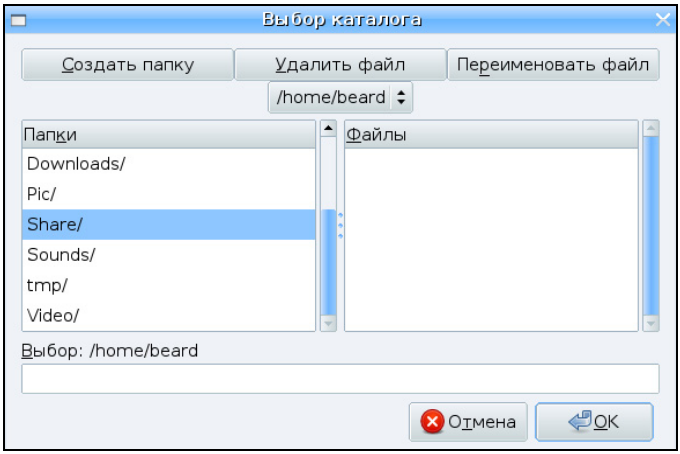


Рис. 1.55. Окно **Выбор каталога**

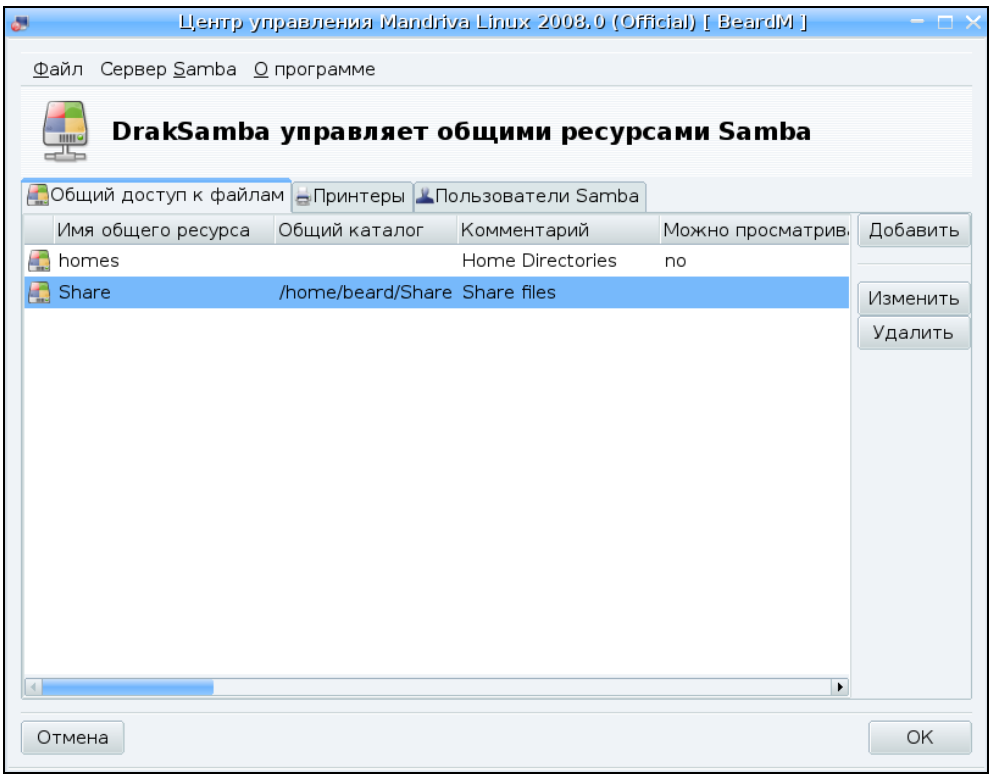


Рис. 1.56. Окно **Центр управления Mandriva Linux 2008.0**, вкладка **Общий доступ к файлам**

Однажды настроив Samba в одной версии Linux, вы легко повторите настройки в любой другой. Рассмотрим настройку Samba в Mandriva Linux.

Итак, пройдите по указанному выше пути и откройте окно **Центр управления Mandriva Linux 2008.0** (рис. 1.52). Прежде чем система допустит вас к настройкам компьютера, потребуется ввести пароль администратора. Введите его.

В окне **Центр управления Mandriva Linux 2008.0** нажмите кнопку **Добавить**. Откроется окно **Добавить пользователя Samba** (рис. 1.53).

Выберите имя пользователя из числа имеющихся учетных записей в раскрывающемся списке. В окне **Центр управления Mandriva Linux 2008.0** на вкладке **Пользователи Samba** (рис. 1.54) появится строка с именем учетной записи, имеющей права доступа.

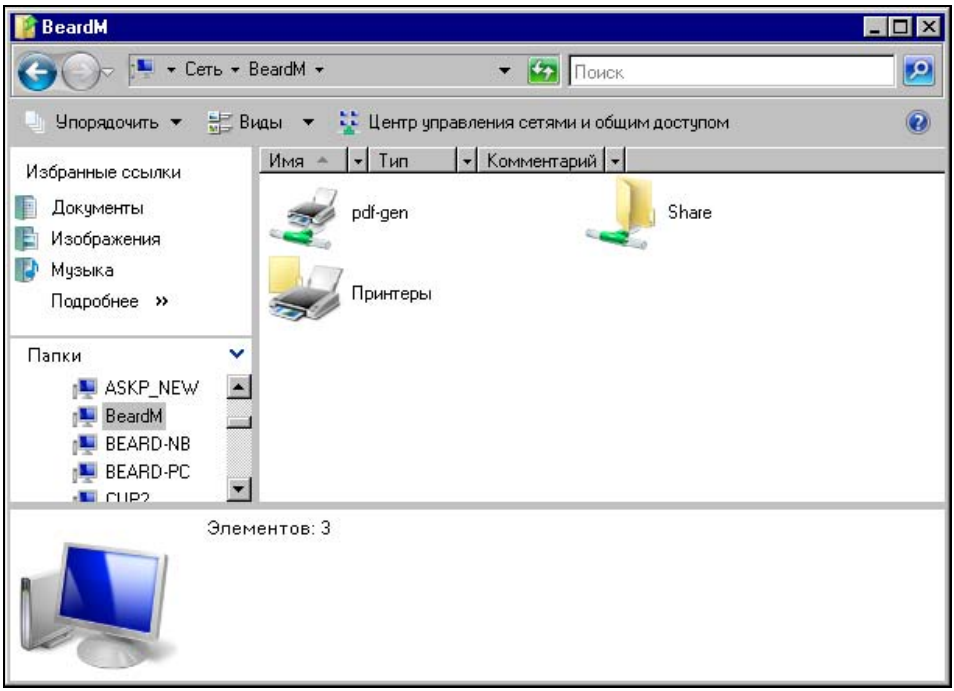


Рис. 1.57. Окно **BeardM**. Доступные по сети ресурсы

В окне **Центр управления Mandriva Linux 2008.0** на вкладке **Общий каталог** нажмите кнопку **Добавить** для добавления каталога общего доступа. От-

кроется окно **Выбор каталога** (рис. 1.55), 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. 1.56) появится строка с именем выбранного каталога. Теперь доступ к каталогу Share возможен с любой рабочей станции под управлением Windows или Linux. На рис. 1.57 представлено окно с доступными ресурсами компьютера под управлением Linux, открытого в сети с компьютера под управлением Windows Vista.

Особенности сетевого доступа к файлам из Linux к Windows Vista

К сожалению, не всегда удается такими простыми настройками обеспечить доступ к файлам и папкам по сети. Если из Linux выполнять подключение к ресурсам Windows до Windows Vista, то проблем не возникает. Но в Windows Vista изменен протокол доступа к файлам и папкам. Этот протокол существует 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 — Terminal.

В ASPLinux это окно можно вызвать **Приложения | Стандартные | Терминал**. Но можно просто войти в консольный сеанс с помощью нажатия комбинации клавиш <Ctrl>+<Alt>+<F*n*>, 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
```

Здесь `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 сможете 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 отмонтировать сетевой каталог, прекратив доступ к его файлам, достаточно ввести команду

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

Общий принтер в Windows

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, под управлением которого работают практически все принтеры HP. Загрузить этот драйвер можно по ссылке:

ftp://ftp.hp.com/pub/softlib/software9/COL17052/ja-45284-6/HPUPD41PCL632.exe

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.

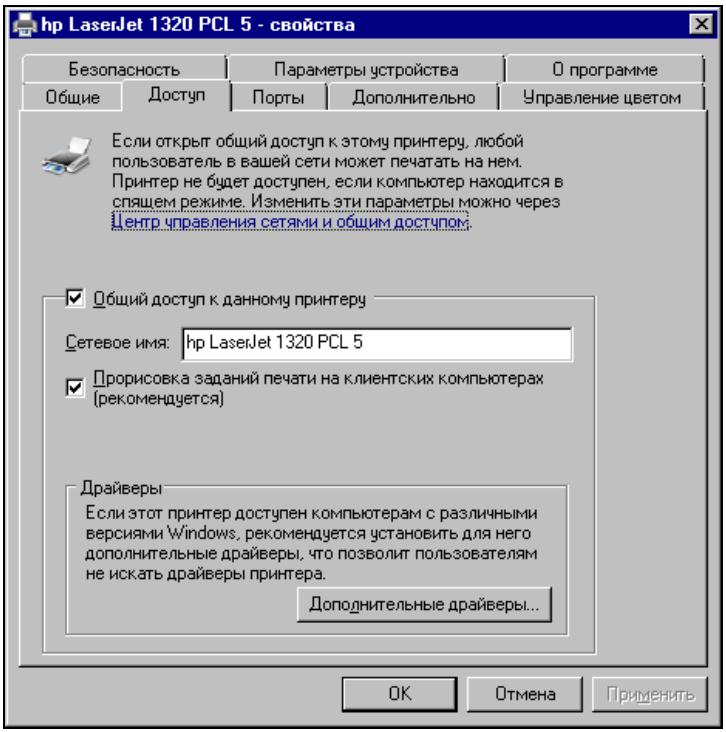


Рис. 1.58. Окно свойств принтера

Для предоставления доступа к принтеру (считаем, что он уже установлен) следует проделать следующее:

1. Откройте окно свойств принтера. Установленные принтеры можно найти в папке **Пуск | Панель управления | Принтеры**. Щелкните правой кноп-

кой мыши по значку выбранного принтера и выберите пункт **Свойства**. В открывшемся окне перейдите на вкладку **Доступ** (рис. 1.58).

2. Отметьте флажок **Общий доступ к данному принтеру**.
3. Нажмите кнопку **OK**.

Теперь перейдите на компьютер, с которого хотите получить доступ к принтеру. Конечно, компьютер должен быть подключен к вашей сети.

Войдите в **Центр управления сетями и общим доступом** (**Пуск | Настройка | Панель управления | Центр управления сетями и общим доступом**).

В левой части окна выберите задачу **Просмотр компьютеров и устройств**. Откроется окно **Сеть**. Найдите в сети компьютер с подключенным принтером и откройте его (рис. 1.59).

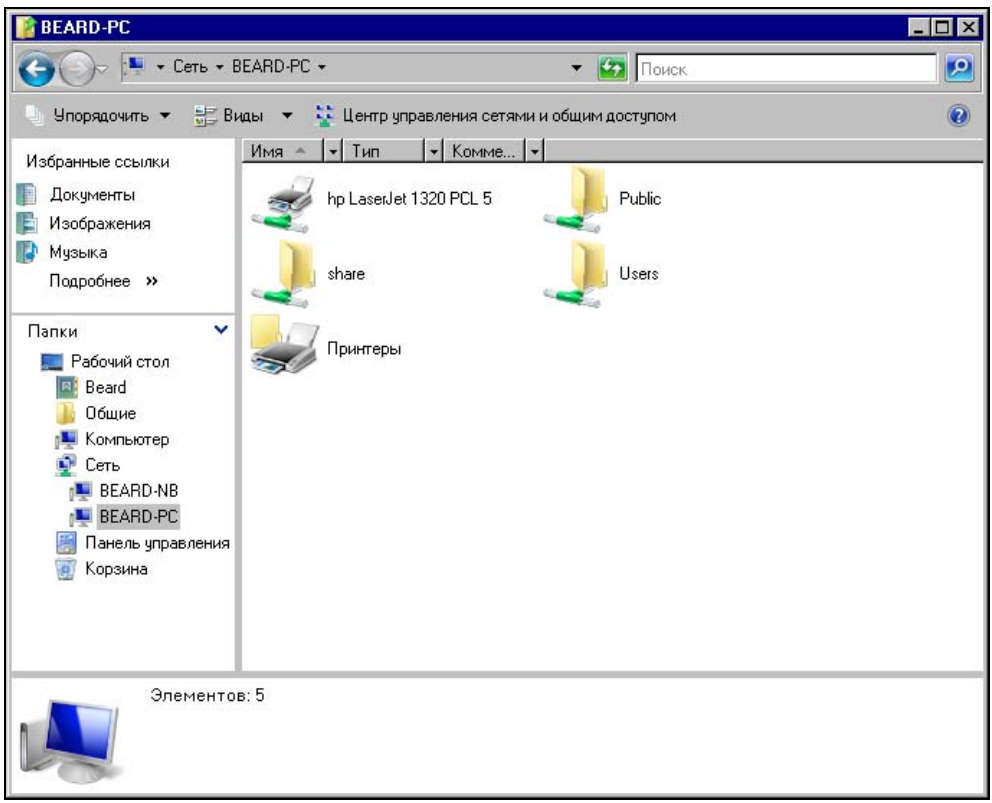


Рис. 1.59. Окно **BEARD-PC**

Выделите подключаемый принтер и в контекстном меню (щелчок правой кнопкой мыши) выберите команду **Подключить**. Если драйверы установлены верно и полностью совместимы с Windows Vista, принтер будет подключен.

На рис. 1.60 приведено изображение папки Принтеры, в которой содержатся (слева направо) локальный принтер с общим доступом, включенный по умолчанию, локальный принтер без общего доступа, подключение к принтеру на компьютере BEARD-NB.

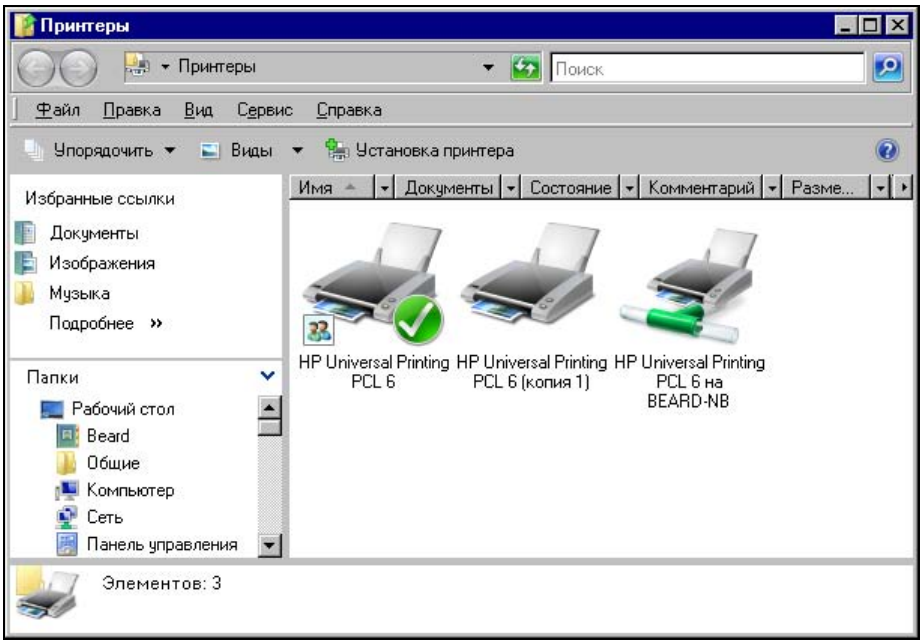


Рис. 1.60. Окно **Принтеры**

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 неизвестна, но известен его тип.

В ASPLinux это делается следующим образом:

1. Откройте окно **Настройка принтера** (рис. 1.61), 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.

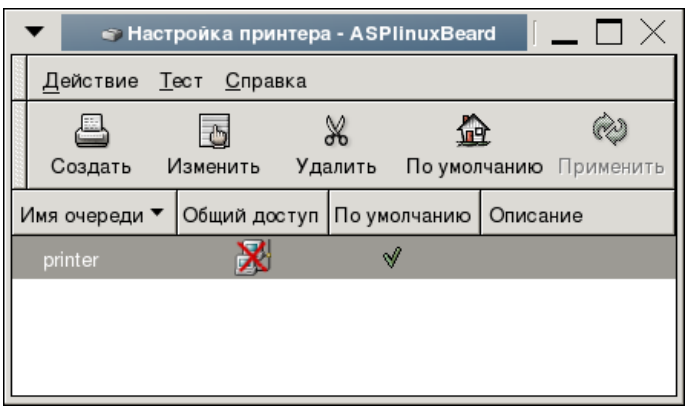


Рис. 1.61. Окно **Настройка принтера**

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. 1.62).
3. Выберите в левой части окна раздел **Оборудование**, а в правой — **Настройка принтеров и очередей печати**. Откроется окно **Printerdrake** (рис. 1.63), в котором следует нажать кнопку **Да**. На другие вопросы системы также отвечайте положительно.

Примечание

Подробно о работе с этой утилитой можно прочитать в Интернете по адресу: **http://wertpage.pp.ru/www/UNIX/MandrivaDrakxtools/printerdrake.html**.

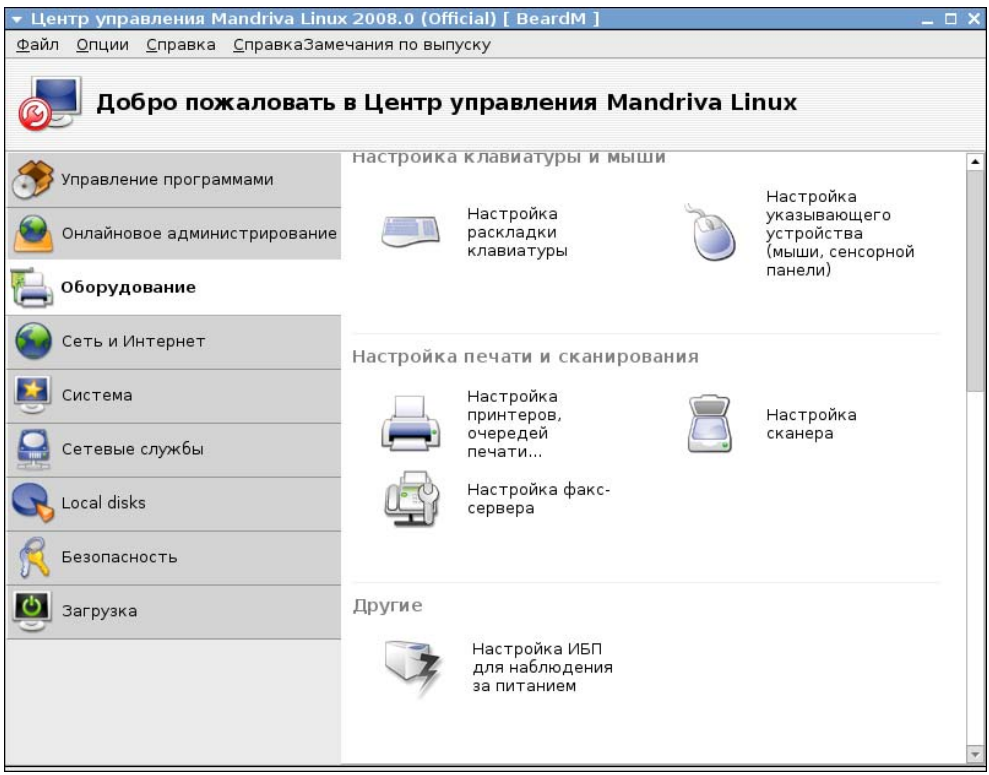


Рис. 1.62. Окно **Центр управления Mandriva Linux**

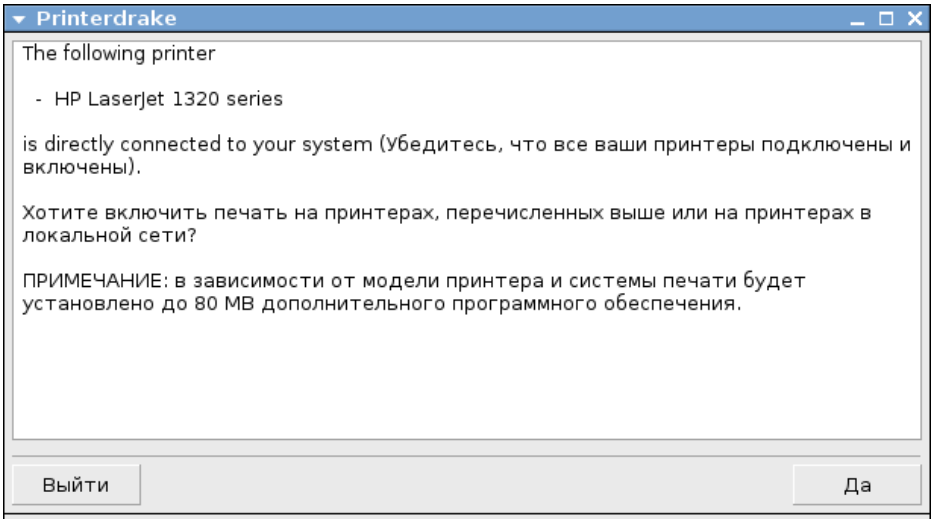


Рис. 1.63. Окно **Printerdrake**

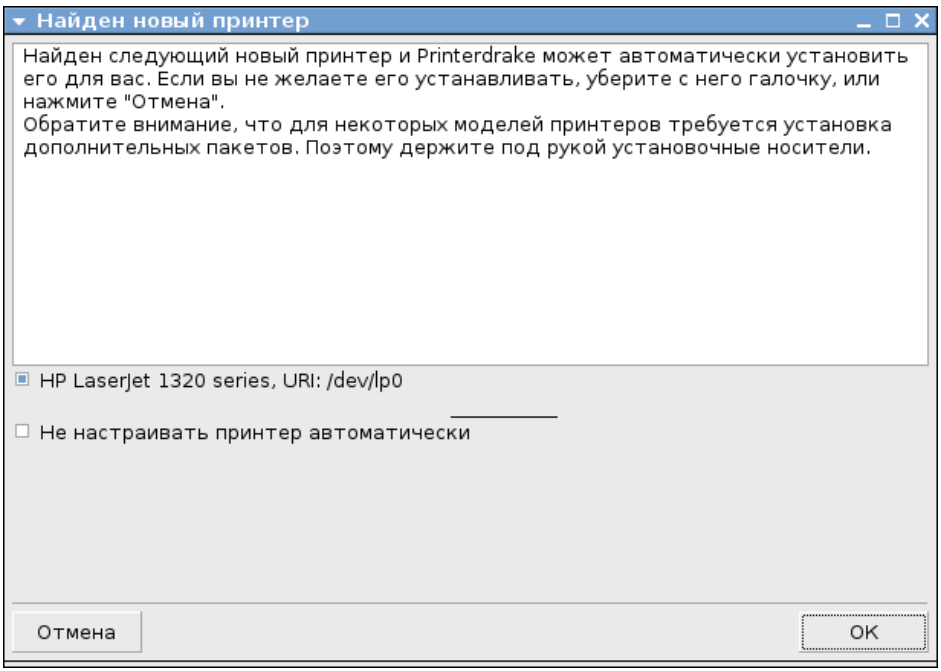


Рис. 1.64. Окно **Найден новый принтер**

4. В открывшемся окне **Найден новый принтер** (рис. 1.64) снова согласитесь с предложением системы установить принтер автоматически, нажав кнопку **OK**. Откроется окно **Центр управления Mandriva Linux** на странице **Принтеры**, в котором вы увидите строку с именем установленного принтера (рис. 1.65).

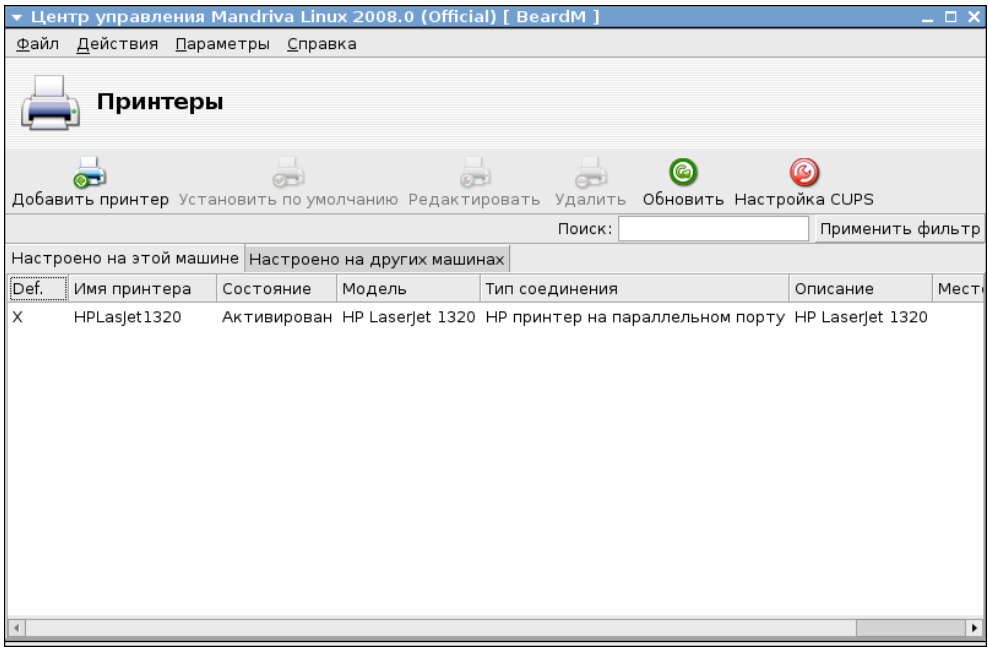


Рис. 1.65. Окно **Центр управления Mandriva Linux**, страница **Принтеры**

Все, принтер установлен. 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.1.66). Следует выбирать самую новую версию драйвера из установленных в системе.

Подключенный принтер можно увидеть в папке Принтеры (рис. 1.67). Можно использовать этот принтер для печати документов.

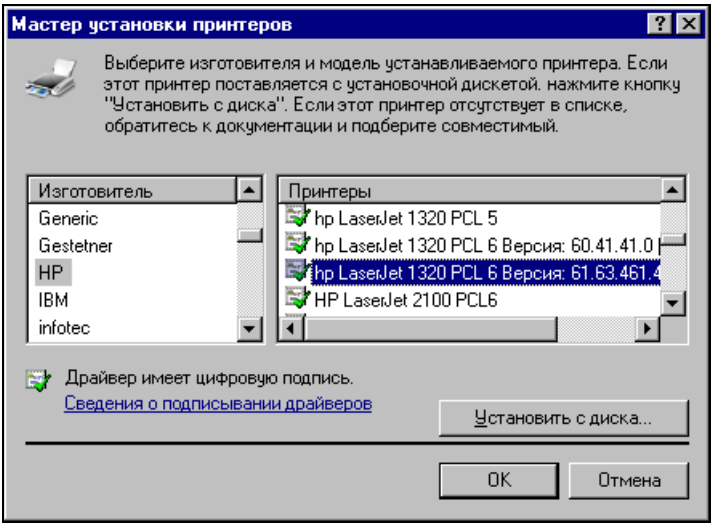


Рис. 1.66. Окно **Мастер установки принтеров**

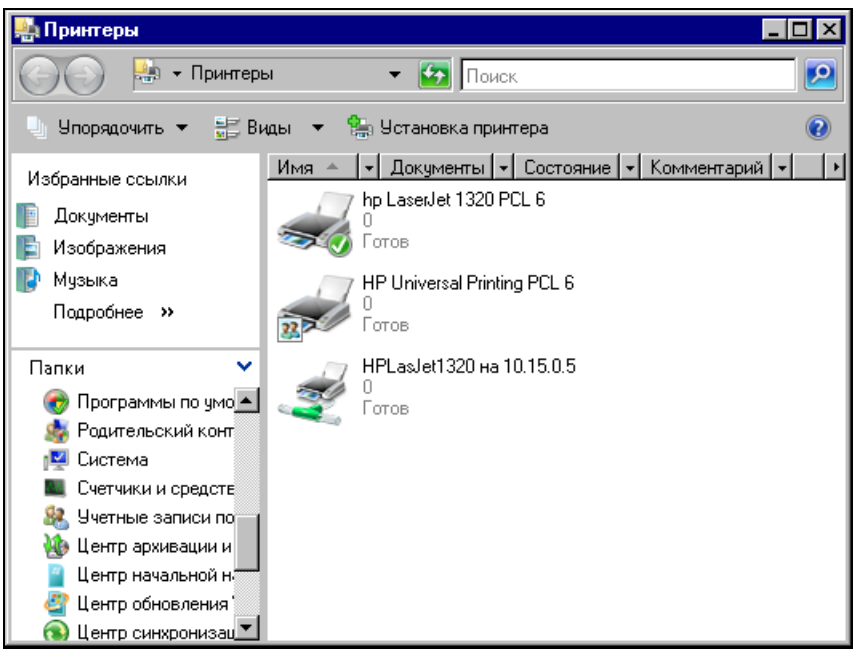


Рис. 1.67. Окно **Принтеры**

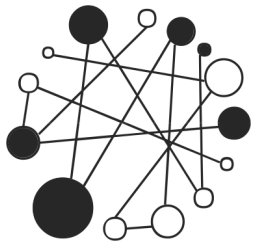
Подключение к принтеру из Linux мы уже рассматривали ранее. Если к принтеру предоставлен общий доступ, то не имеет существенного значения, в какой ОС он установлен. Подключение к нему можно выполнять также из любой операционной системы.

* * *

Ну, вот и завершилась *глава 1*.

Нам удалось решить основные задачи нашей сети. Мы получили возможность обмена файлами и использования общего принтера. В следующей главе рассмотрим варианты подключения нашей сети к Интернету.

Глава 2



Подключаем сеть к Интернету

Работа на персональном компьютере редко проходит без взаимодействия с Интернетом. Школьники и студенты ищут материал для рефератов и курсовых работ, 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 часто требуют провайдеры, то для такого же подключения второго компьютера потребуется вторая телефонная линия, а для подключения третьего компьютера — третья... Кабельный Интернет тоже доступен 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 варианты осуществления этой идеи существуют?

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 кото-

рый 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. 2.1). 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.

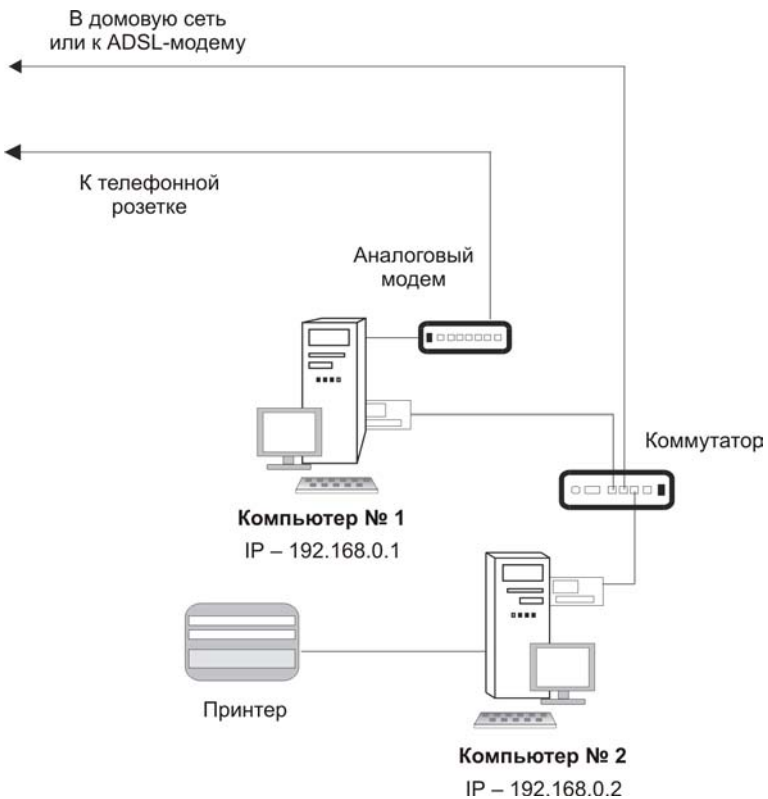


Рис. 2.1. Вариант простой домашней сети с общим принтером и общим доступом в Интернет

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, условные, 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 Интернетом.

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 МТС 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 сетью 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 ноутбуки). 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 предполагая, что открывается окно свойств сетевого подключения.

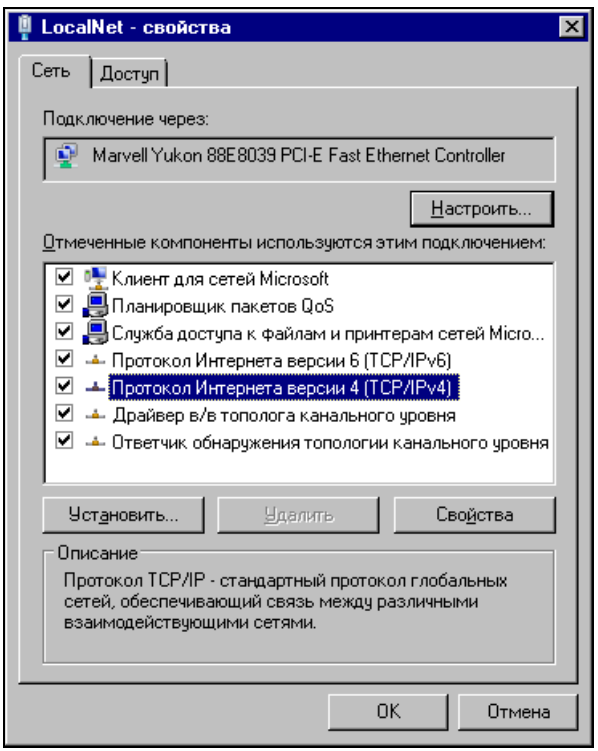


Рис. 2.2. Окно **LocalNet - свойства**

Само сетевое подключение имеет имя, которое вы можете изменить самостоятельно, как имя файла. В данном примере используется имя LocalNet. Подобные короткие имена удобны, 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. 2.2).

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 (рис. 2.3).

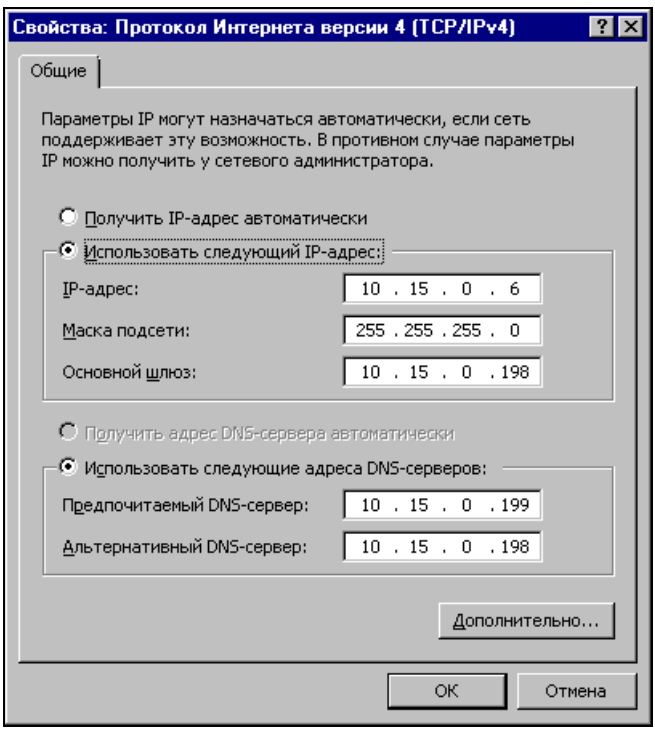


Рис. 2.3. Окно **Свойства: Протокол Интернета версии 4 (TCP/IPv4)**

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 интернет-связи со шлюзом.

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

Для обеспечения возможности работы в Интернете важны все следующие параметры.

- Поле **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. Они будут продолжать "видеть" и после его изменения.
- Переключатель **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, то 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 ASPLinux доступ к рассматриваемым настройкам можно получить так, как уже было показано в *главе 1*. В окне **Настройка сети** на вкладке **Устройства** (рис. 2.4) нужно выбрать сетевой адаптер, используемый для подключения к локальной сети, и нажать кнопку **Изменить**. При этом откроется окно **Устройство Ethernet** (рис. 2.5).

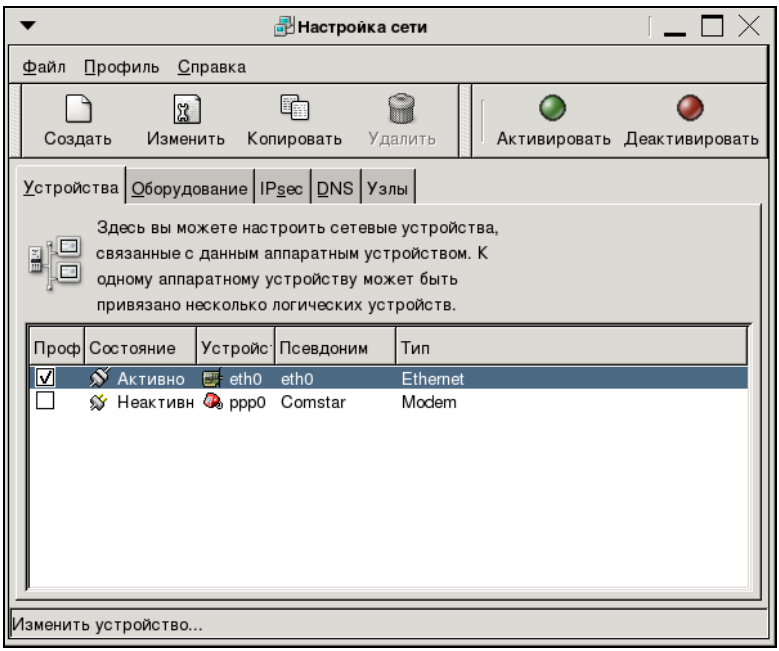


Рис. 2.4. Окно **Настройка сети**

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. 2.6) необходимо выбрать сетевой интерфейс и нажать кнопку **Настройка**. В открывшемся окне **Network setting** появятся знакомые вам параметры (рис. 2.7).

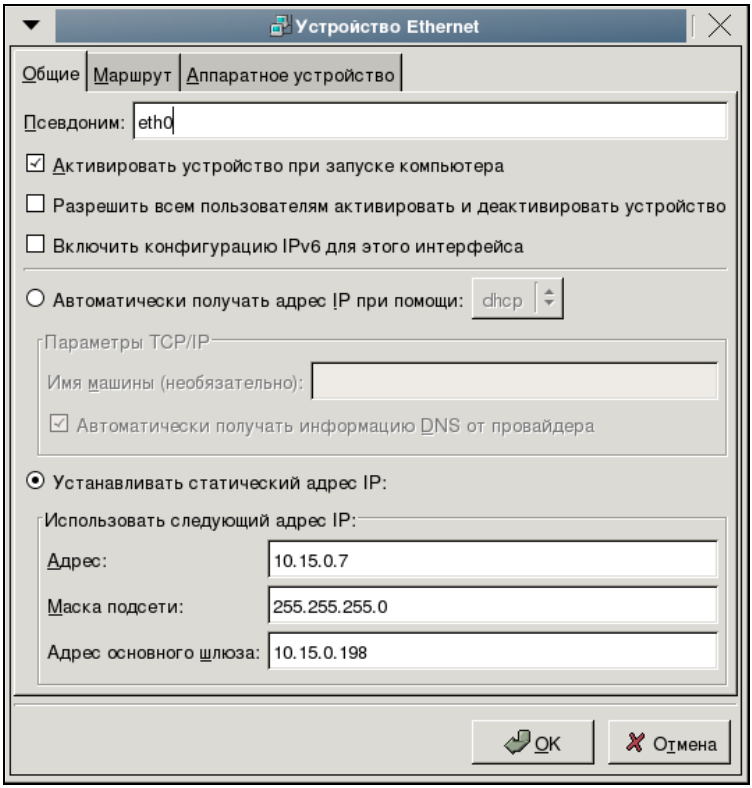


Рис. 2.5. Окно **Устройство Ethernet**

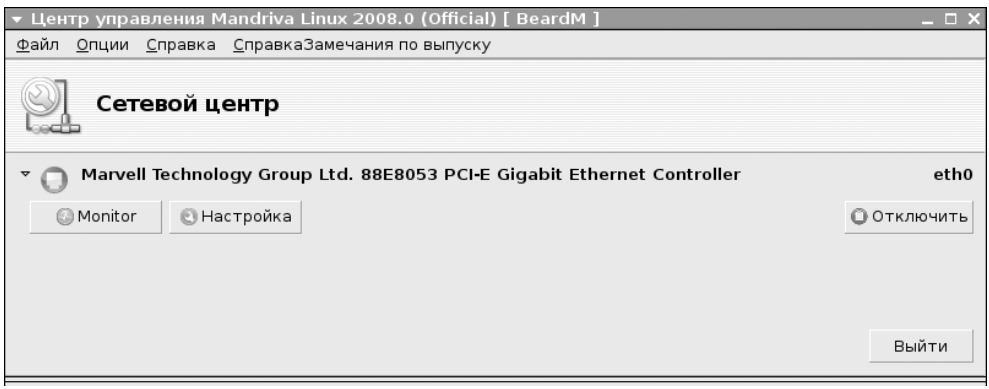


Рис. 2.6. Окно **Центр управления Mandriva Linux 2008.0**, страница **Сетевой центр**

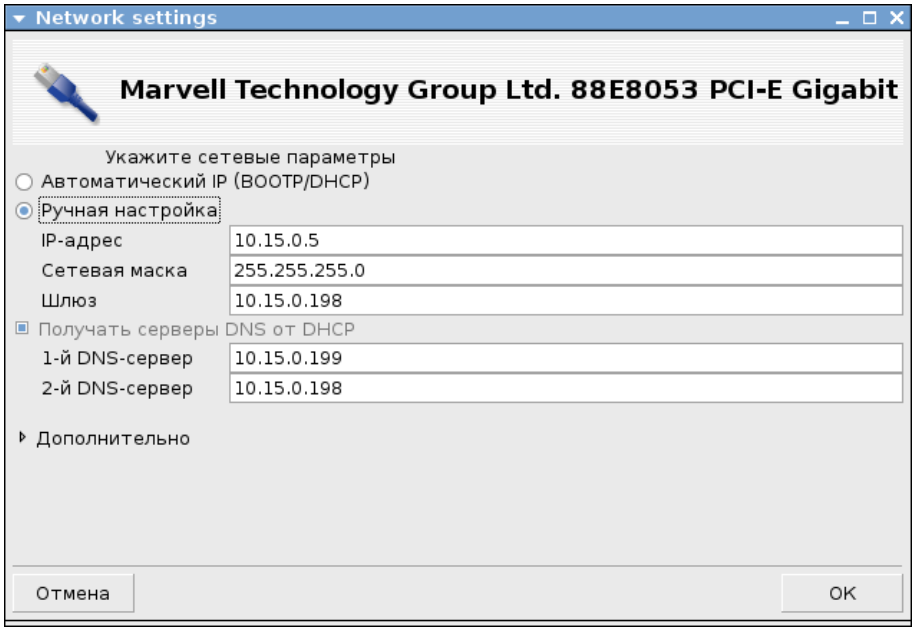


Рис. 2.7. Окно **Network setting**

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.

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 (на рис. 2.1 изображен самостоятельный коммутатор). Один из распространенных ADSL-модемов — D-Link 500T, настройки которого для подключения к Stream (**http://stream.ru**) мы и рассмотрим. Для подключения к другим провайдерам придется сделать корректировки настроек, но их общий 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, имеющие Web-интерфейс для настроек, имеют заранее заданный производи-

телем 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. 2.8).

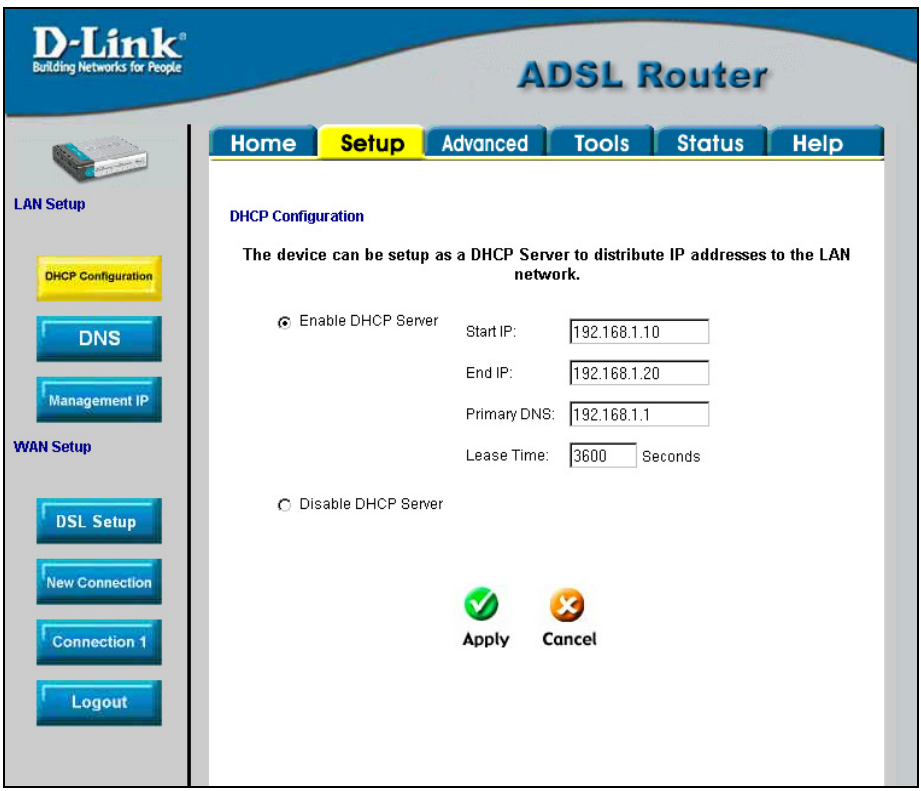


Рис. 2.8. Окно **ADSL Router**, вкладка **Setup**, нажата кнопка **DHCP Configuration**

На открывшейся странице отметьте переключатель **Enable DHCP Server** (Включить DHCP-сервер). Такой сервер был упомянут 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 рис. 2.8 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;

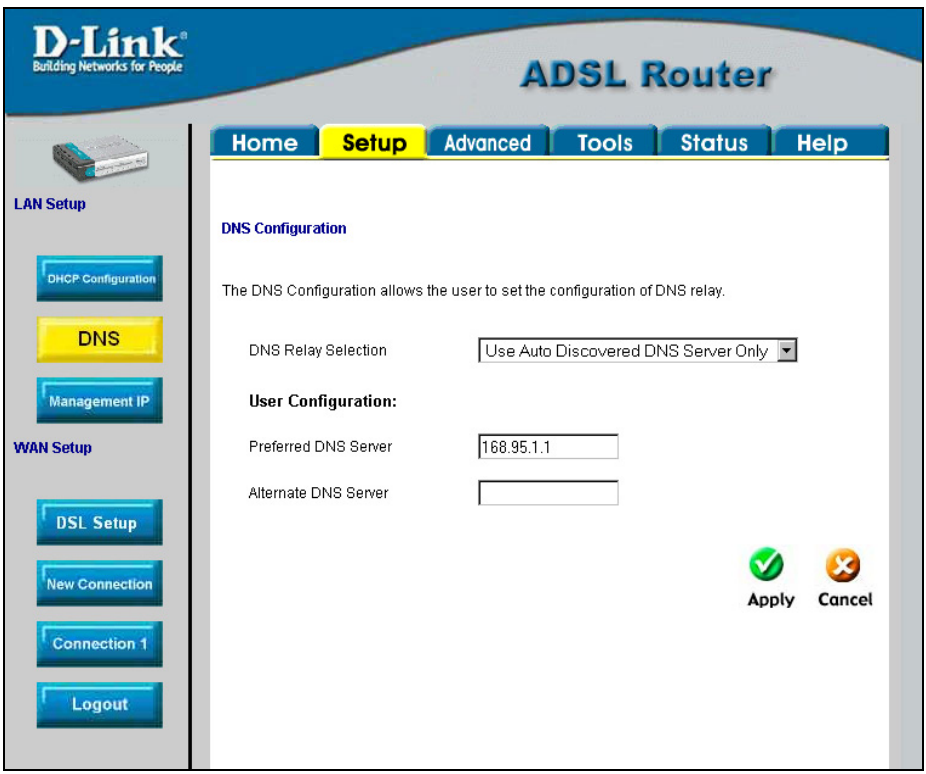


Рис. 2.9. Окно **ADSL Router**, вкладка **Setup**, нажата кнопка **DNS**

- **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 Интернете, 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.

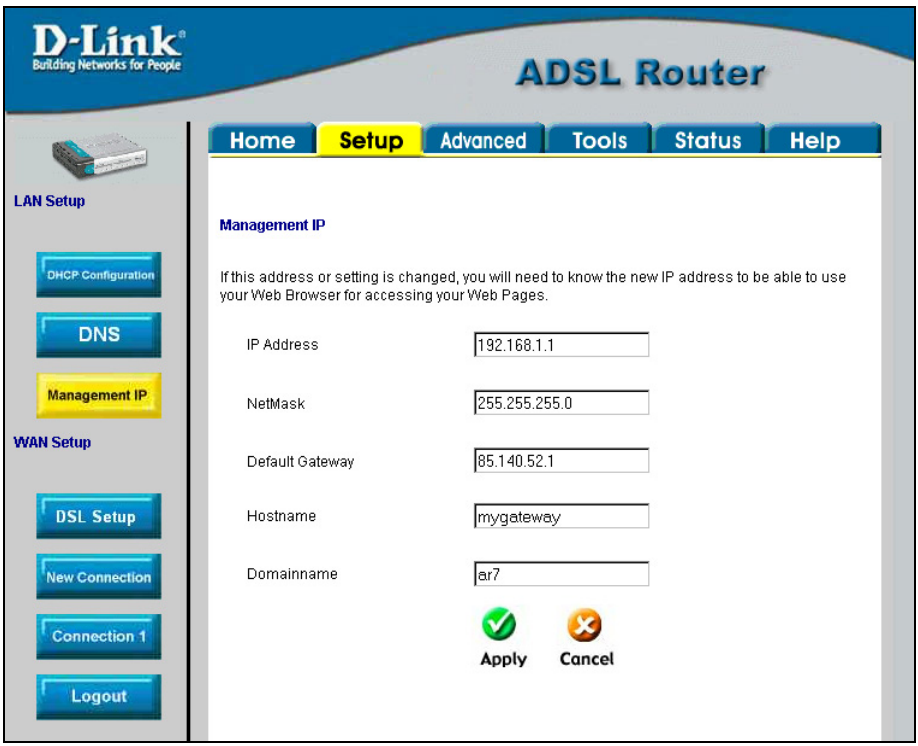


Рис. 2.10. Окно **ADSL Router**, вкладка **Setup**, нажата кнопка **Management IP**

Нажав кнопку **DNS**, переходим к указанию DNS-серверов или способу получения их адресов модемом (рис. 2.9). В данном случае модем автоматически получает их адреса от провайдера, а клиенты сети могут использовать адрес модема вместо DNS-сервера.

Кнопкой **Management IP** (Маршрутизация IP) открывается страница настройки адресов шлюзов (рис. 2.10). Маршрутизатор модема для внешней сети выглядит сетевым устройством, которое имеет свои 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. Символьные 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.

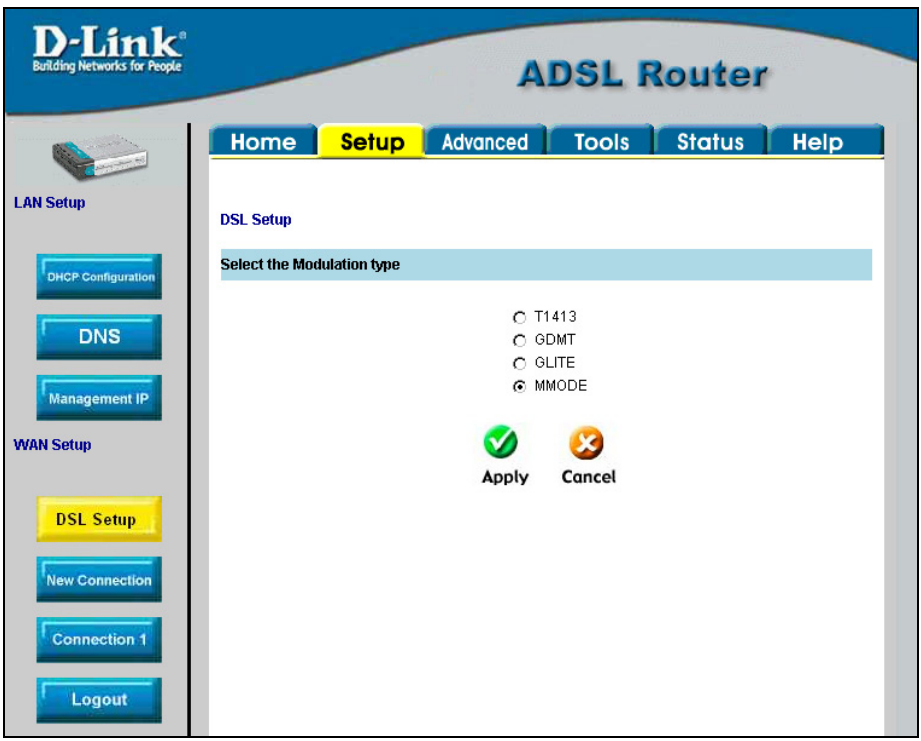


Рис. 2.11. Окно **ADSL Router**, вкладка **Setup**, нажата кнопка **DSL Setup**

Кнопка **DSL Setup** открывает окно выбора используемого провайдером типа модуляции при передаче данных между модемами (рис. 2.11). Если провайдер не дает других рекомендаций, то обычно подходит режим **MMODE**.

После создания нового подключения на странице, открываемой кнопкой **New Connection**, для него автоматически создается новая страница и кнопка для ее открытия **Connection 1** (рис. 2.12). Параметры подключения могут быть отредактированы после его создания. Имя подключения может быть любым, тип подключения — **PPPoE**, имя пользователя и пароль предоставляются провайдером. Параметры **VPI** и **VCI** также предоставляются провайдером.

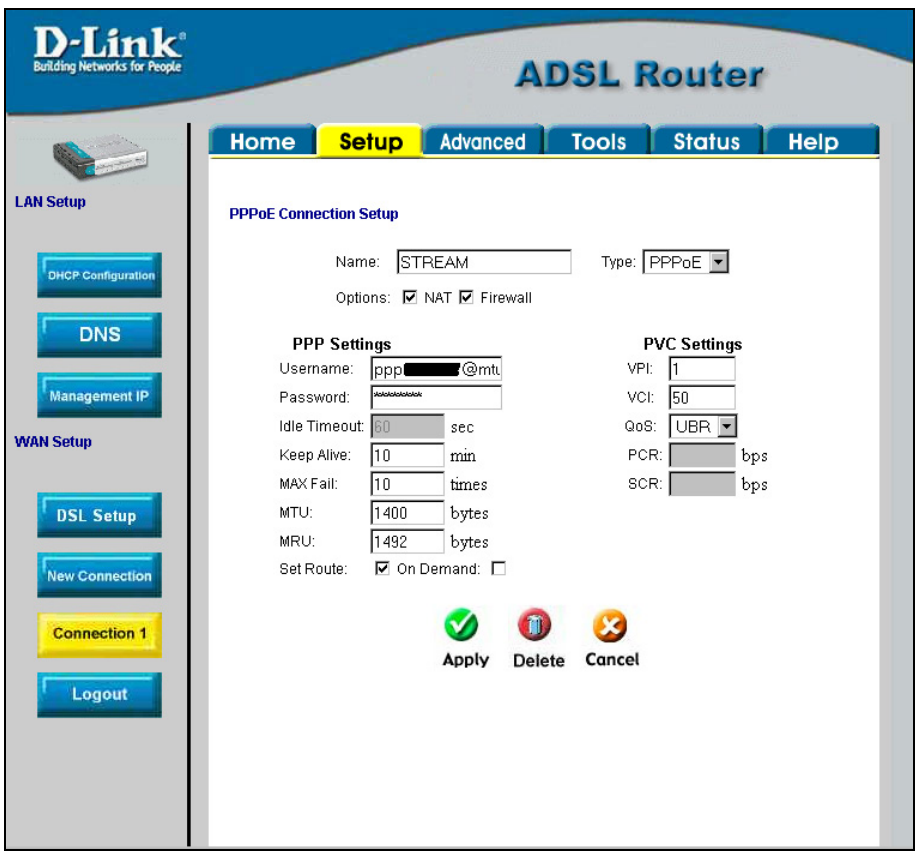


Рис. 2.12. Окно **ADSL Router**, вкладка **Setup**, нажата кнопка **Connection 1**

Необходимо включить опции **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. О возможности работы с вашими компьютерами из Интернета мы поговорим в *главе 5*. Сейчас только покажем страницу, открывающуюся кнопкой **Port Forwarding** на вкладе **Advanced**, где выполняются настройки для доступа к вашим компьютерам из Интернета (рис. 2.13).

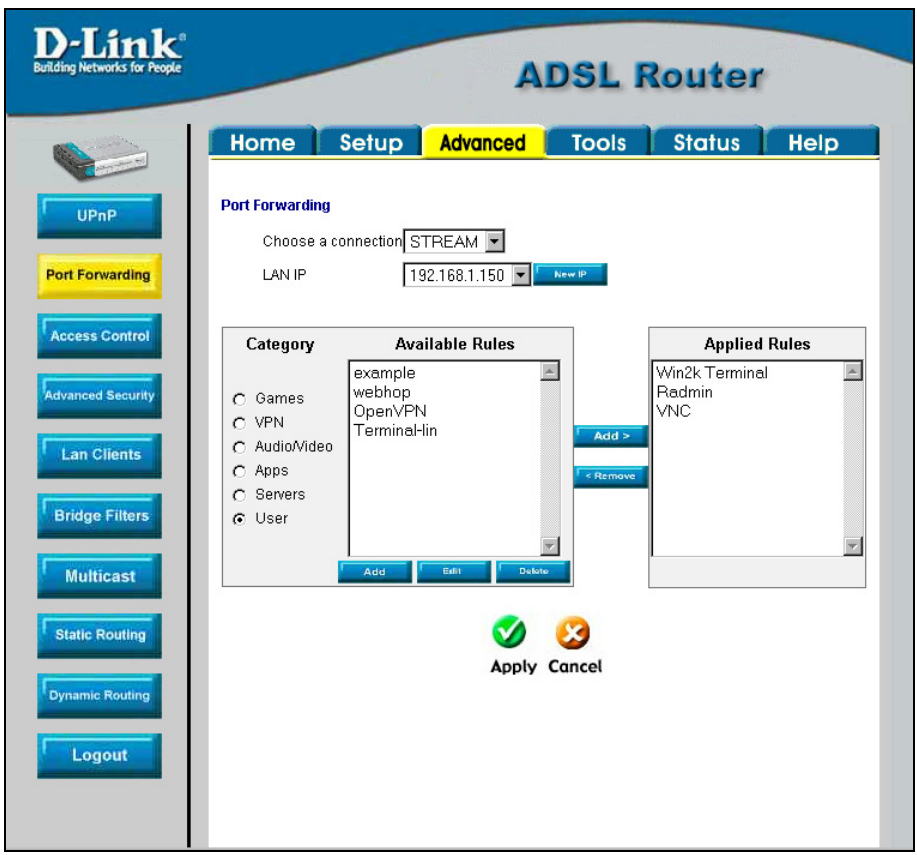


Рис. 2.13. Окно **ADSL Router**, вкладка **Advanced**, нажата кнопка **Port Forwarding**

На вкладке **Advanced** кнопкой **Advanced Security** (рис. 2.14) включается доступ к Web-серверу и Telnet-серверу, которые могут находиться в вашей сети, и может быть задан компьютер, к которому определен доступ из Интернета, но сам этот компьютер не имеет связи с вашей сетью (**Enable DMZ**).

Для этого компьютера маршрутизатором может быть создана демилитаризованная зона (DMZ), откуда невозможны внешние атаки на вашу сеть.

И, наконец, на вкладке **Advanced** кнопкой **Lan Clients** открывается страница, где можно указать IP-адреса компьютеров, к которым будет определен доступ извне (рис. 2.15).

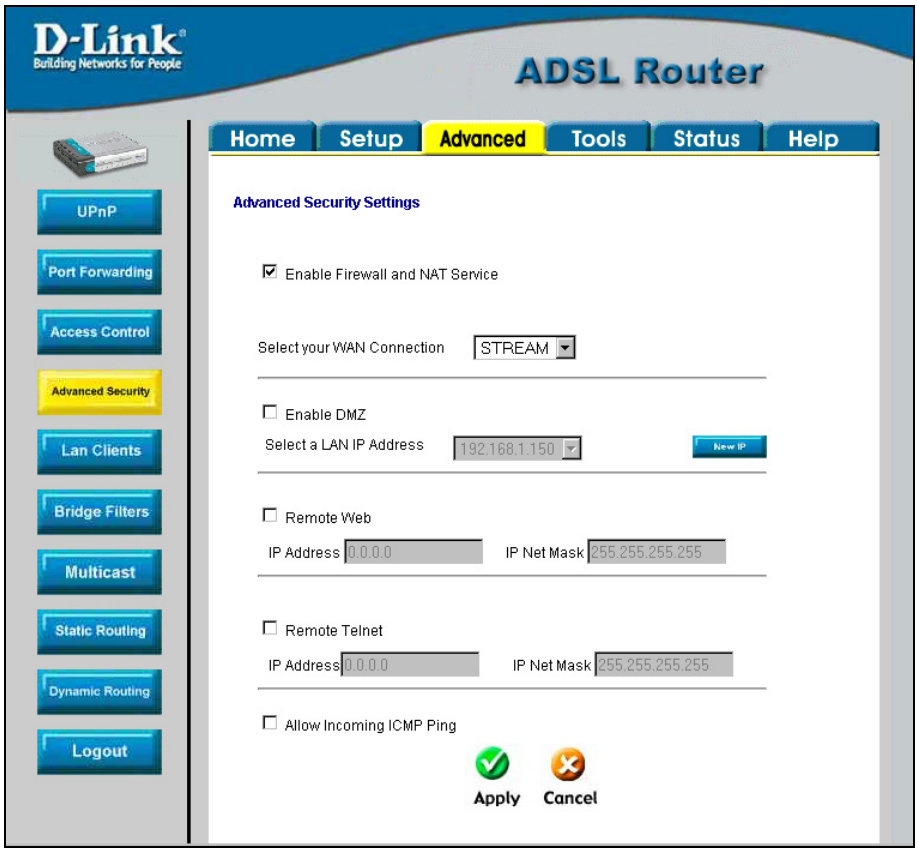


Рис. 2.14. Окно **ADSL Router**, вкладка **Advanced**, нажата кнопка **Advanced Security**

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 сведений будет недостаточно. Тогда вы сможете эти настройки указать самостоятельно.

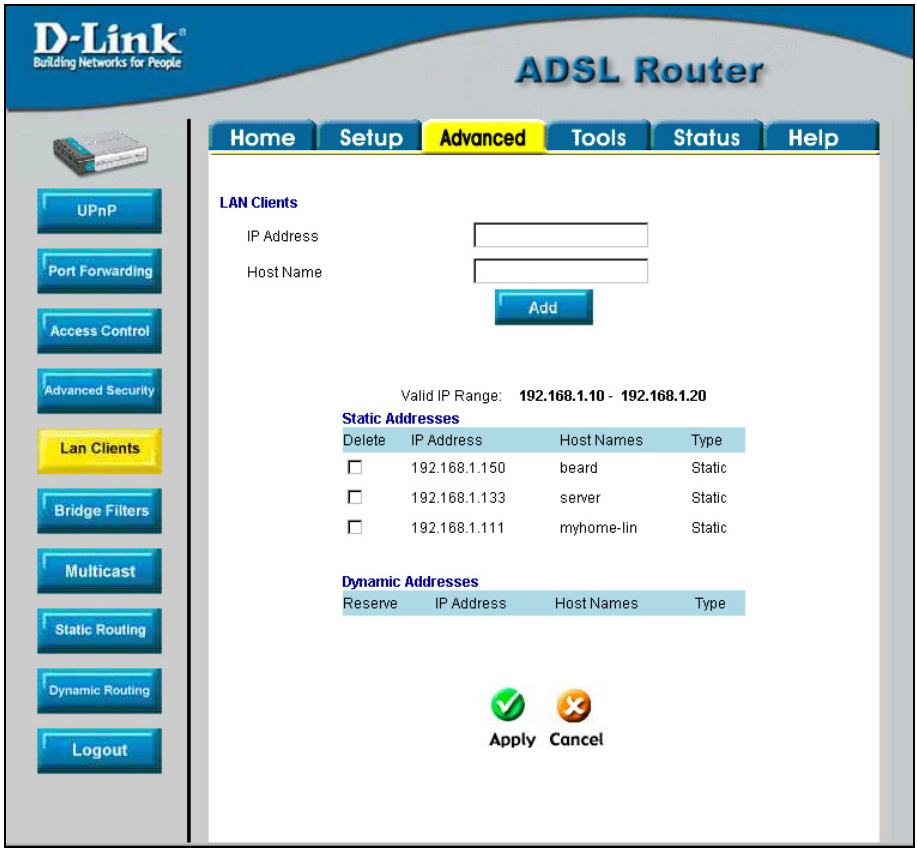


Рис. 2.15. Окно **ADSL Router**, вкладка **Advanced**, нажата кнопка **Lan Clients**

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.

Возможно, если доступно, и использование в качестве модема сотового телефона, если оператор сотовой связи предоставляет эту услугу. Рассмотрим

настройку доступа в Интернет через коммутируемое соединение в Windows и Linux.

В Windows

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

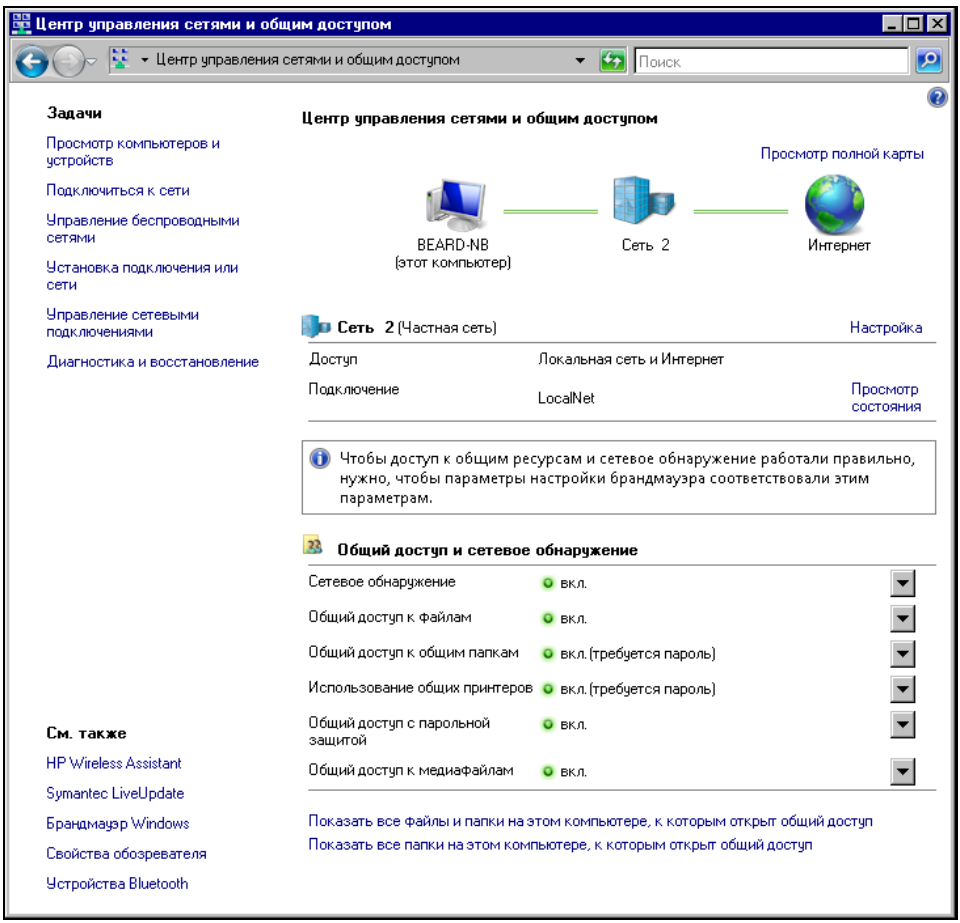


Рис. 2.16. Окно **Центр управления сетями и общим доступом**

В левой части окна **Центр управления сетями и общим доступом** (рис. 2.16) найдите задачу **Установка подключения или сети**. Щелкнув на этом пункте меню, откройте одноименное окно (рис. 2.17).

В этом окне выберите вариант подключения **Настройка телефонного подключения** и нажмите кнопку **Далее**.

В открывшемся окне **Настройка телефонного подключения** выберите установленный модем (рис. 2.18). В следующем окне (рис. 2.19) введите информацию о телефонном подключении, полученную от провайдера. Имя пользователя и пароль, необходимые для подключения, можно ввести через Internet Explorer, открыв меню **Сервис | Свойства обозревателя | Подключения | Настройка**.

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 данной машине.

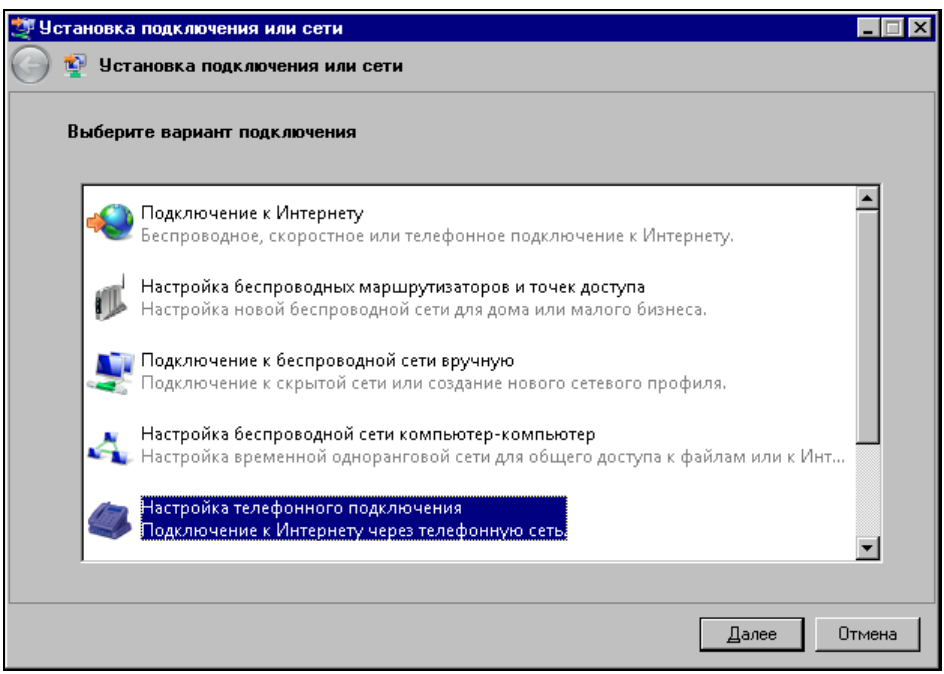


Рис. 2.17. Окно **Установка подключения или сети**

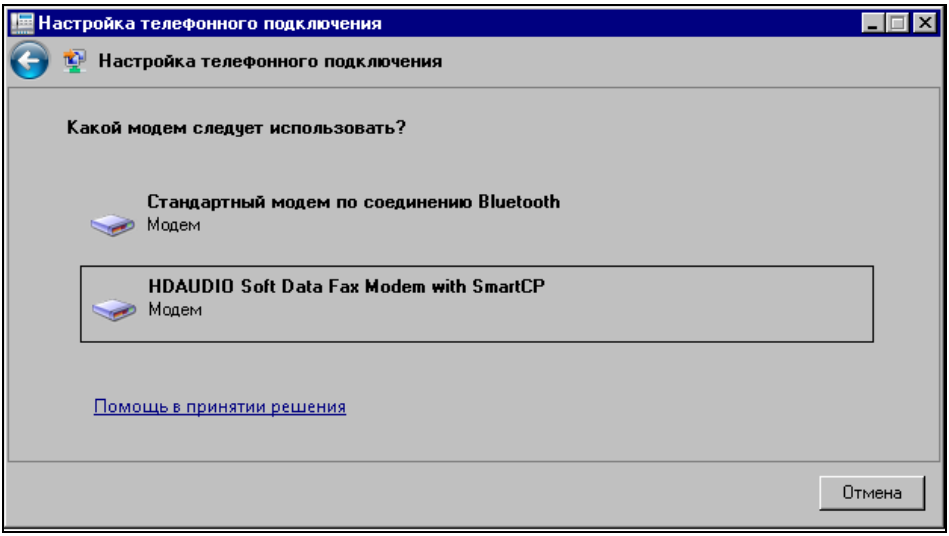


Рис. 2.18. Окно **Настройка телефонного подключения**: выбор модема

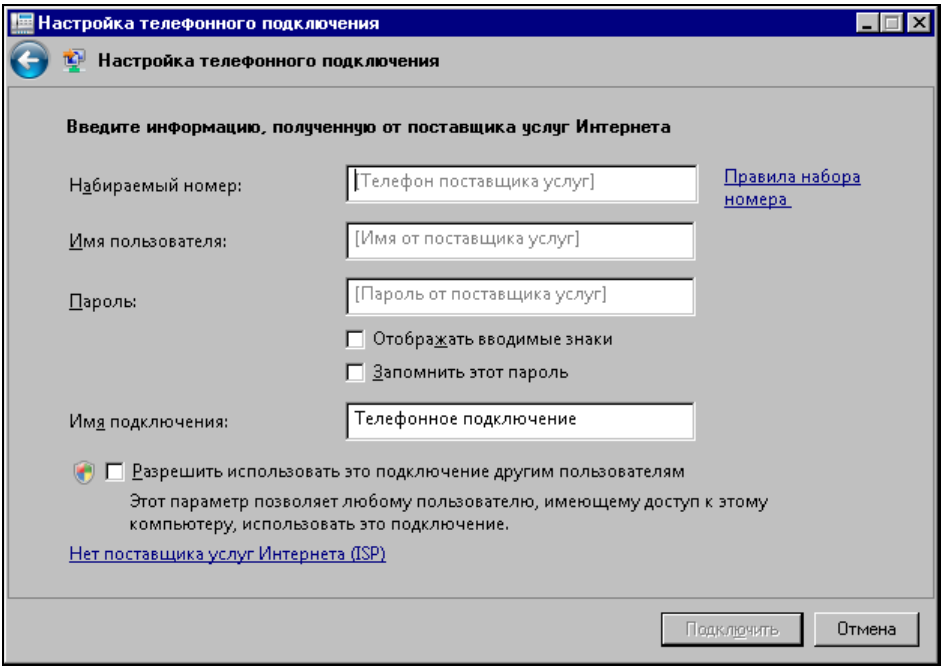


Рис. 2.19. Окно **Настройка телефонного подключения**: ввод информации

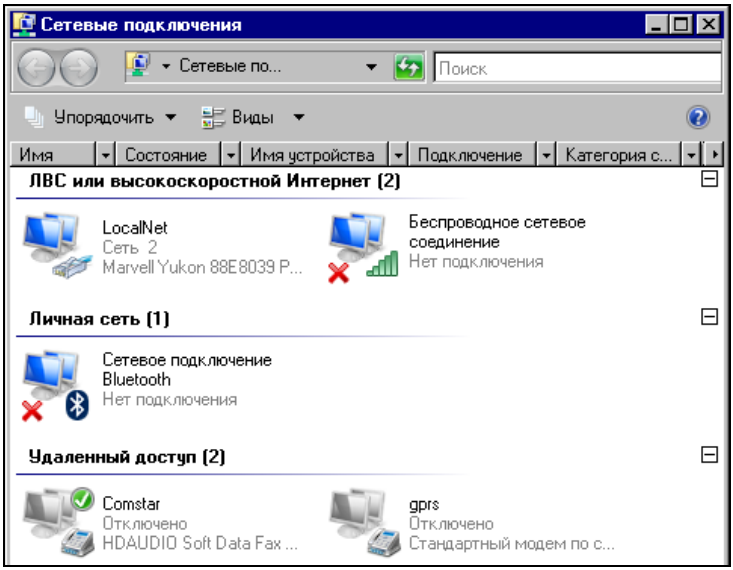


Рис. 2.20. Окно **Сетевые подключения**

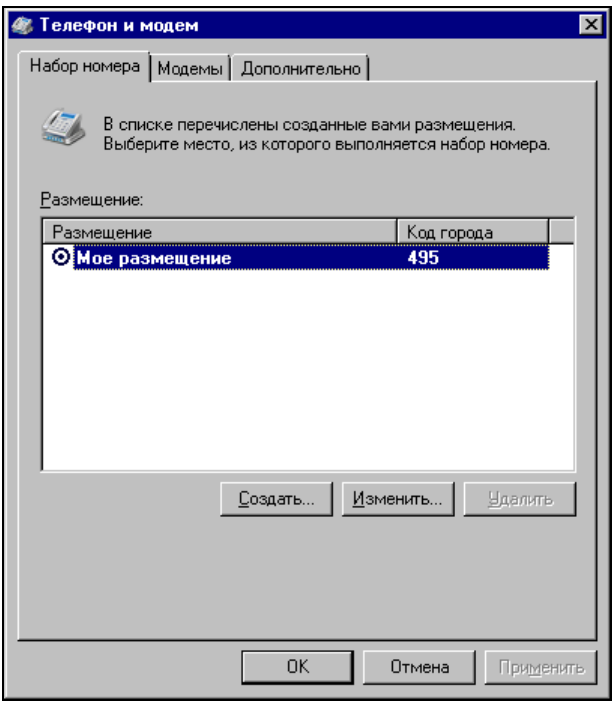


Рис. 2.21. Окно **Телефон и модем**, вкладка **Набор номера**

Созданное подключение появится в окне **Сетевые подключения** (рис. 2.20), которое можно найти по пути: **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 несложно. Найдите в Панели управления апплет **Телефон и модем** и откройте его.

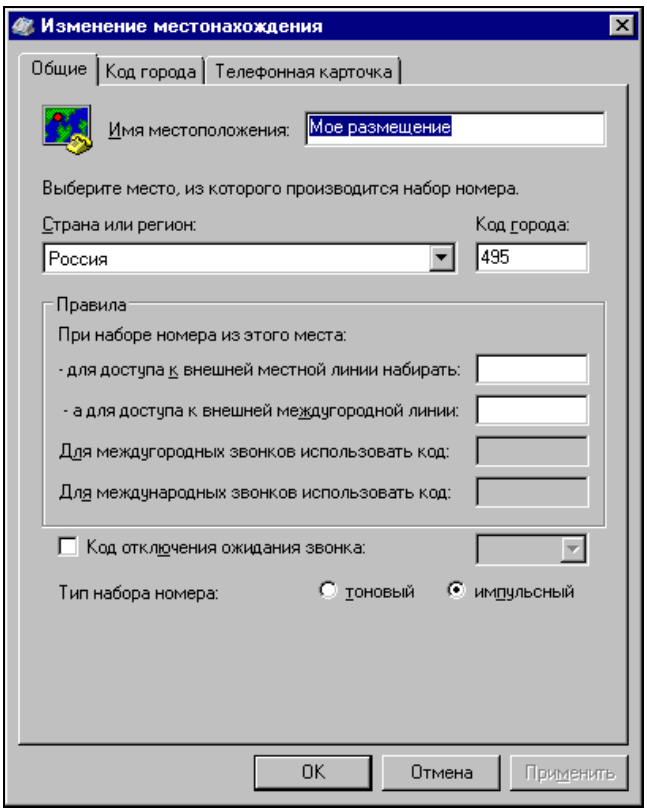


Рис. 2.22. Окно **Изменение местонахождения**

Окно откроется на вкладке **Набор номера** (рис. 2.21). Название размещения, которое вы увидите в поле **Размещение**, всегда можно изменить на желаемое. Но важно, чтобы это размещение было настроено в соответствии с ва-

шими местными условиями. Нажмите кнопку **Изменить...** и установите параметры размещения в открывшемся окне **Изменение местонахождения** (рис. 2.22).

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 по очереди кнопки **Применить** и **OK**.

Перейдите в окне **Телефон и модем** на вкладку **Модемы** и откройте окно свойств установленного в вашей системе модема. Нажмите кнопку **Опросить модем** и убедитесь, что модем отвечает на запросы системы.

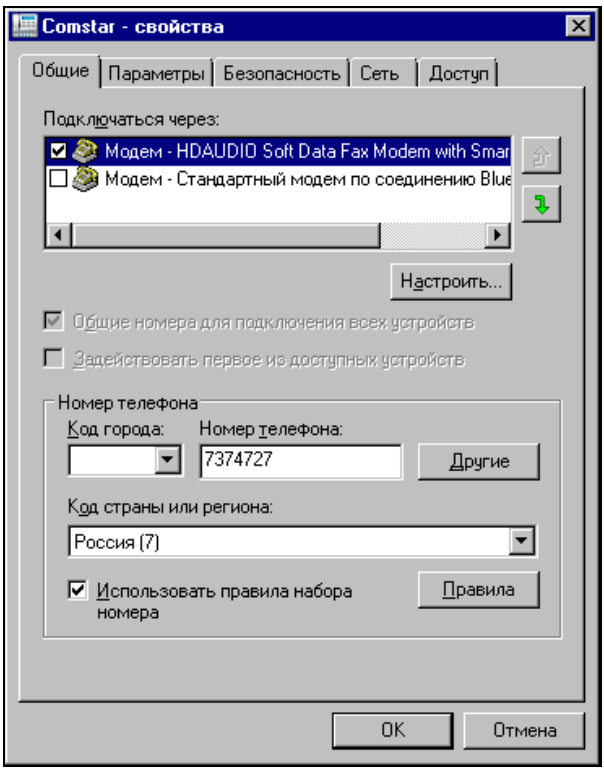


Рис. 2.23. Окно **Comstar - свойства**

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

правила, настраивая 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. 2.23).

На вкладке **Общие** установите флажок **Использовать правила набора номера**.

Перейдите на вкладку **Безопасность** (рис. 2.24) и отметьте флажок **Сценарий**. Сценарий потребуется потому, что при подключении к Интернету из сети некому будет вводить имя пользователя и пароль.

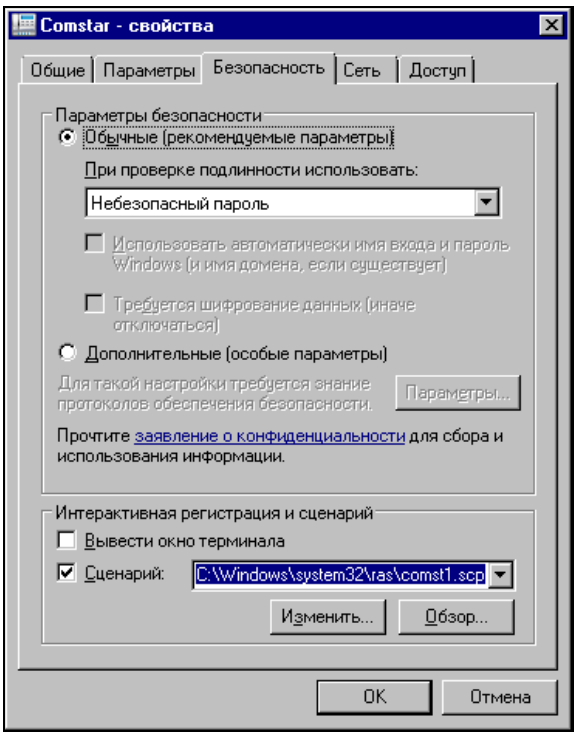


Рис. 2.24. Окно **Телефонное подключение - свойства**, вкладка **Безопасность**

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
```

Сохраните файл под любым именем, но с расширением scp.

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

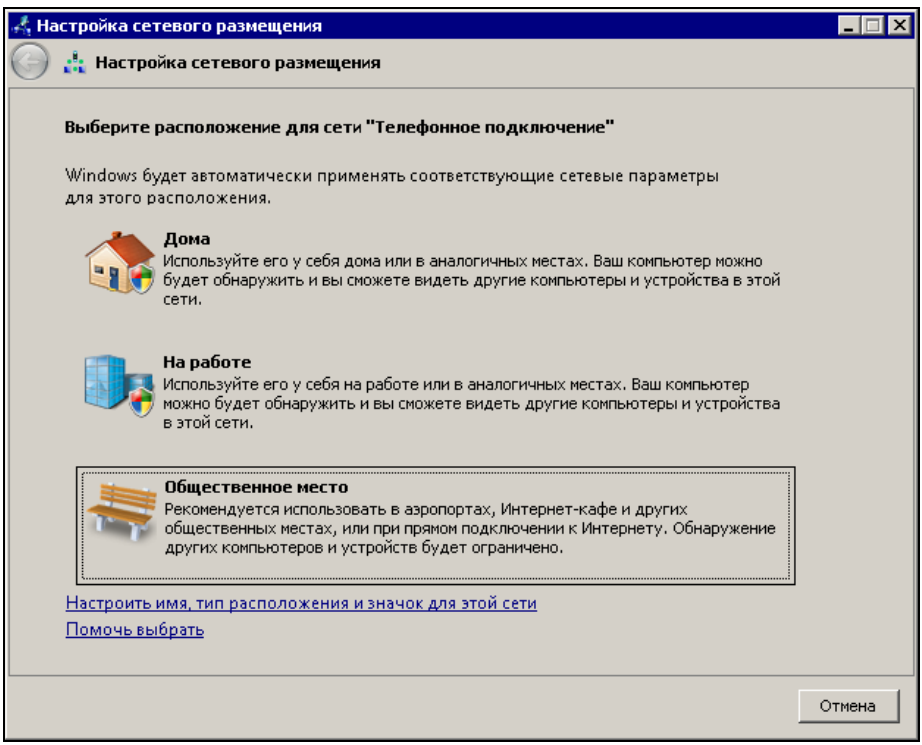


Рис. 2.25. Окно **Настройка сетевого размещения**

Закрыв окно свойств телефонного подключения, выберите команду **Подключить** в контекстном меню подключения. Если все параметры подключения введены верно, соединение должно установиться, но система предложит выбрать сетевое размещение (рис. 2.25).

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. 2.26) вы должны увидеть IP-адреса сервера и клиента.

Снова откройте окно свойств телефонного подключения, но на вкладке **Доступ** (рис. 2.27).

Отметьте в этом окне все флажки. Вы увидите сообщение системы, показанное на рис. 2.28.

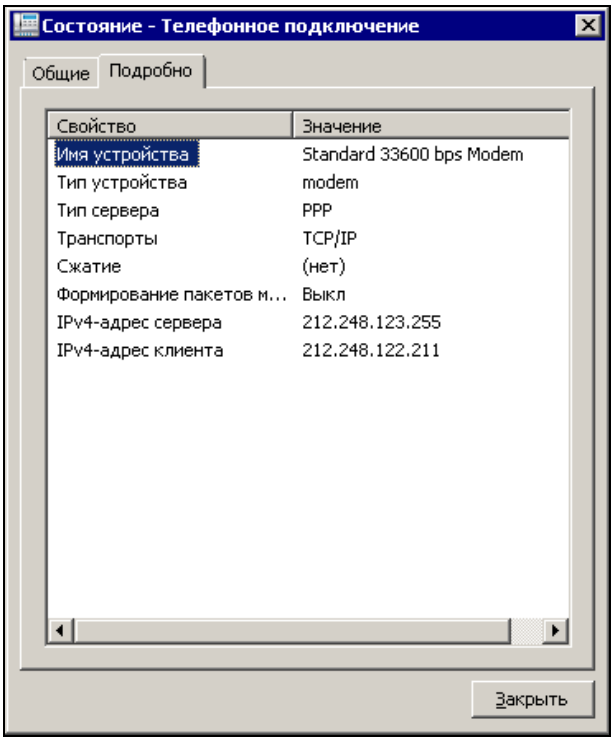


Рис. 2.26. Окно **Состояние - Телефонное подключение**

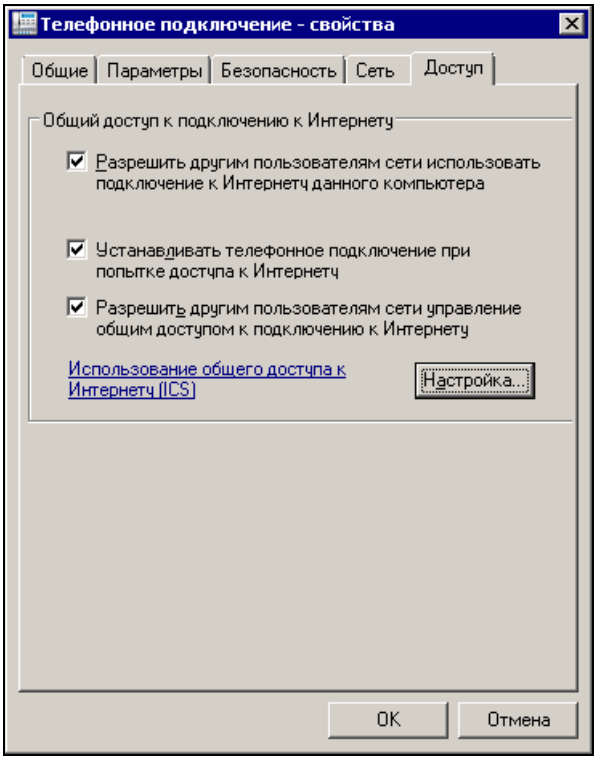


Рис. 2.27. Окно **Телефонное подключение - свойства**, вкладка **Доступ**

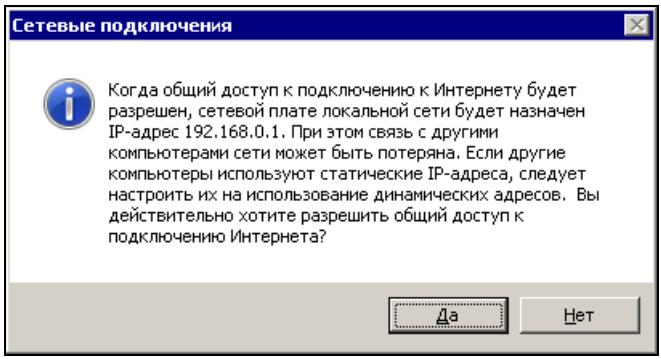


Рис. 2.28. Окно **Сетевые подключения** с сообщением

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 общего 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 укажите тот адрес DNS-сервера, что выдан провайдером, а IP-адреса компьютеров сети должны находиться в одной подсети.

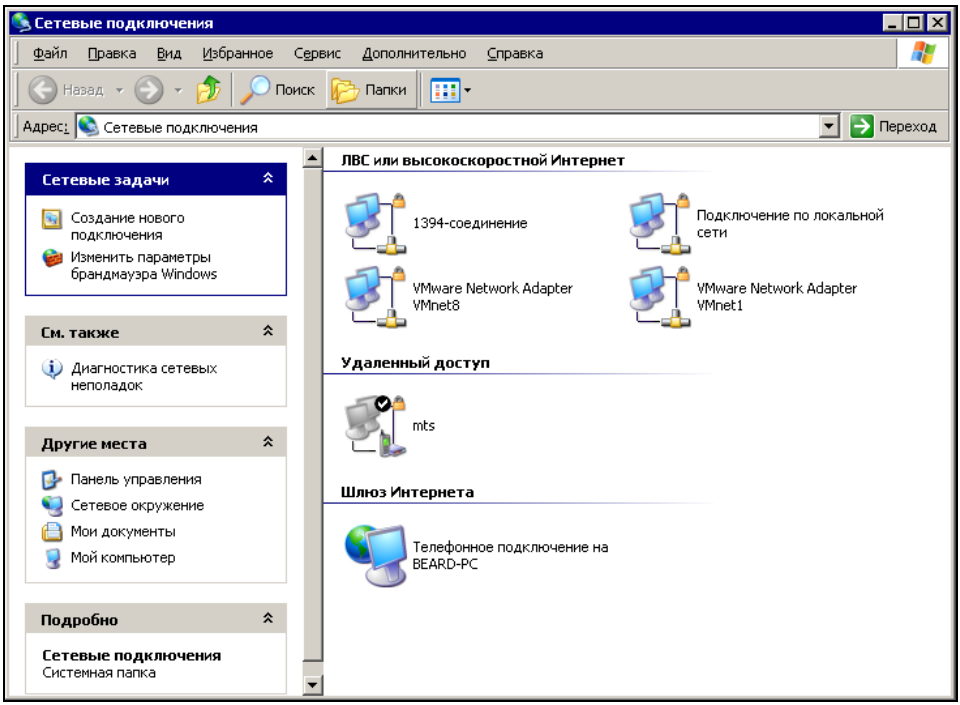


Рис. 2.29. Окно **Сетевые подключения** на других компьютерах сети

В окне **Сетевые подключения** на других компьютерах сети (рис. 2.29) 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 получат 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 соз-

дать пакетный файл с командой `rasdial` и настроить его запуск с помощью планировщика задач Windows (**Панель управления | Администрирование | Планировщик задач | Создать задачу**).

Команда *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 Linux

Подключение к Интернету настроим в Mandriva Linux. Надеемся, что настройки в других дистрибутивах Linux вы сможете выполнить по аналогии с теми, что рассматриваются в этой главе.

Подключите модем к компьютеру. Войдите в **Центр управления Mandriva Linux 2008.0**. Выберите в левой части окна меню **Сеть и Интернет** (рис. 2.30), после чего в правой части окна найдите значок утилиты **Настройка нового сетевого интерфейса** и откройте ее.

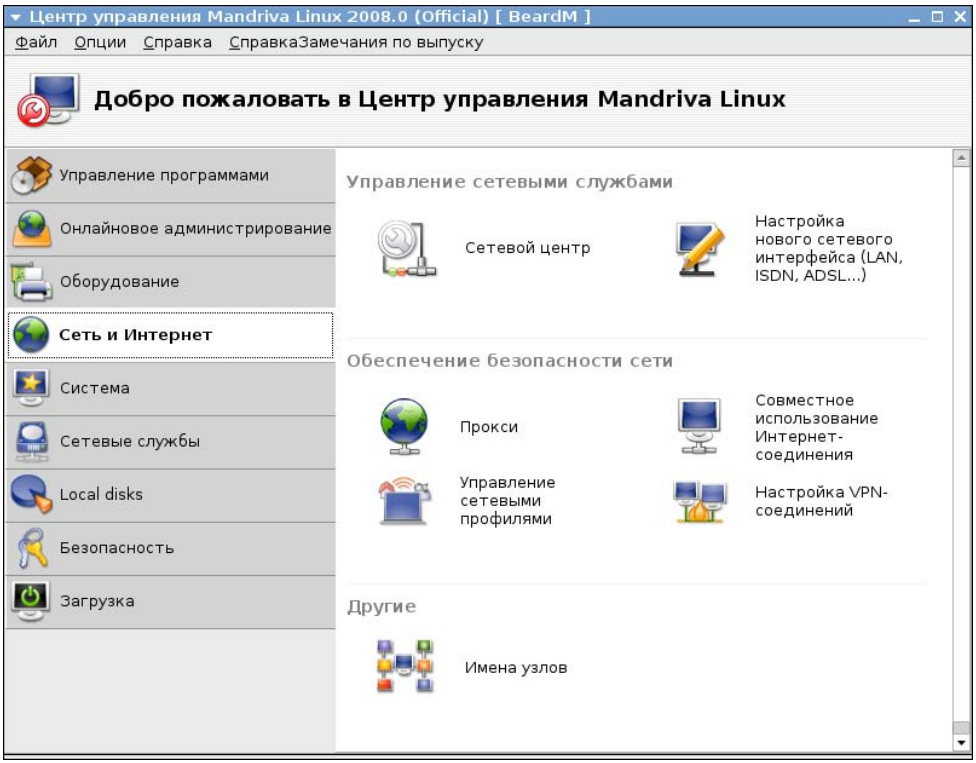


Рис. 2.30. Окно **Центр управления Mandriva Linux 2008.0**, раздел **Сеть и Интернет**

В открывшемся окне **Настройка нового сетевого интерфейса** (рис. 2.31) выберите сетевой интерфейс, который необходимо настроить, и нажмите кнопку **Далее**. В данном случае наш выбор — аналоговый телефонный модем.

В следующем окне возможен выбор модели модема (рис. 2.32). Если вы подключили полноценный аппаратный модем, то система его не определит и предложит самостоятельно выбрать модем для настройки.

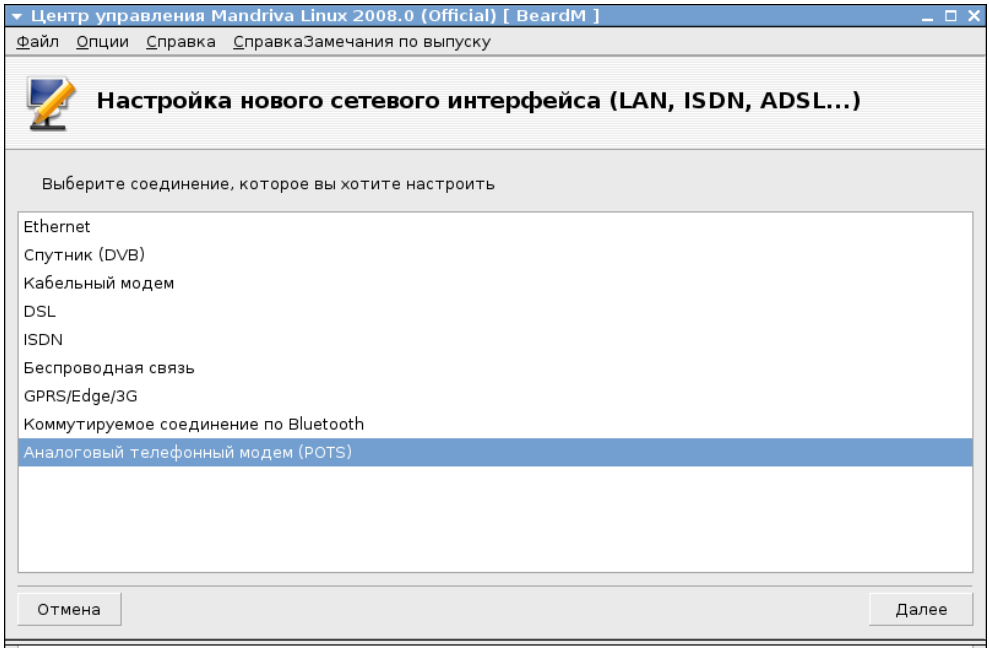


Рис. 2.31. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка нового сетевого интерфейса**: выбор настраиваемого соединения

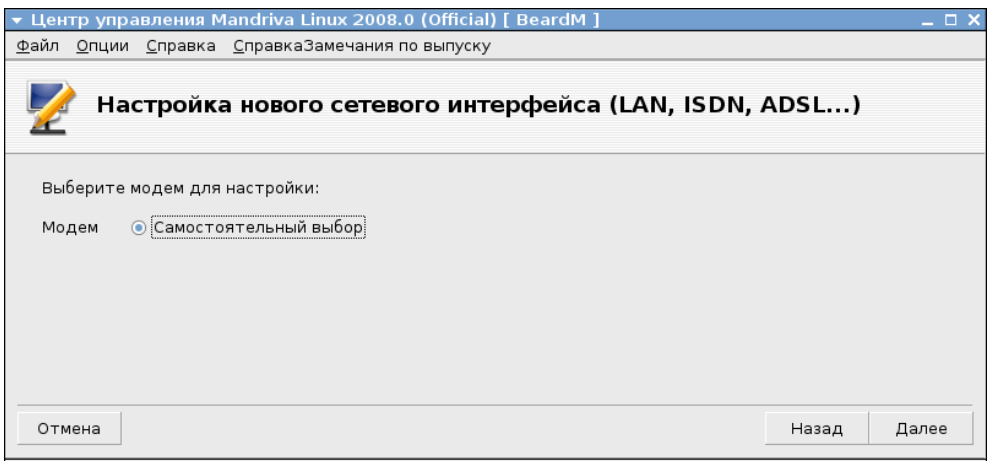


Рис. 2.32. Окно **Центр управления Mandriva Linux 2208.0**, страница **Настройка нового сетевого интерфейса**: выбор модема

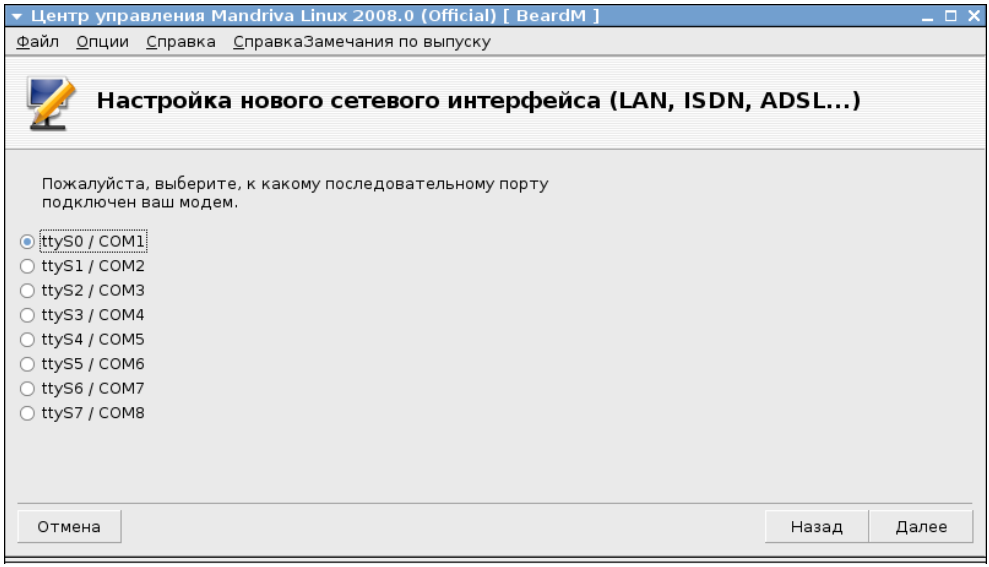


Рис. 2.33. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка нового сетевого интерфейса**: выбор порта модема

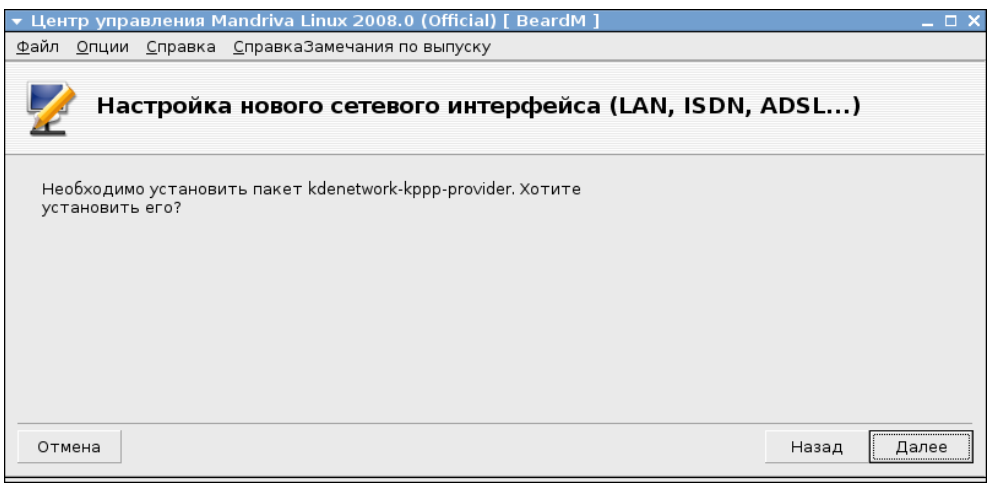


Рис. 2.34. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка нового сетевого интерфейса**: запрос на установку дополнительных пакетов

Теперь необходимо указать порт, к которому подключен модем. В данном случае это порт COM1. В Linux этому порту соответствует устройство `ttyS0` (рис. 2.33).

Может так случиться, что в системе недостает какого-либо пакета, система предложит установить его (рис. 2.34).

Далее появится окно (рис. 2.35) со списком возможных провайдеров. Российских провайдеров вы в нем не найдете, следовательно, будем редактировать вручную. В следующем окне (рис. 2.36) необходимо указать параметры учетной записи, которые вами получены у провайдера.

Далее необходимо указать параметры подключения (рис. 2.37). Оставим для всех параметров автоматическое получение.

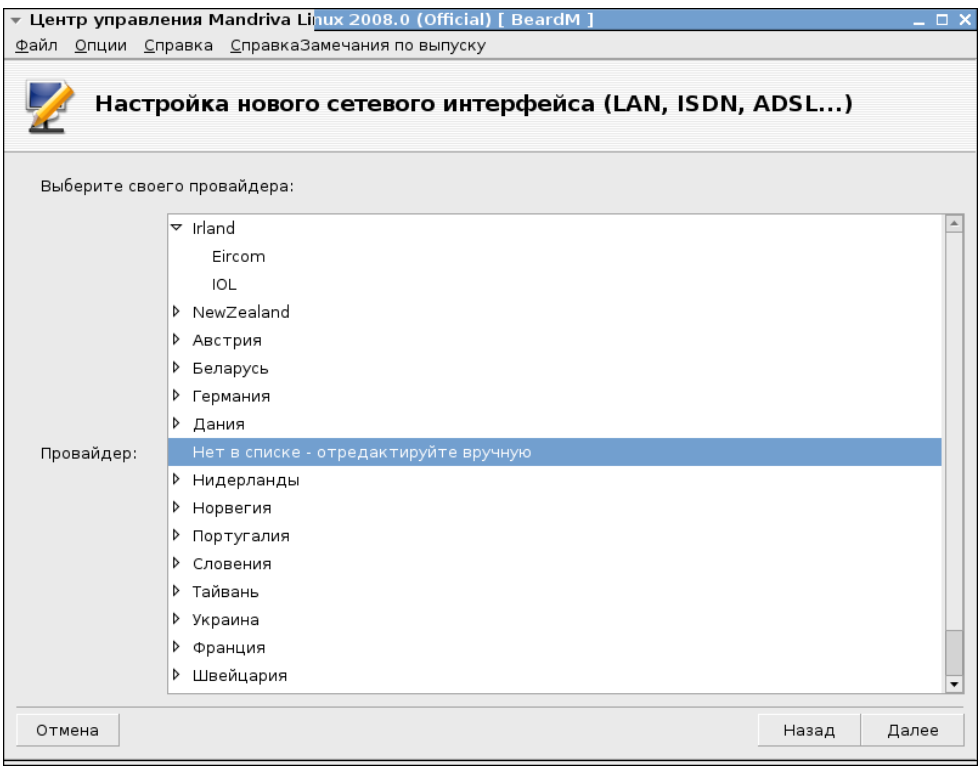


Рис. 2.35. Окно **Центр управления Mandriva Linux 2208.0**, страница **Настройка нового сетевого интерфейса**: выбор провайдера

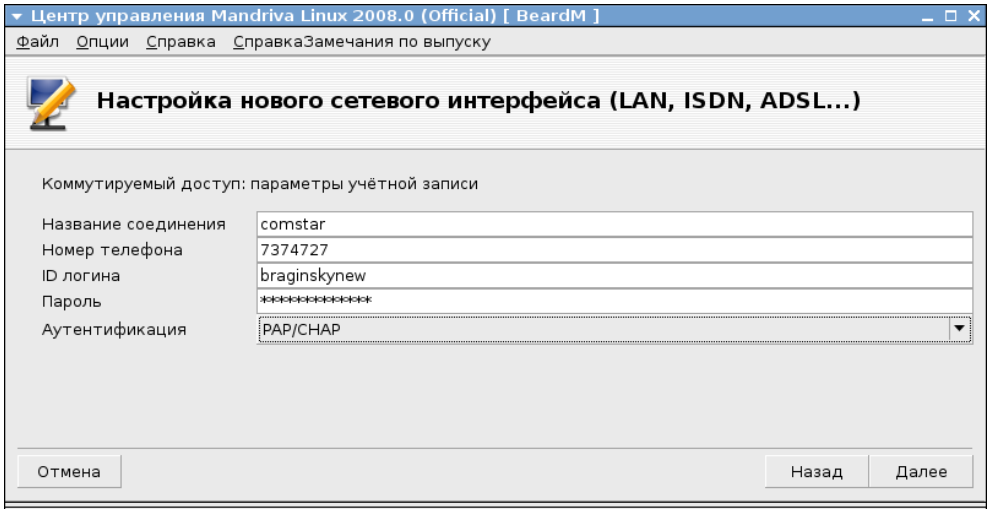


Рис. 2.36. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка нового сетевого интерфейса**: параметры учетной записи

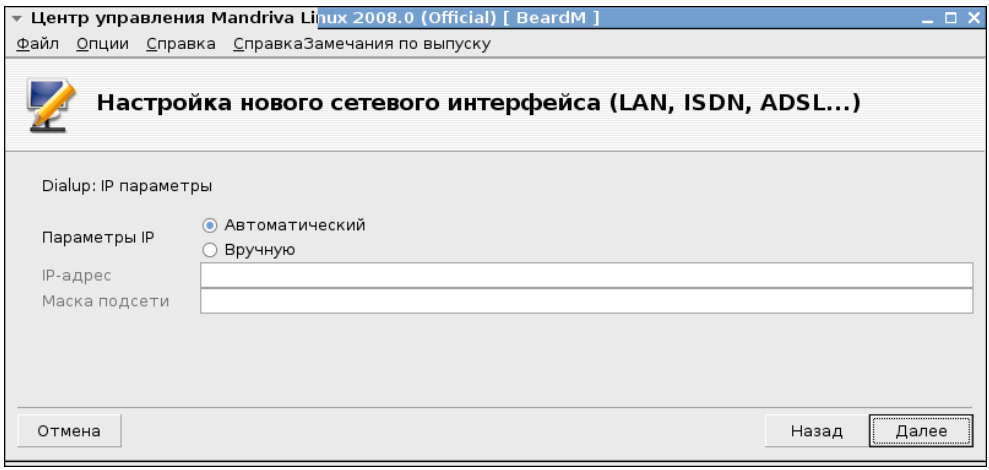


Рис. 2.37. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка нового сетевого интерфейса**: IP-параметры

Мы уже близки к завершению настройки подключения к Интернету через модемное соединение. В очередном окне (рис. 2.38) следует установить возможность управлять подключением, но не включать установку соединения при загрузке.

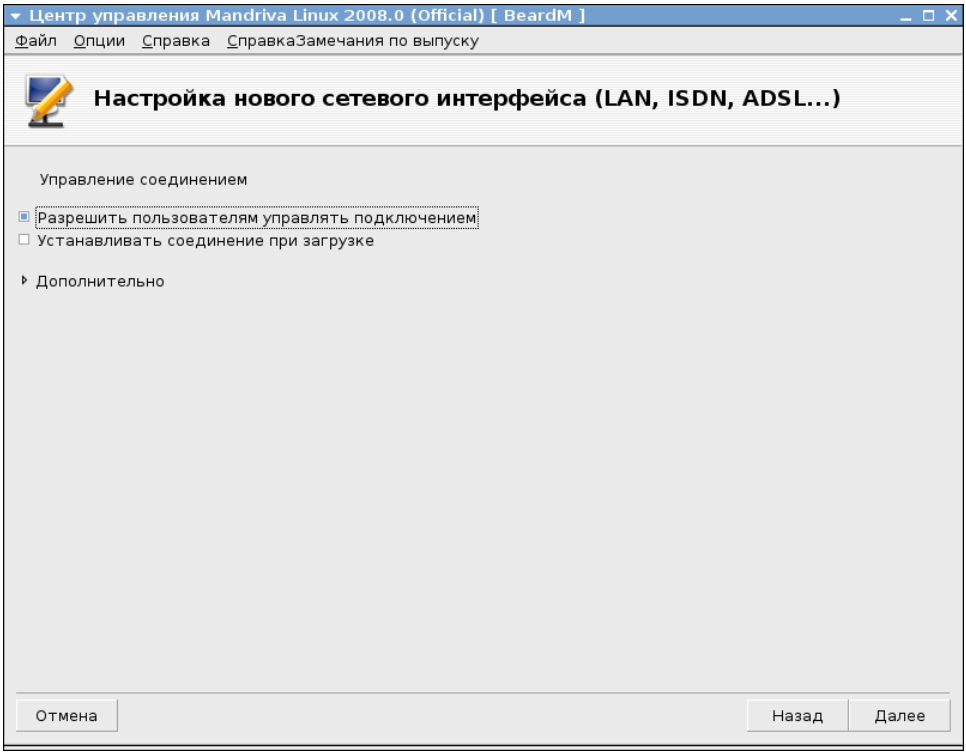


Рис. 2.38. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка нового сетевого интерфейса**: управление соединением

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. 2.39). Если она не установлена, то установите ее. 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 обра-

тимся к **Центру управления Mandriva Linux | Сеть и Интернет** (см. рис. 2.30). Если ваш модем распознан системой, то утилита **Совместное использование Интернет-соединения** (рис. 2.40) поможет выполнить настройку общего доступа.

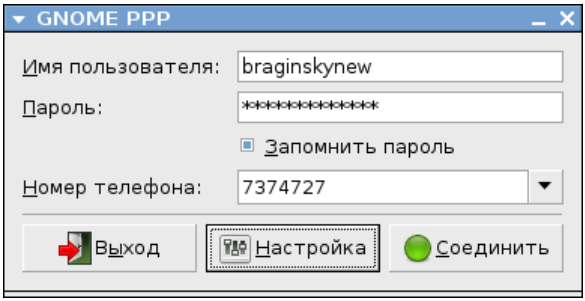


Рис. 2.39. Окно **GNOME PPP**

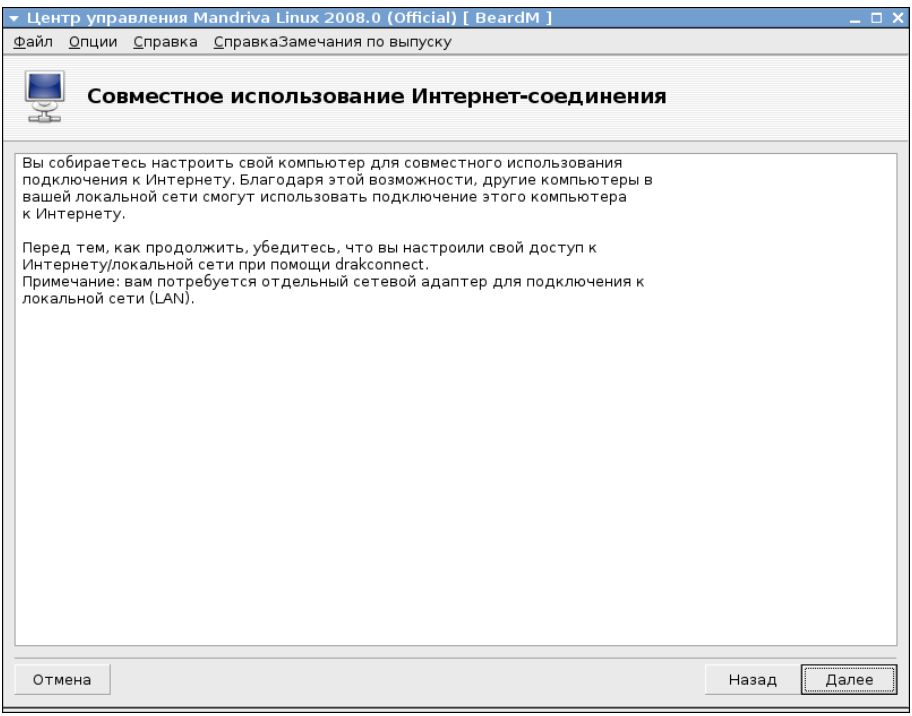


Рис. 2.40. Окно **Центр управления Mandriva Linux 2008.0**, страница **Совместное использование Интернет-соединения**

В следующем окне (рис. 2.41) 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).

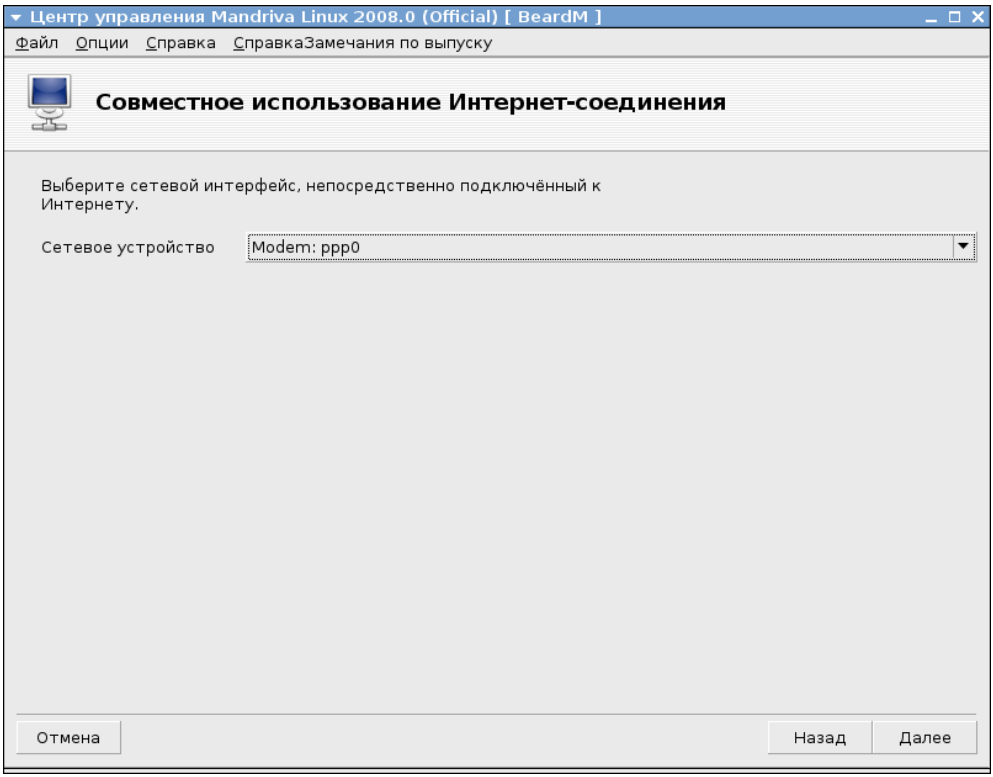


Рис. 2.41. Окно **Центр управления Mandriva Linux 2008.0**, страница **Совместное использование Интернет-соединения**: выбор сетевого интерфейса

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 на единицу.

> ***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.

Теперь выполните команду

```
/sbin/sysctl -p /etc/sysctl.conf
```

и перезагрузите компьютер. Маршрутизация теперь включена, и наш компьютер может быть шлюзом в Интернет.

Защита от внешних вторжений (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 непредсказуемы. 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 (от англ. *firewall*) и брандмауэры.

Брандмауэр Windows

Для того чтобы защитить компьютер от несанкционированного доступа к нему, в состав Windows Vista 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 можно изменить настройки защиты.

Получить доступ к настройкам Брандмауэра Windows можно, открыв из окна **Центр обеспечения безопасности Windows** окно **Брандмауэр Windows** (рис. 2.42), воспользовавшись соответствующим пунктом меню.

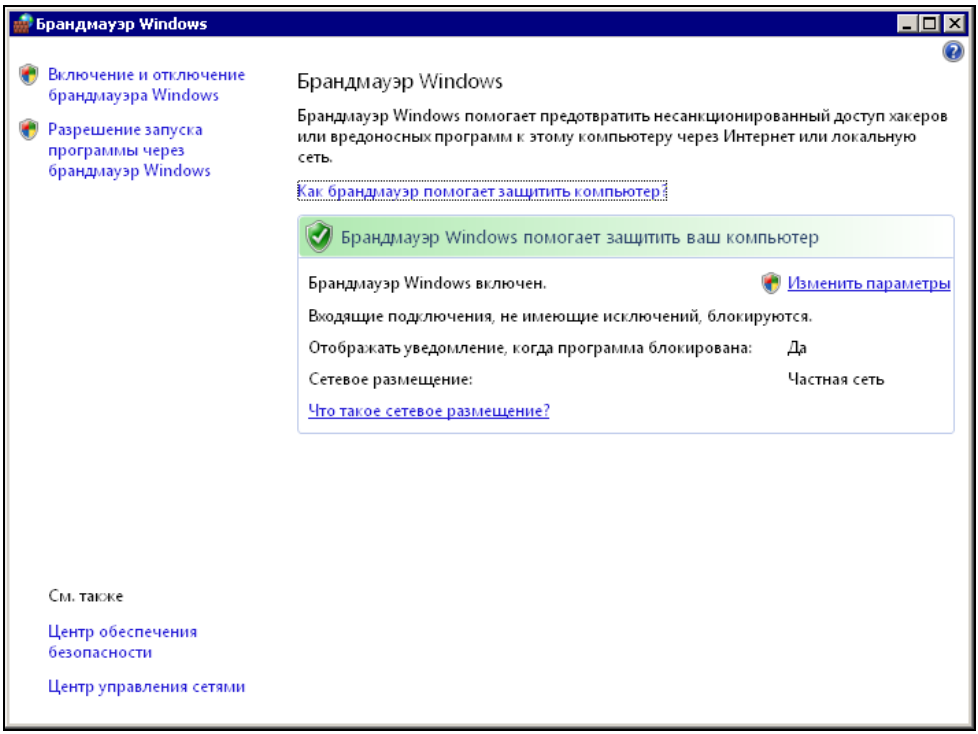


Рис. 2.42. Окно **Брандмауэр Windows**

Воспользовавшись ссылкой **Изменить параметры**, имеющейся в этом окне, можно открыть окно **Параметры брандмауэра Windows** (рис. 2.43) с тремя вкладками, на каждой из которых можно выполнить определенные настройки.

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

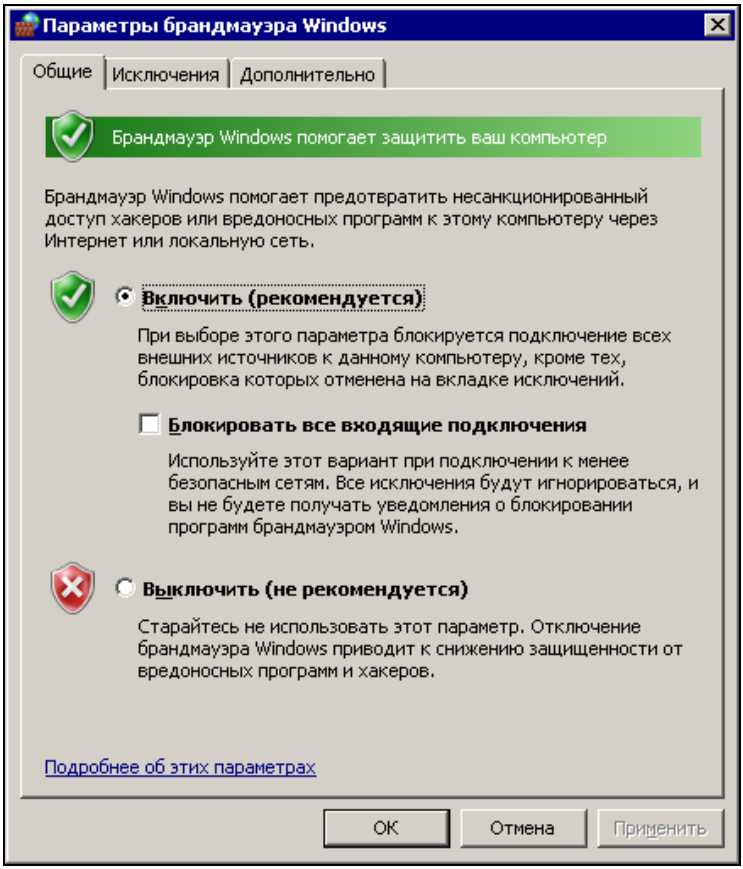


Рис. 2.43. Окно **Параметры брандмауэра Windows**, вкладка **Общие**

На вкладке **Дополнительно** (рис. 2.44) 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.

На вкладке **Исключения** (рис. 2.45) 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. 2.46).

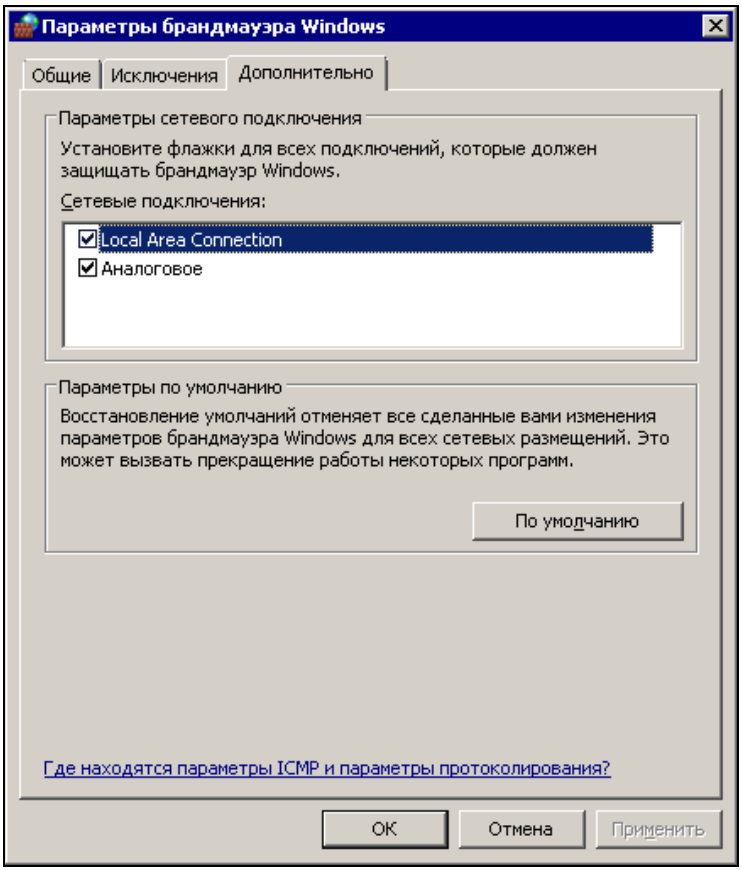


Рис. 2.44. Окно **Параметры брандмауэра Windows**, вкладка **Дополнительно**

Но исходя из соображений безопасности, вы 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. 2.47).

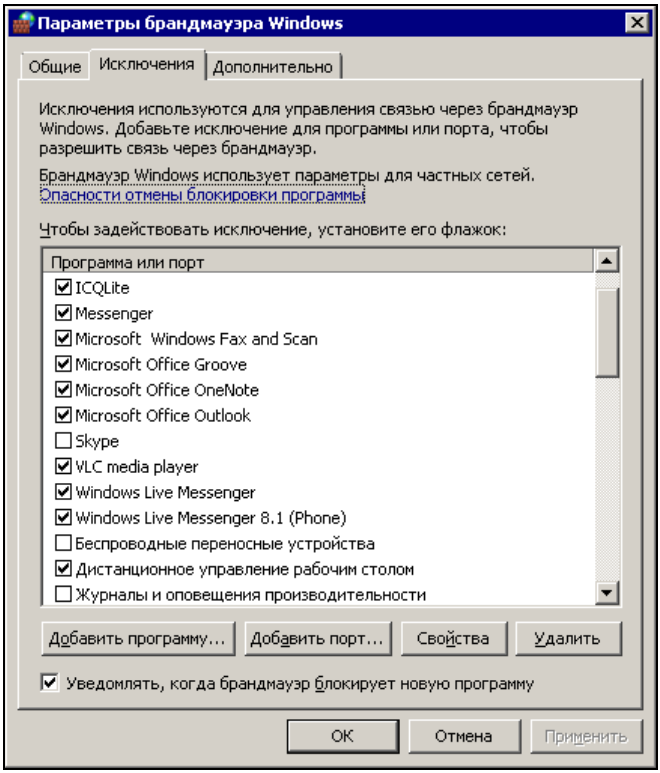


Рис. 2.45. Окно **Параметры брандмауэра Windows**, вкладка **Исключения**

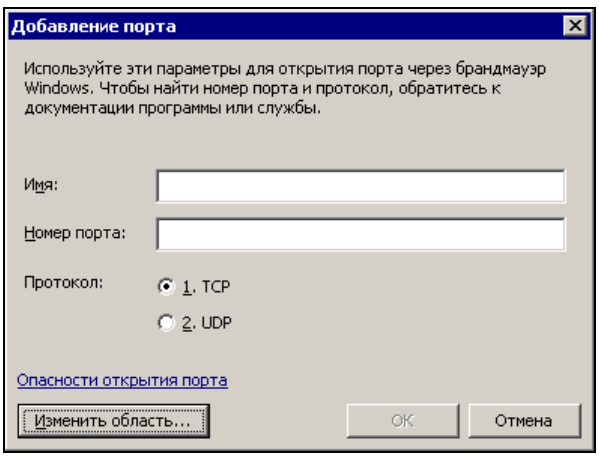


Рис. 2.46. Окно **Добавление порта**

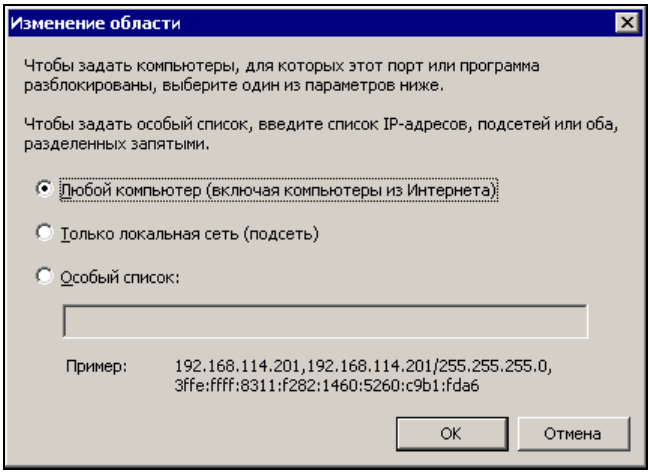


Рис. 2.47. Окно **Изменение области**

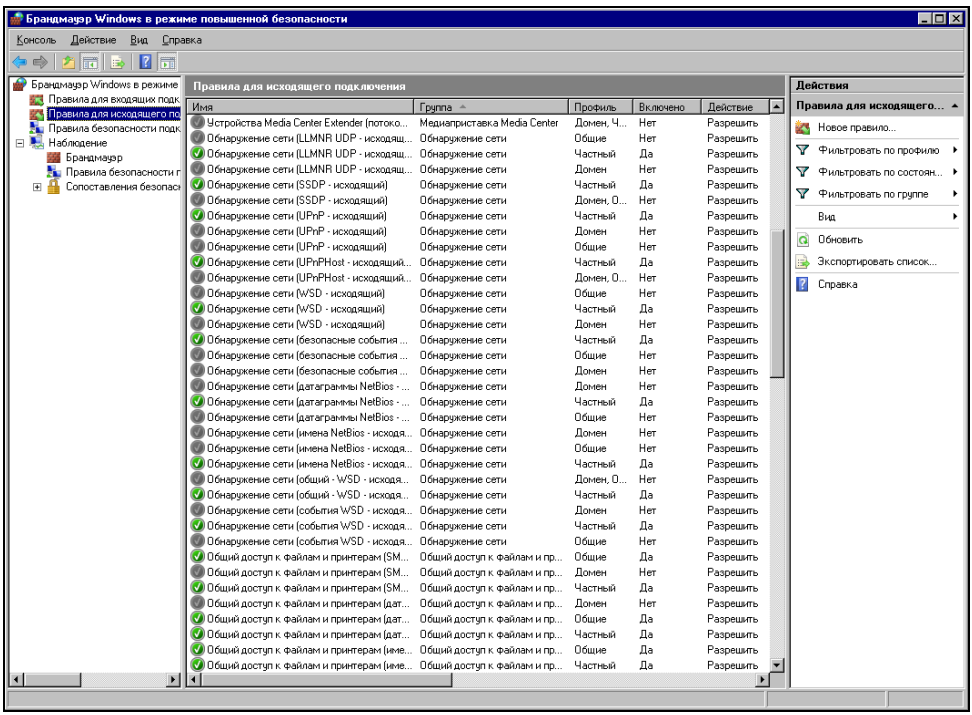


Рис. 2.48. Окно
Брандмауэр Windows в режиме повышенной безопасности

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. 2.48). 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 **Центр управления Mandriva Linux** и выберите пункт **Безопасность** в левой части окна (рис. 2.49).

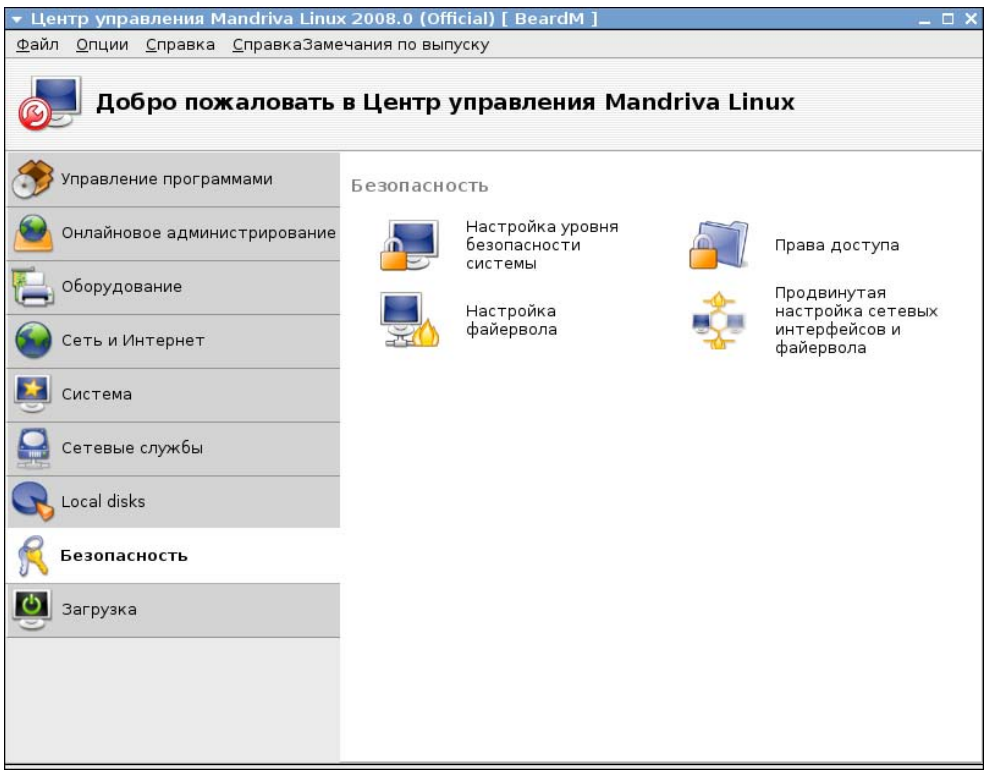


Рис. 2.49. Окно **Центр управления Mandriva Linux 2008.0**, раздел **Безопасность**

В правой части откройте утилиту **Настройка файервола**. На отрывшейся одноименной странице (рис. 2.50) 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 кнопку **OK** и в появившемся окне (рис. 2.51) выберите службы, обращение к которым будет сопровождаться сообщением.

В следующем окне (рис. 2.52) отметьте интерфейсы, которые необходимо защитить.

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

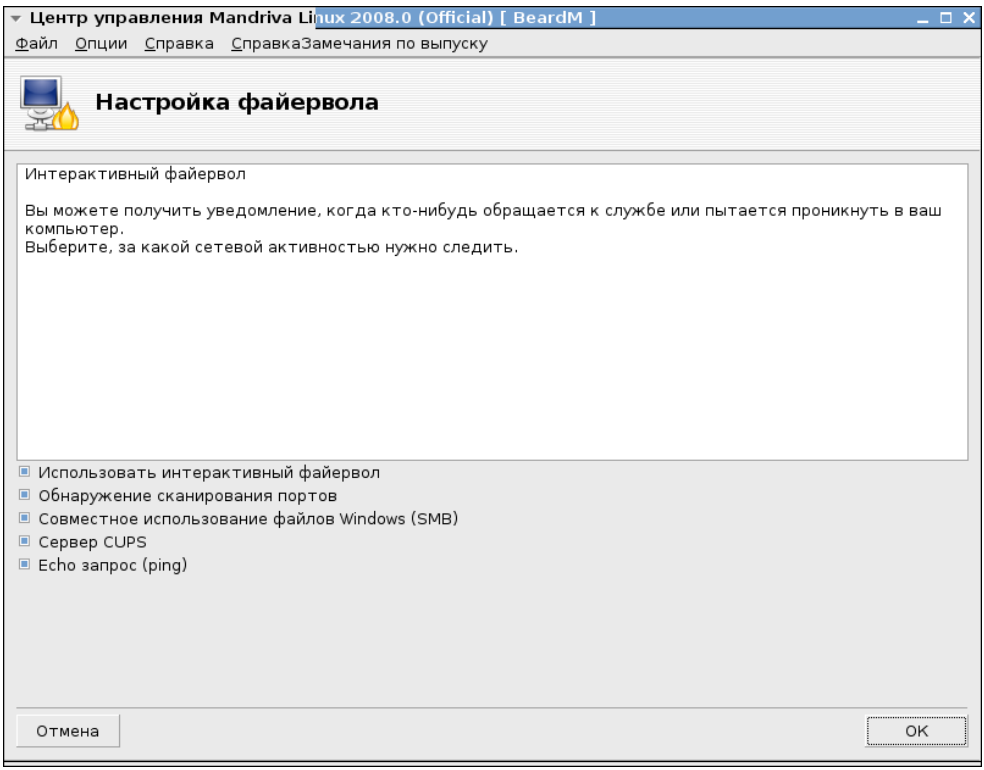


Рис. 2.50. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка файервола**: выбор служб

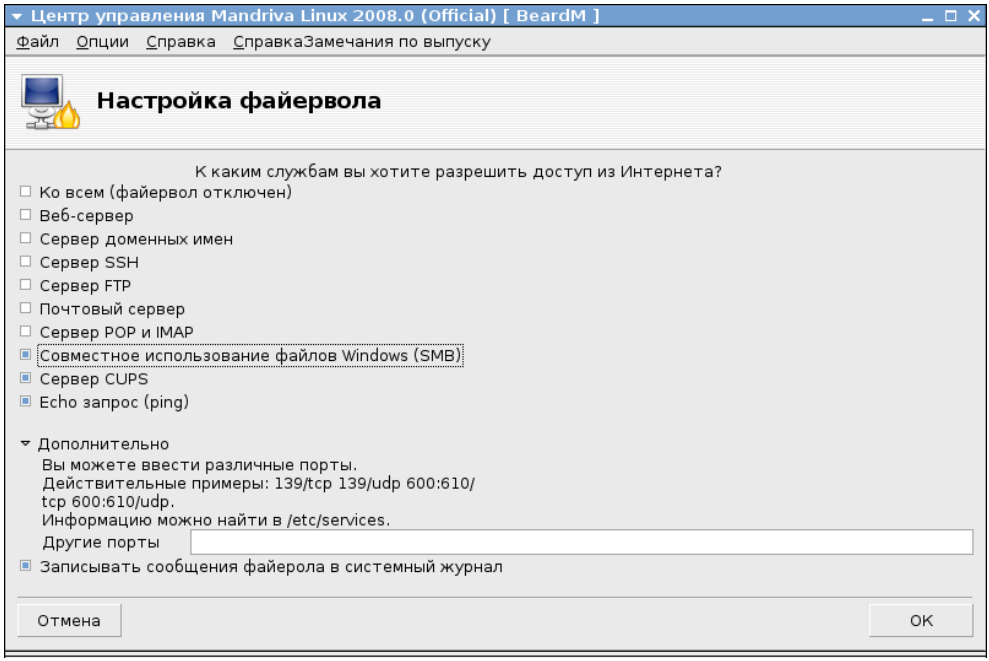


Рис. 2.51. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка файервола**: интерактивный файервол

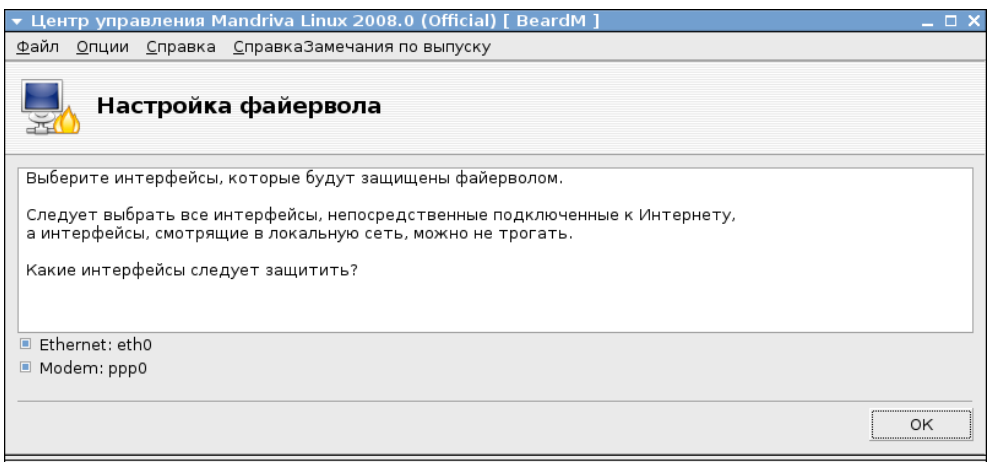


Рис. 2.52. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка файервола**: выбор защищаемых интерфейсов

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 Linux.

"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 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 Vista, а для Windows написано несколько десятков тысяч вирусов. Конечно, можно соблюдать правила, приведенные выше при работе в Windows Vista, 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 налету. 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 Интернете через Linux. Эта ОС 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. Какую же программу выбрать? Многие пользователи Windows хотели бы найти бесплатную антивирусную программу. И такая программа есть. Она не имеет ограничений по времени использо-

вания, обновляет через Интернет свои базы и совершенно легально 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 флэш-носителя (**http://portableapps.com/apps/utilities/clamwin_portable**).

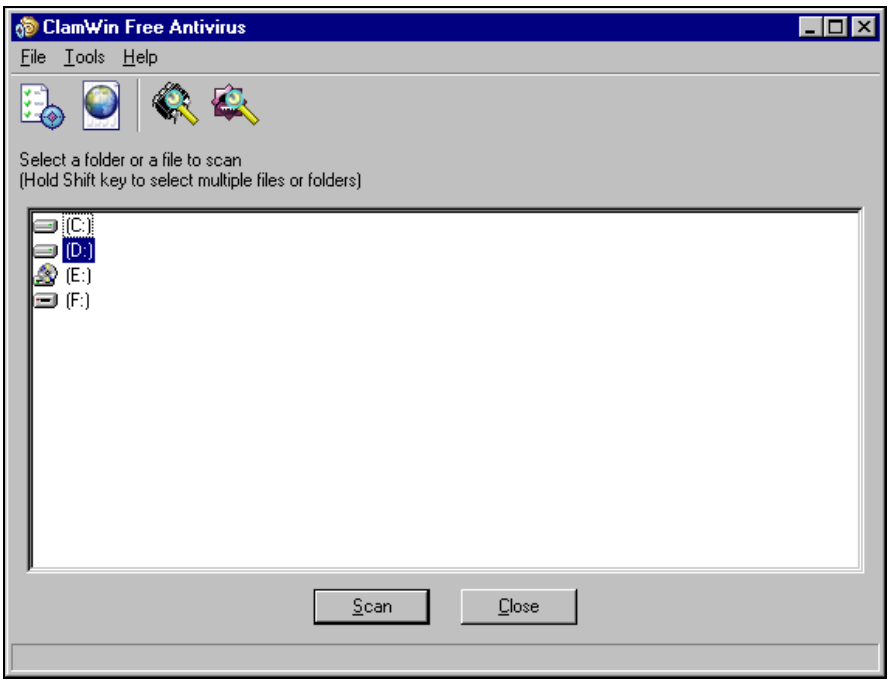


Рис. 2.53. Окно **ClamWin Free Antivirus**

Интерфейс программы английский, но очень простой (рис. 2.53). Четыре кнопки под меню окна позволяют (в порядке расположения) вызвать настройки программы, обновить антивирусные базы, сканировать память компьютера, сканировать 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/**.

Об организации беспроводной сети

Беспроводная сеть дает определенную свободу размещения компьютеров на вашей площади. Это особенно полезно для ноутбуков. Имея беспроводную сеть, вы можете предоставить к ней доступ гостям с ноутбуками, снабженными беспроводными адаптерами. Настройка беспроводной сети требует определенного внимания к ее безопасности. Ведь в ней может появиться компьютер, который вы сами не проверяли на наличие вирусов, например. Поэтому и рассматриваем мы этот вариант организации вашей малой сети уже после вопросов обеспечения защиты ваших компьютеров.

Не только ноутбуки могут иметь такое подключение. Кто мешает подключить без проводов обычную рабочую станцию? Существуют также беспроводные медиаплееры и другие устройства, которые можно подключать к сети. Проведя в квартиру кабель домовой сети или организовав доступ в Интернет через ADSL-модем, вы можете и не прокладывать по квартире кабели для обеспечения работы всех домашних компьютеров. Достаточно приобрести средства радиодоступа к сети. В последнее время таких средств выпускается все больше и больше. Качество соединений и их безопасность повышаются.

Оборудование

Какой тип оборудования вы будете применять в своей практике, зависит от ваших потребностей и возможностей. Рассматривая следующий пример, мы совершенно не настаиваем на использовании именно такого оборудования. Просто в нашем распоряжении оказался именно этот комплект, на базе которого был подготовлен пример. Комплект был приобретен обычным пользователем ПК для организации доступа к домовой сети и Интернету с ноутбука.

В состав комплекта входило следующее оборудование.

- Модем D-Link DFM-562E (рис. 2.54). 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 дает возможность пользователю путешествовать по Интернету и получать доступ к почтовому серверу. В дополнение к

коммуникационному программному обеспечению, совместимому с AT-командами, модем DFM-562E предлагает средства передачи и приема факсов на скорости до 14,4 Кбит/с. Модем выполняет V.42bis и MNP 2—4 сжатие данных и коррекцию ошибок для быстрого и надежного приема/передачи.

Рис. 2.54. Вид модема D-Link DFM-562E

В примере не описываются настройки модема, поскольку для большинства модемов они похожи. Но если будет необходимость применения модема совместно с маршрутизатором, который используется в примере, то желательно, чтобы оба устройства были от 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.

- Беспроводной адаптер D-Link DWL-G122 USB стандарта 802.11g (рис. 2.55), который используется для соединения компьютера с высокоскоростной беспроводной сетью. Этот адаптер легко подключается к компьютеру через быстрый порт USB 2.0 и обеспечивает скорость беспроводного соединения до 54 Мбит/с. DWL-G122 поддерживает стандарт взаимодействия 802.11g, сохраняя обратную совместимость с устройствами 802.11b, и обеспечивает установку Plug and Play. Адаптер DWL-G122 обеспечивает скорость передачи данных до 54 Мбит/с при совместной работе с другими беспроводными устройствами стандарта 802.11g. Это выгодно отличает его от адаптеров 802.11b, которые работают только на скорости до 11 Мбит/с. Как и устройства 802.11b, DWL-G122 использует один диапазон частот — 2,4 ГГц, избегая сложностей, присущих

двухдиапазонным сетям. Совместимость стандарта 802.11g с существующими стандартами беспроводных сетей означает, что нет необходимости менять все сетевое оборудование для поддержки соединения. DWL-G122 и другие устройства стандарта 802.11g можно постепенно добавлять в существующую сеть, в то время как остальное оборудование сети сможет продолжать взаимодействовать. Реализация Wi-FI Protected Access в DWL-G122 предоставляет необходимые протоколы и средства обеспечения безопасности, поэтому пользователи могут общаться между собой с сохранением конфиденциальности, а при получении доступа к важной информации компании или передаче данных динамически выполняется шифрование данных. WPA обеспечивает авторизацию и идентификацию пользователей на основании секретного ключа, который автоматически меняется по истечении некоторого периода времени. 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, что 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.

Рис. 2.55. Вид адаптера D-Link DWL-G122 USB

- Беспроводной 802.11g VPN-маршрутизатор DI-824VUP+, объединяющий функции широкополосного доступа в Интернет с надежной VPN-защитой межсетевым экраном, встроенным принт-сервером и 4-портовым коммутатором для подключения принтера и рабочих станций (рис. 2.56). Маршрутизатор обеспечивает высокую скорость передачи по беспроводной

сети, безопасные VPN-подключения, расширенную защиту межсетевым экраном и фильтрацию содержимого пакетов, основанную на политиках. Это устройство предоставляет экономичный способ установки безопасной и быстродействующей сети с каналом связи без узких мест к внешнему миру. Благодаря встроенной беспроводной точке доступа, 4-портовому коммутатору 10/100 Мбит/с и принт-серверу 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+ обеспечивается пропускная способность в 10 раз выше, чем у стандарта 802.11b. При работе с другими устройствами 802.11g, DI-824VUP+ поддерживает передачу данных на скорости до 54 Мбит/с. Маршрутизатор совместим со всеми беспроводными устройствами стандарта 802.11b/b+. Маршрутизатор имеет встроенную поддержку VPN, что позволяет создавать множество туннелей IPSec для удаленных офисов. Реализация IPSec использует шифрование DES, 3DES, AES и управление ключами Automated Key Management согласно спецификации IKE/ISAKMP. Туннель VPN может быть активирован от маршрутизатора к удаленному офису или мобильному пользователю для безопасной передачи потока данных с 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 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 со-

вместно использовать один, видимый извне IP-адрес и в то же время останутся защищенными от атак хакеров. Установки DMZ (демилитаризованная зона) применяются для единичного клиента (например, Web-сервера), находящегося за маршрутизатором для полного доступа к нему из Интернета и гарантии полной совместимости интернет-приложений, 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, предоставляя возможность пользователям офисной сети совместно использовать параллельный и USB-принтеры для печати файлов и Web-страниц.

Рис. 2.56. 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. 2.57 пред-

ставлена 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 бóльшим 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.

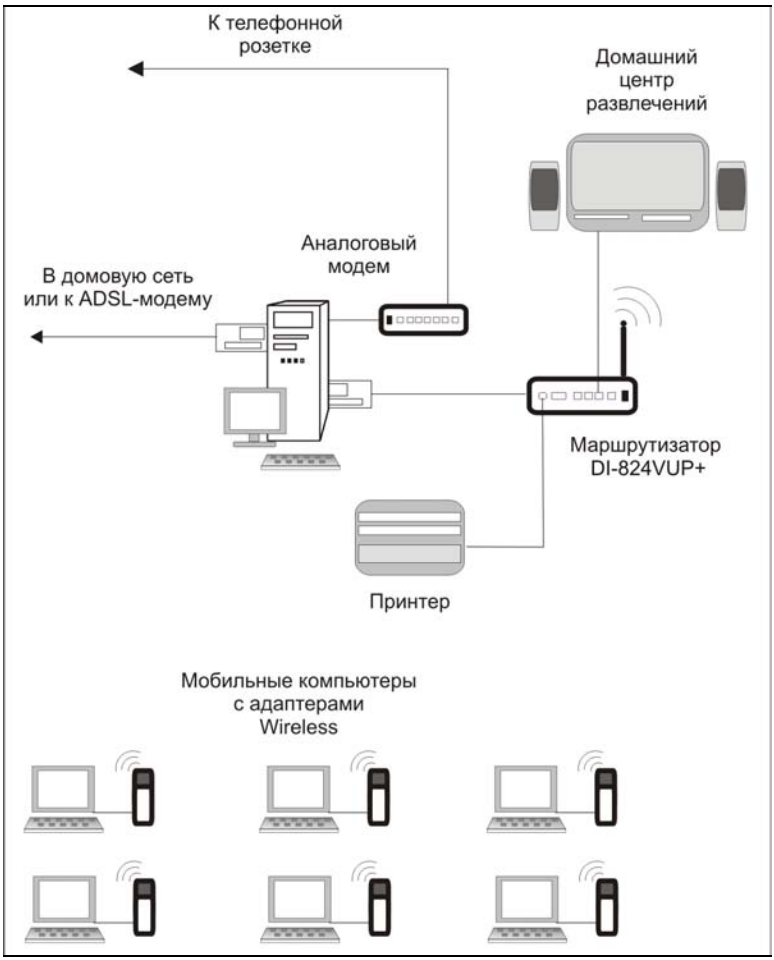


Рис. 2.57. Общая схема домашней сети с использованием маршрутизатора DI-824VUP+

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 домовой сетью, через которую обеспечено предоставление доступа в Интернет. К этому подключению также обеспечивается общий доступ.

Канал связи с Интернетом может быть подключен непосредственно к маршрутизатору, но сначала мы рассмотрим вариант, когда он подключен к компьютеру или локальной сети. Это было вызвано, во-первых, тем, что 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 вовнутрь 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. Для того чтобы работа маршрутизатора уже на самом начальном этапе была близка к реальной, мы взяли ноутбук с подключенным к нему беспроводным адаптером D-Link DWL-G122 USB стандарта 802.11g.

Достаточно установить программное обеспечение, прилагаемое к адаптеру, и вы уже можете соединяться с маршрутизатором для его настройки и администрирования, подключив его, конечно, к источнику питания. Для подключения к маршрутизатору через радиоканал необходимо в адресной строке Internet Explorer набрать 192.168.0.1. Именно такой адрес по умолчанию имеет маршрутизатор.

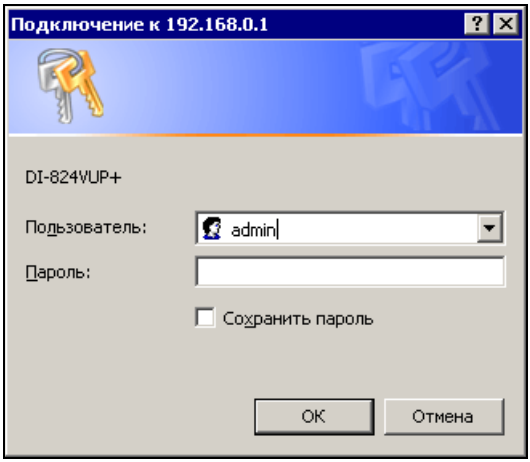


Рис. 2.58. Подключение к 192.168.0.1. Окно авторизации

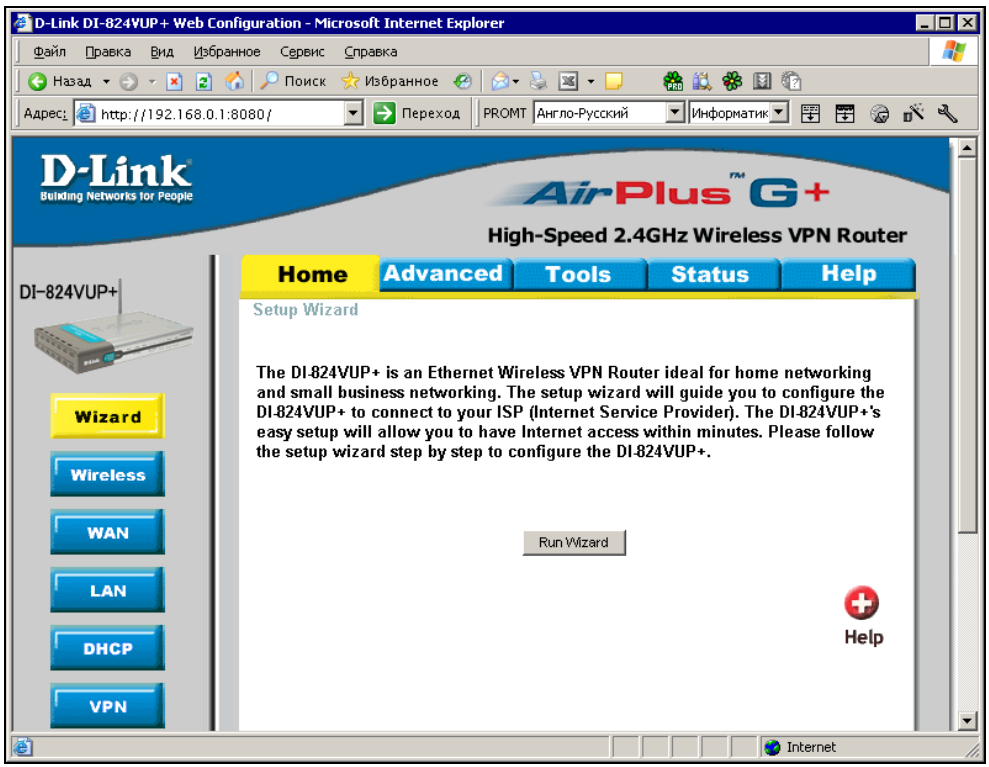


Рис. 2.59. Окно конфигурации маршрутизатора DI-824VUP+

Для подключения нужно ввести имя и пароль администратора (рис. 2.58). Для нового устройства это имя — admin, а пароль просто пустой (отсутствует). Конечно, есть возможность изменить и имя, и пароль, но до завершения всех настроек этого делать не стоит.

После успешной авторизации появится страница, предлагающая для настройки воспользоваться мастером настройки (рис. 2.59). 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.

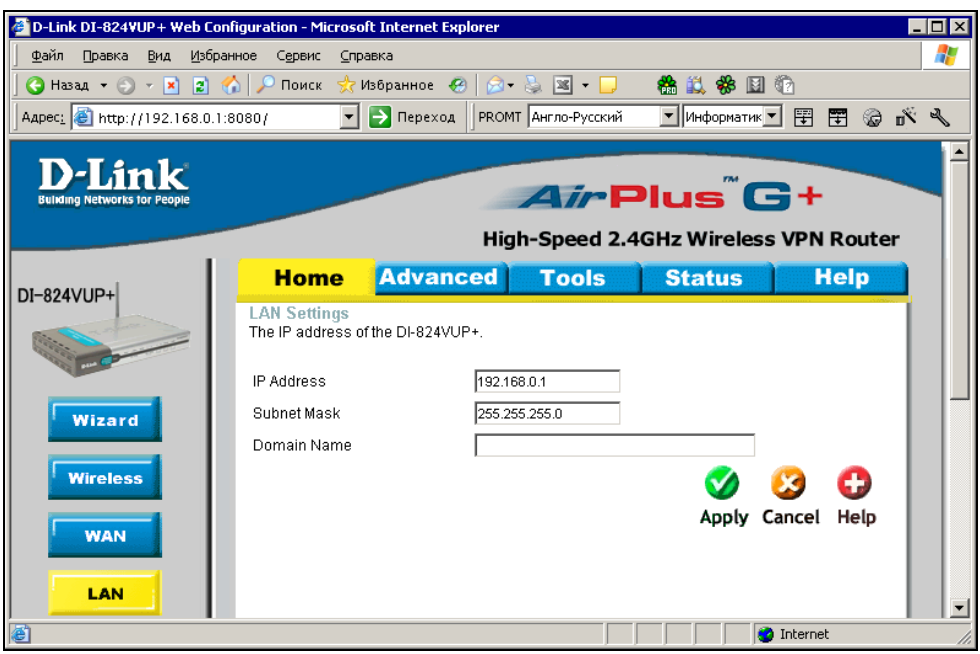


Рис. 2.60. Окно конфигурации маршрутизатора DI-824VUP+ .
Настройка локальной сети

Некоторых настроек мастер конфигурации не касается. В их числе и параметры сети, в которой должен работать маршрутизатор (рис. 2.60). Нажав

кнопку **LAN**, можно увидеть, а при необходимости и изменить эти настройки. Но в этом редко возникает нужда. Значительно чаще требуются настройки внешней для маршрутизатора WAN-сети. Нажав кнопку **WAN**, вы получите доступ к этим настройкам (рис. 2.61).

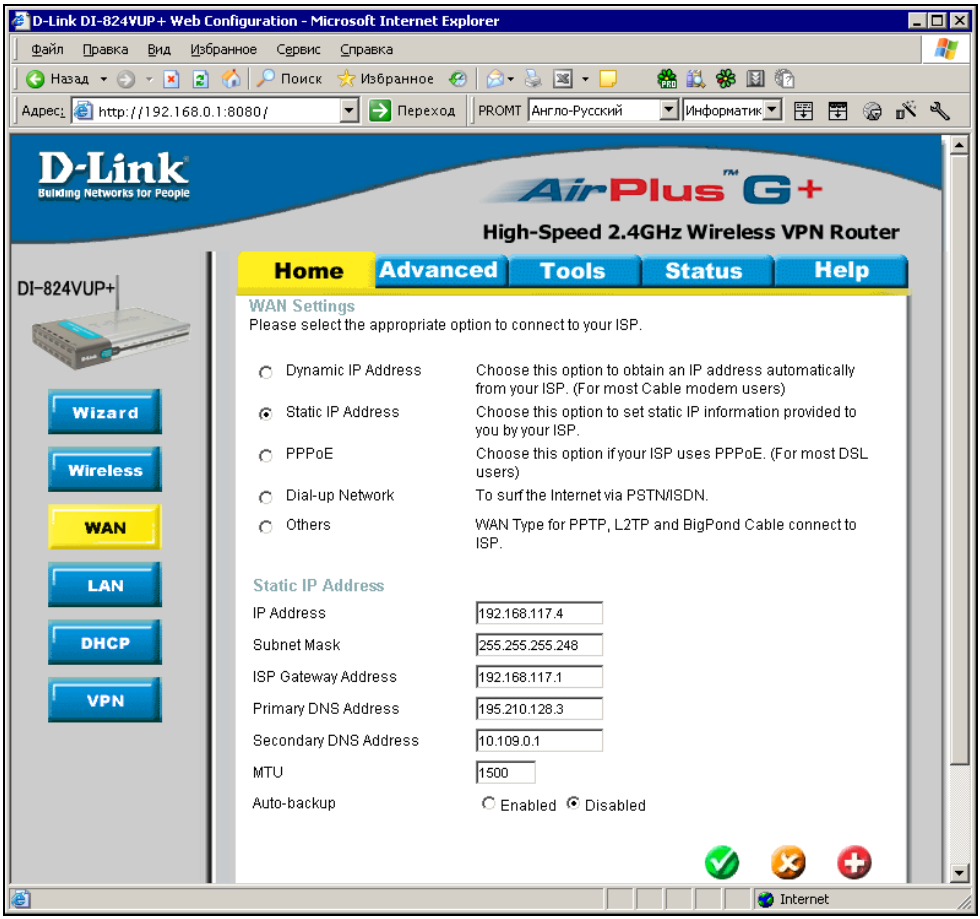


Рис. 2.61. Окно конфигурации маршрутизатора DI-824VUP+ . Настройка параметров глобальной сети

Маршрутизатор может быть подключен к сети как одно из рядовых устройств. Поэтому и IP-адрес маршрутизатора не отличается какими-либо особенными признаками. В примере внешняя для маршрутизатора сеть может иметь шесть устройств, включая главный компьютер (сервер) и сам маршру-

тизатор. Ограничение, конечно, условно. Просто установлена маска подсети 255.255.255.248. В данном случае маршрутизатор настраивается для доступа в Интернет, который обеспечен внешней сетью. В полях для адресов DNS-серверов вводим доступные адреса. Один из них соответствует сети еще более крупной (городской), в которой работает поставщик услуг доступа в Интернет, но все-таки и эта сеть тоже локальная. Адрес 10.109.0.1 не может принадлежать Интернету. Для компьютеров, которые будут подключены по радиоканалу к нашему маршрутизатору, будут доступны как ресурсы домашней (квартирной, офисной) сети, так и ресурсы внешней городской сети (FTP- и Web-серверы), и ресурсы Интернета.

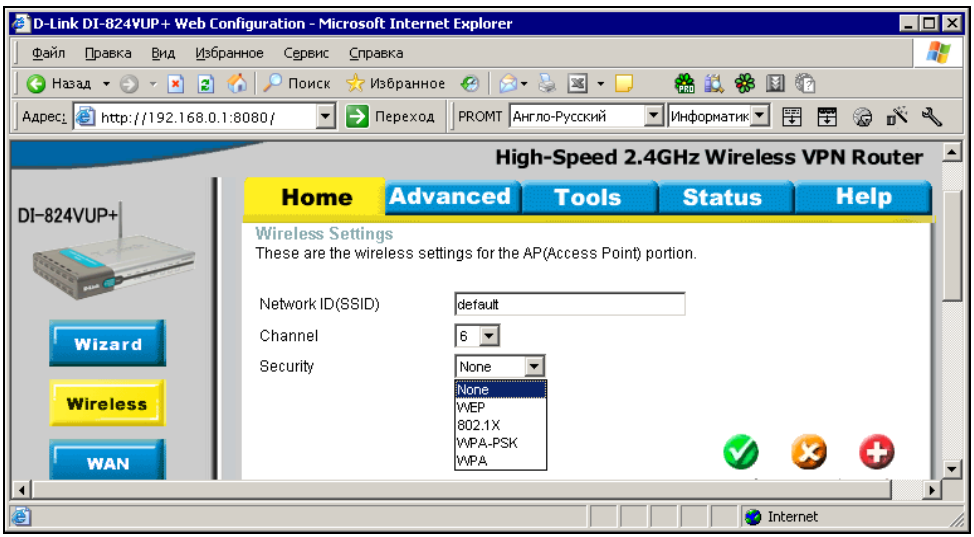


Рис. 2.62. Окно конфигурации маршрутизатора DI-824VUP+ .
Настройка параметров защиты радиосети

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. Можно и 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 при-

обрести 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 много шире, чем описанные в примере. Но не стремитесь использовать сразу все. Так, например, не пытайтесь подключить маршрутизатор к двум каналам доступа к Интернету. Маршрутизация может быть обеспечена к одному источнику. Можно, конечно, подключить все, но при необходимости воспользоваться тем или иным вариантом подключения изменять настройки маршрутизатора.

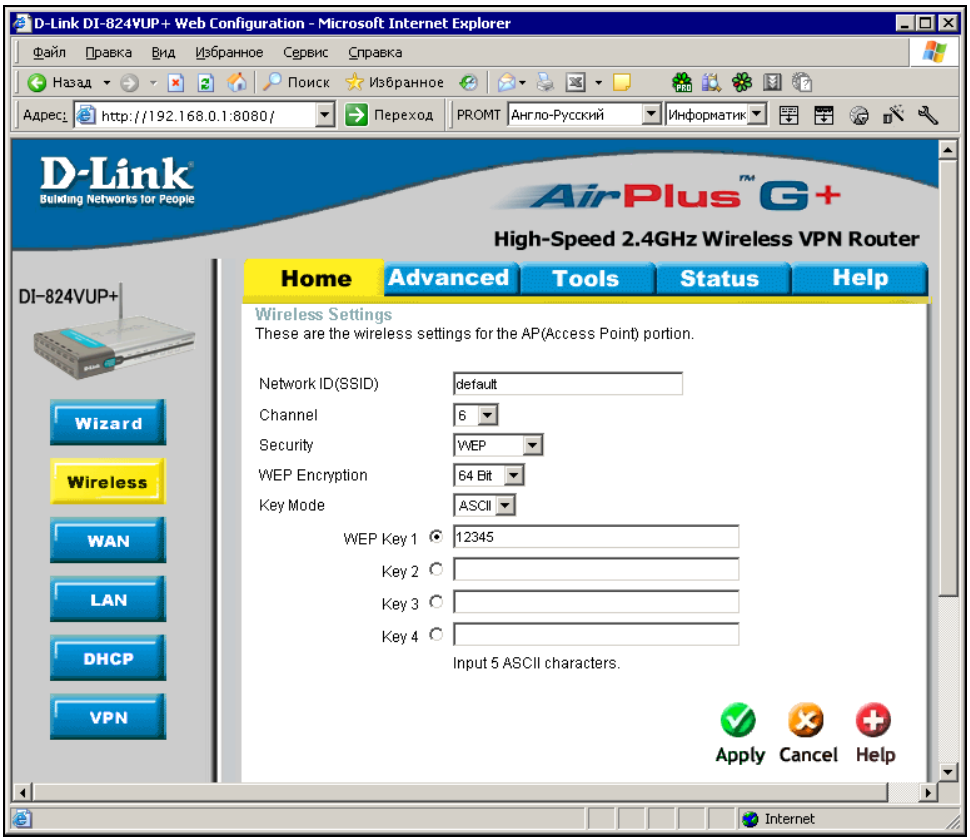


Рис. 2.63. Окно конфигурации маршрутизатора DI-824VUP+ .
Настройка параметров защиты радиосети,
выбор варианта шифрования

Среди прочих устройств на схеме сети (см. рис. 2.57) 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, нужно проанализировать потребности и не покупать устройства с излишне широкими возможностями. Давно замечено, что чем у́же специализация, тем выше качество работы устройств, меньше сбоев и непонятных процессов.

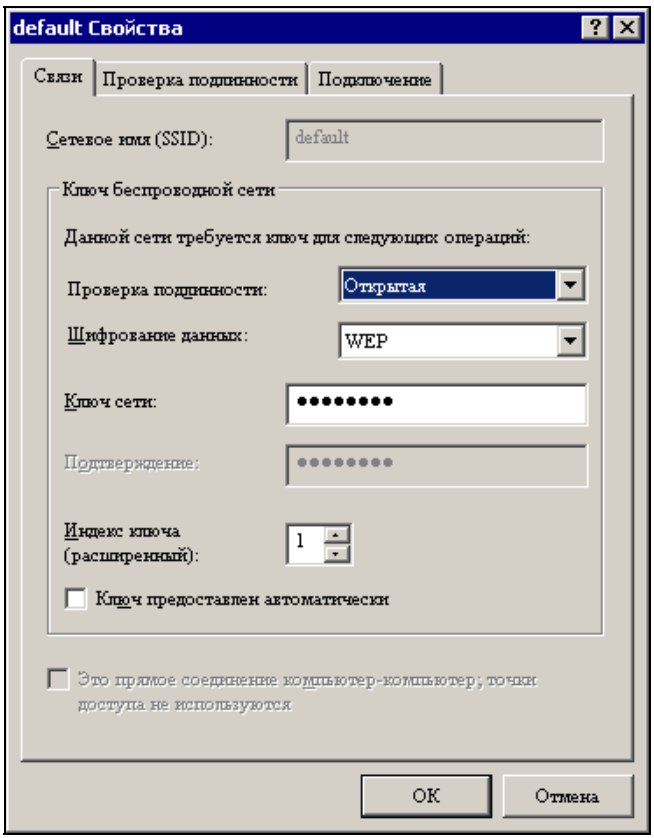


Рис. 2.64. Окно свойств Wireless-подключения на компьютере. Ввод ключа сети

Не стоит забывать и о защите. Как только к ноутбуку подключился Wireless сетевой адаптер DWL-G122 USB, появляется теоретическая возможность подключения к этому компьютеру из другой радиосети. Но это возможно только при отключенном брандмауэре для данного подключения. Но независимо от наличия защиты на компьютерах сети возможен доступ к настройкам маршрутизатора со стороны злоумышленника. Можно выбрать защищенный режим работы сети. На рис. 2.62 представлено окно настройки сети со списком возможных вариантов.

На рис. 2.63 уже выбран вариант шифрования информации в сети и введен ключ, который только что пришел в голову администратору.

> ***Внимание!***
>
> Запишите этот ключ, не закрывая страницу в интернет-браузере! Теперь у вас нет доступа к сети, ноутбук настроен на работу с открытой сетью без шифрования!

Ну, на самом деле паниковать не стоит. Откройте свойства вашего подключения (рис. 2.64) 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.

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 особенно 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.

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.cir-sanych.ru**;
- **http://www.citforum.netis.ru/nets/wireless/seti_efir**

или к справочной информации Windows.

Модем

А теперь опишем подключение аналогового модема к маршрутизатору с целью получения выхода в Интернет через коммутируемое соединение без компьютера-посредника. На странице настройки **WAN** выбираем вариант **Dial-up Network** и заполняем поля известными данными (рис. 2.65).

Assigned IP Address и **Extra Settings** оставляем такими, как есть, **Baud Rate** (скорость порта в бодах) ставим минимально доступной из списка — **38400**. Позднее можете попробовать увеличить это значение, но только после успешного подключения.

Перейдя на вкладку **Advanced** (Расширенные) и нажав кнопку меню **Routing** (Маршрутизация), включаем динамическую маршрутизацию (Dynamic Routing) RIPv1 (Routing Information Protocol, протокол обмена информацией о маршрутизации). Ниже на той же странице несколько полей для ввода данных. В них не вводим ничего — оставляем пустыми.

Теперь подключаем модем к маршрутизатору, переходим на вкладку **Status**, выбираем кнопку меню **Device Info**, а на открывшейся странице — кнопку **Dial-up**. Ждем установления соединения. После того как соединение установилось, можем открывать Internet Explorer и выходить в Интернет.

Если все нормально работает, то остается выбрать вариант установления связи. На вкладке **Home** меню **WAN** доступны три варианта. **Always-on** (Всегда включено), **Manual** (Вручную) и **Connect-on-demand** (По требованию).

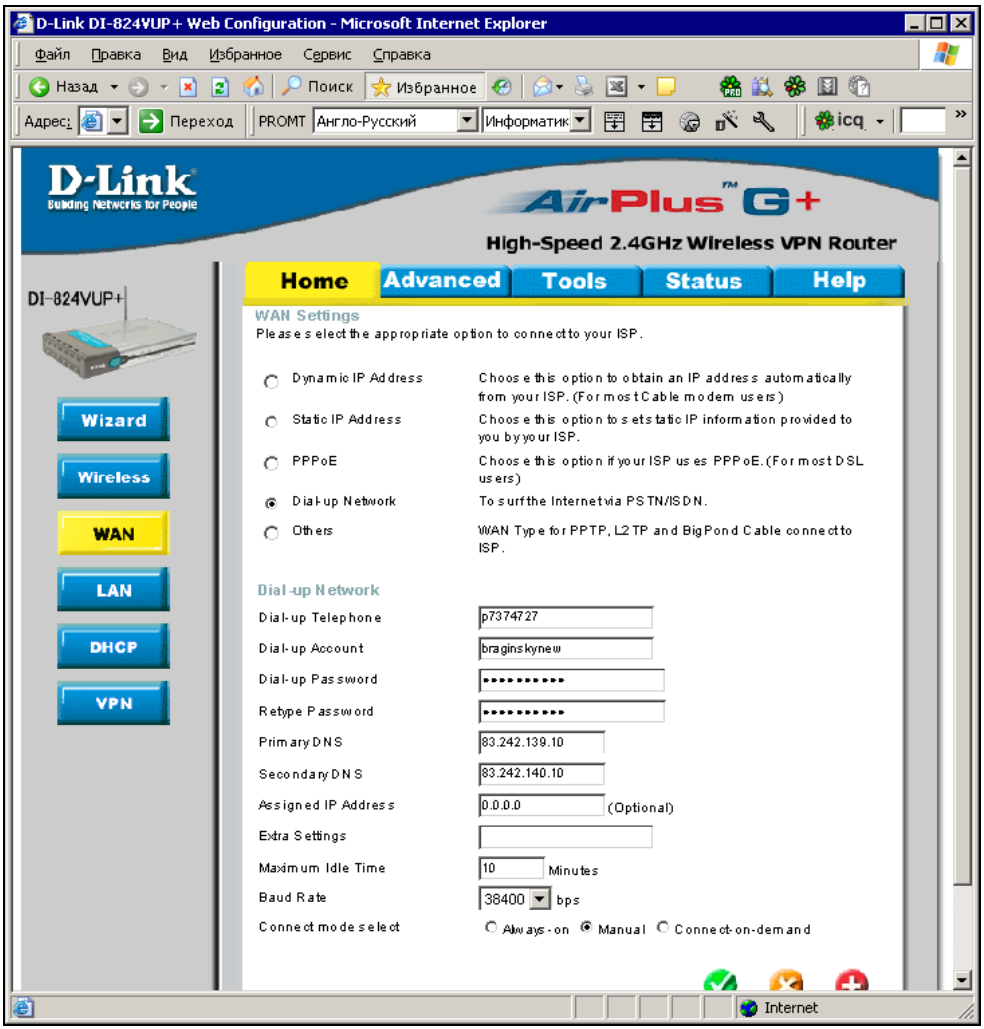
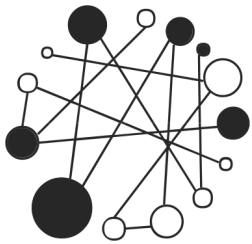


Рис. 2.65. Окно конфигурации маршрутизатора DI-824VUP+ .
Настройка параметров глобальной сети
для модемного коммутируемого подключения

* * *

Надеюсь, что информации в этой главе достаточно для того, чтобы подключить к Интернету нашу сеть. Используя общий доступ к подключению Интернета или маршрутизатор с модемом, можно обеспечить доступом в Интернет все ваши компьютеры одновременно. Получив доступ в Интернет, можно подумать о средствах общения с друзьями и коллегами, у которых доступ в Интернет уже есть. Эти же средства могут быть применены и для общения между вашими компьютерами. Моя дочь частенько присылает мне сообщения чрез ICQ, будь я дома или на работе. Иногда она подключает Web-камеру, и общение становится еще более живым. О средствах общения через Интернет и локальную сеть поговорим в следующей главе.

Глава 3



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 Windows, так и в Linux, другую часть можно получить через Интернет. Используя возможности связи через Интернет, вы сможете найти много новых знакомых и друзей, интересную работу или подработку. Интернет объединяет людей, помогает найти единомышленников.

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, опустить в почтовый ящик и ждать, когда его доставят получателю, а тот, в свою очередь, напишет вам ответ. 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 почти 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 позволяют 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 этой 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 следует настроить программу **Факсы и сканирование Windows**. Настоящие факсимильные сообщения требуют наличия 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. 3.1.

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. 3.2) требуется только подключенный аналоговый модем.

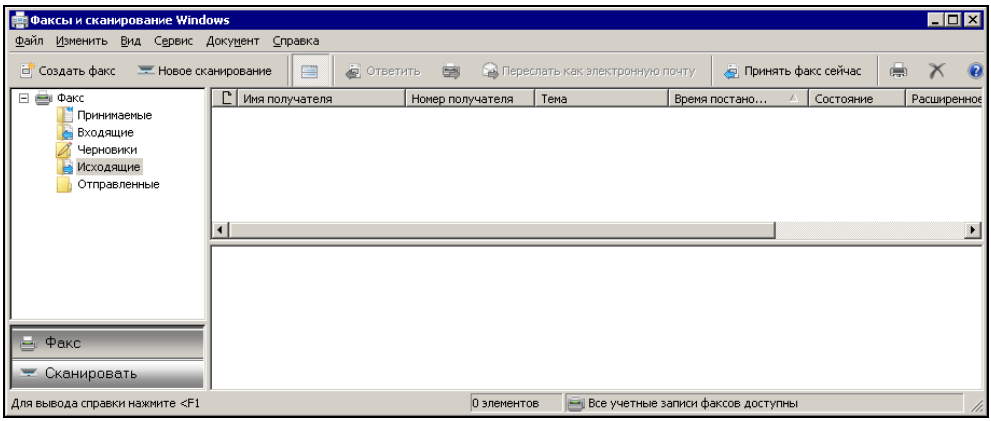


Рис. 3.1. Окно **Факсы и сканирование Windows**

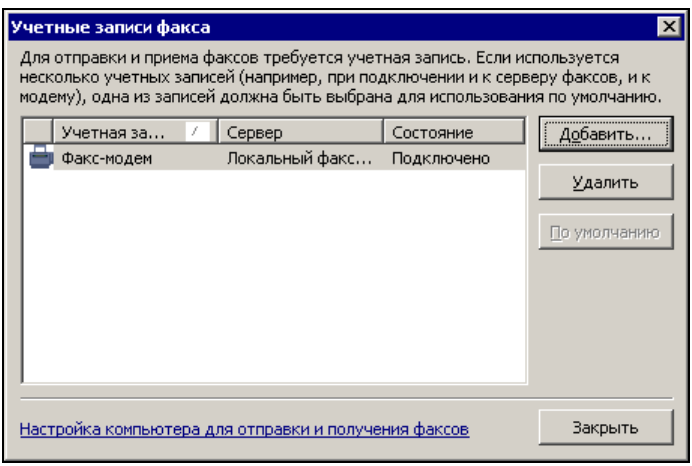


Рис. 3.2. Окно **Учетные записи факса**

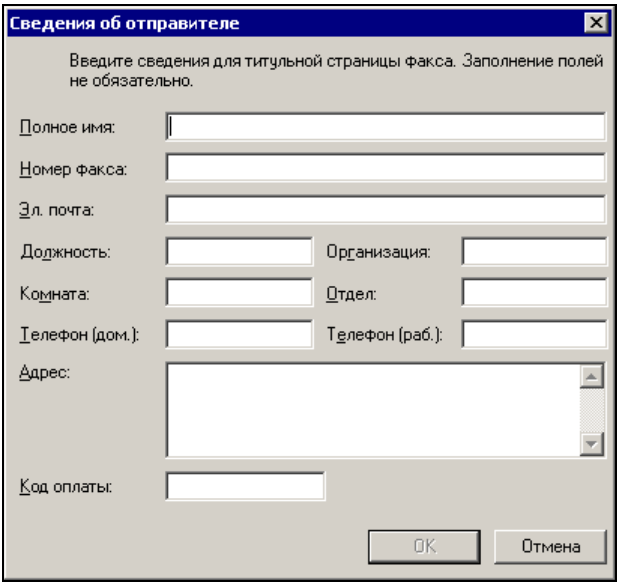


Рис. 3.3. Окно **Сведения об отправителе**

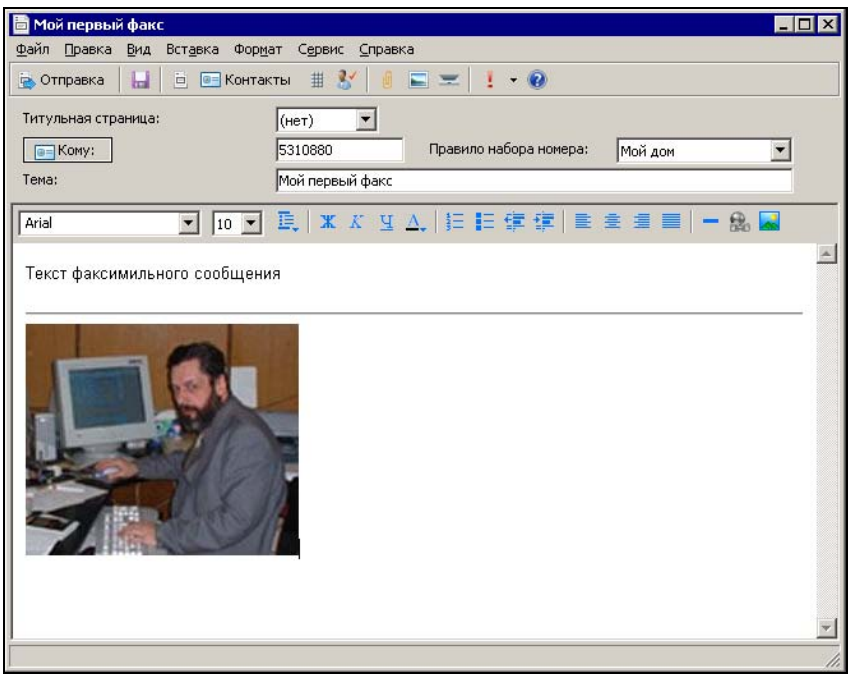


Рис. 3.4. Окно **Мой первый факс**

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. 3.3), окно которой вызывается из меню **Сервис | Сведения об отправителе**.

Заполнить можно только поля, которые предоставят получателю достаточные сведения, чтобы идентифицировать вас.

Теперь все готово для того, чтобы создать факс. Нажмите кнопку **Создать факс**. Появится окно создания вашего сообщения с заголовком, соответствующим его теме (рис. 3.4).

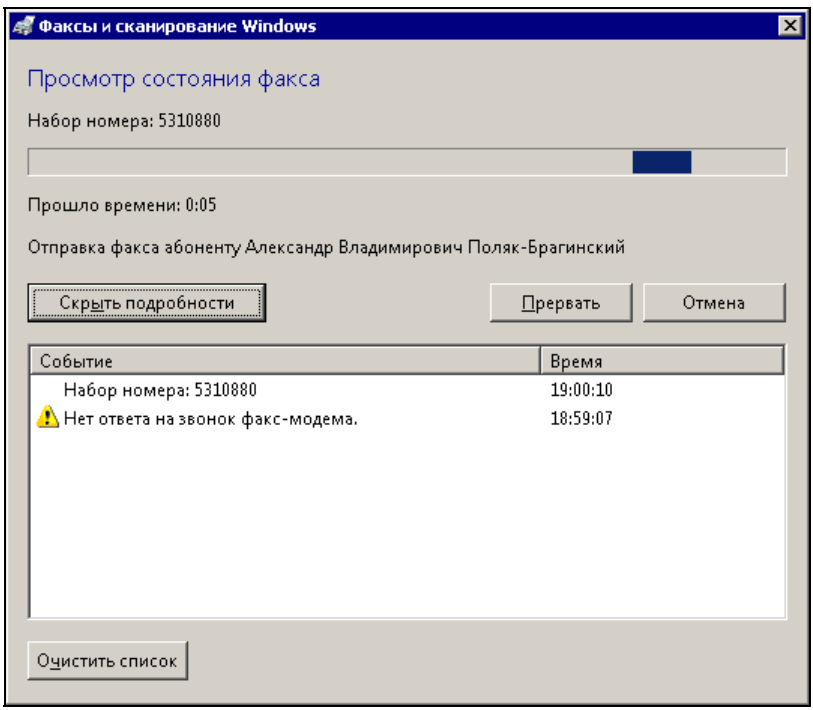


Рис. 3.5. Окно **Факсы и сканирование Windows**: просмотр состояния факса

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**. Начнется отправка факса. При этом вы увидите окно, в котором будет комментироваться процесс отправки и будут указываться проблемы, которые возникли при отправке (рис. 3.5).

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. 3.6).

Есть и много других параметров, с которыми вы можете ознакомиться самостоятельно, если решите использовать эту программу.

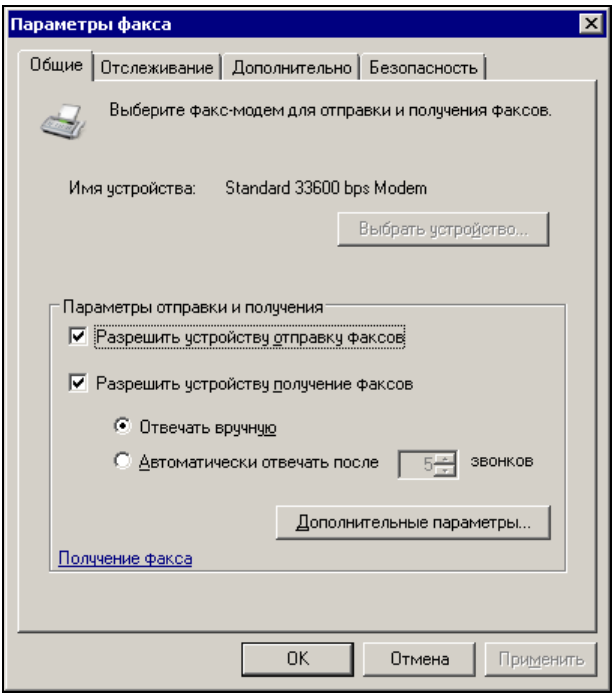


Рис. 3.6. Окно **Параметры факса**

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 позво-

ляет использовать эту возможность. Или на самом диске с дистрибутивом, или в репозиториях — хранилищах файлов для Linux, или в Интернете обязательно найдется программа для отправки факсов, и не одна. С помощью встроенного графического средства Управление программами (рис. 3.7) (в Mandriva Linux, в других дистрибутивах название может быть иным) вы всегда можете установить необходимые пакеты.

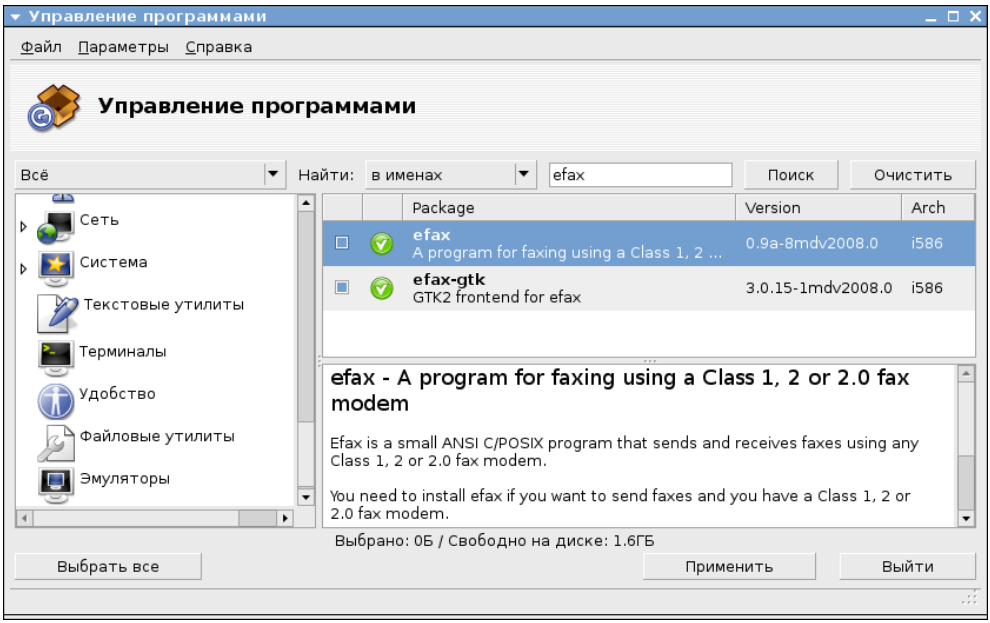


Рис. 3.7. Окно **Управление программами**

Найдите в перечне доступных программ 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. 3.8). Практически все текстовые редакторы для Linux могут сохранять документы в формате PDF. Этот формат может быть использован для подготовки факсов. Если модем уже установлен и настроен для подключения к Интернету, программа обнаружит его, и вы сможете отправить подготовленный файл или получить факс.

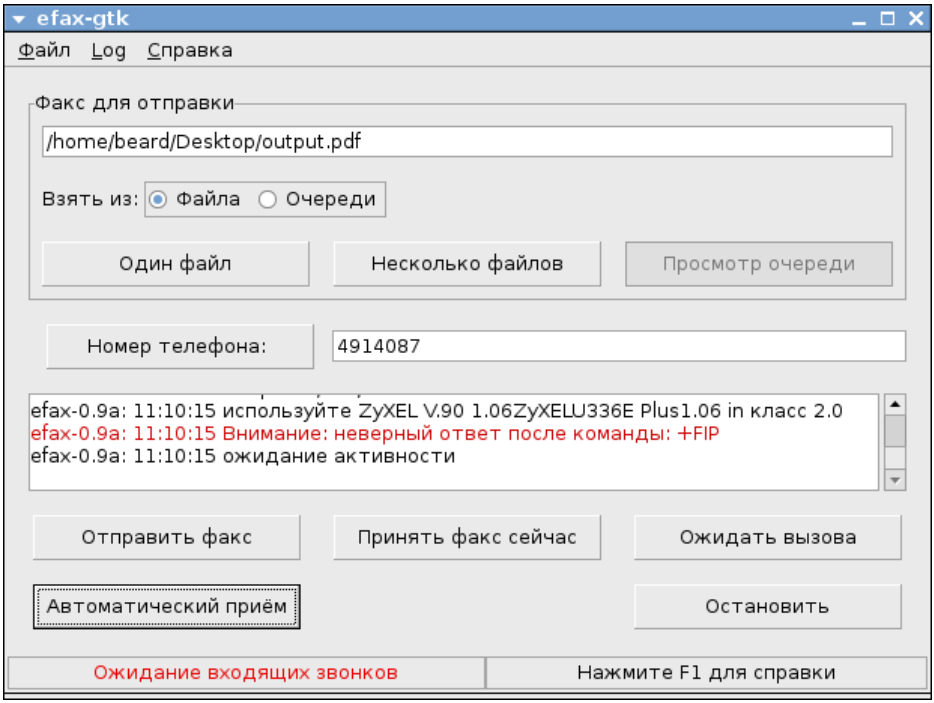


Рис. 3.8. Окно **efax-gtk**

Настроек у efax-gtk не много, и все они достаточно просты для понимания. Если требуется более подробная справка, нажмите клавишу <F1>. И интерфейс программы, и справка по ней в Mandriva Linux на языке системы (в данном случае на русском).

Электронная почта в Windows

Для отправки факсов подключение к Интернету не требуется. Электронная почта без Интернета работать не будет. Почтовые серверы доступны только через Интернет, а создание и отправка сообщений выполняются с помощью специализированных программ.

В Windows Vista входит почтовая программа Почта Windows (рис. 3.9).

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.

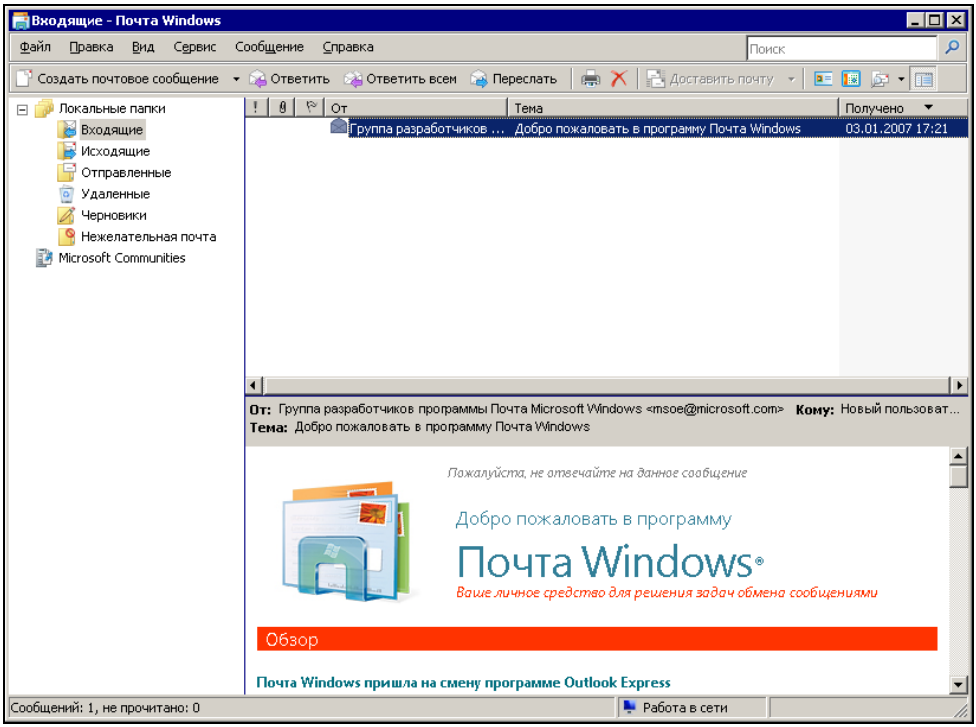


Рис. 3.9. Окно **Входящие - Почта Windows**

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.

Получив данные своей учетной записи, внесите их в программу. Для этого в меню **Сервис** выберите команду **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. 3.10). 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. 3.11).

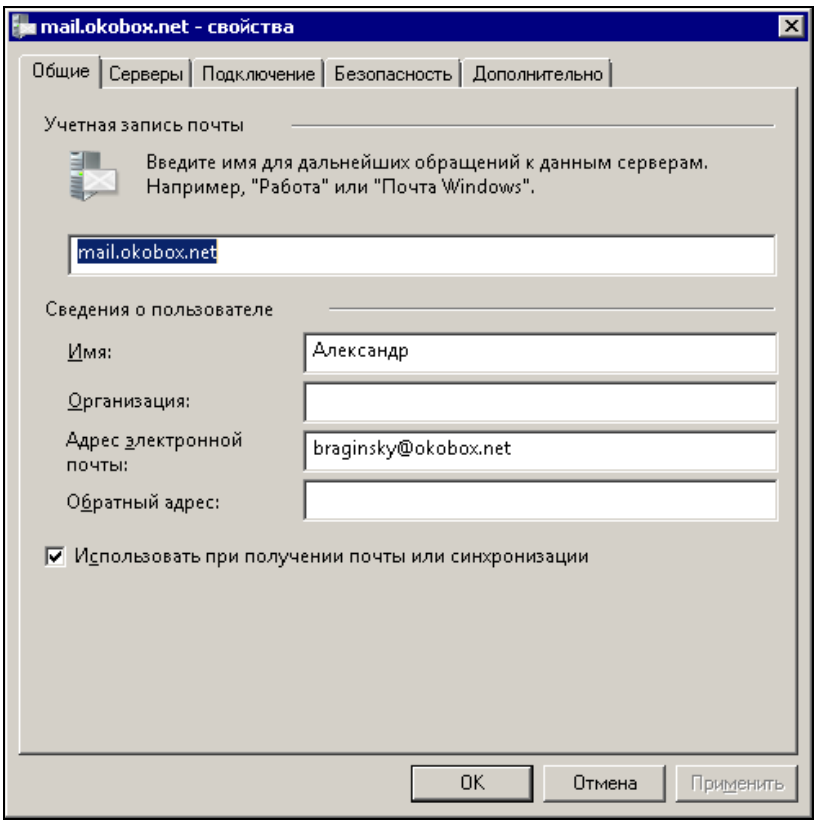


Рис. 3.10. Окно ***<имя_учетной _записи>*** **- свойства**

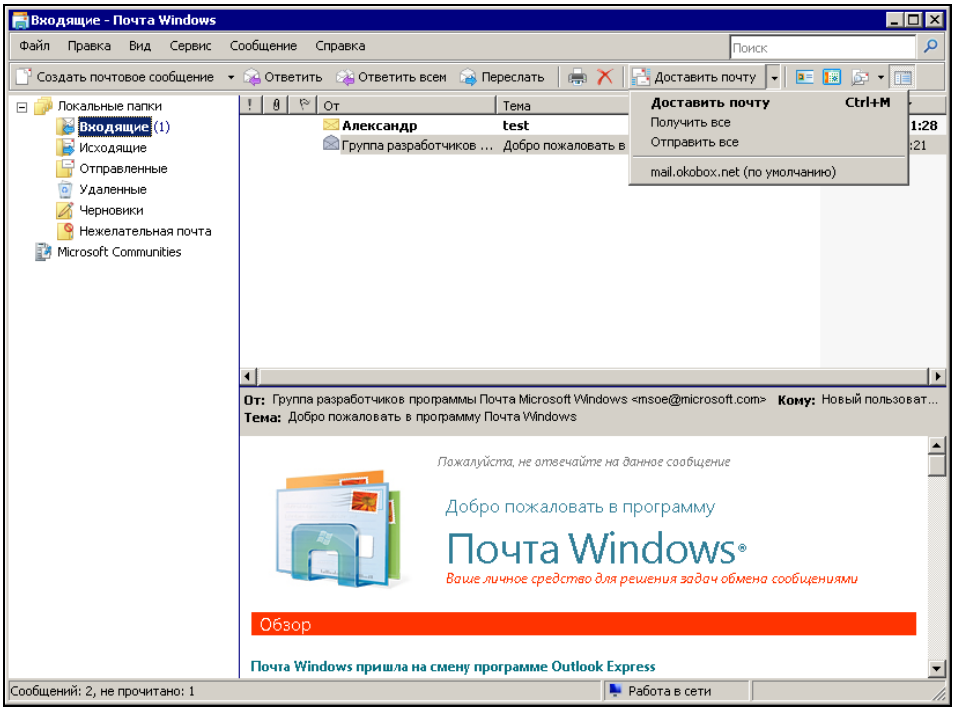


Рис. 3.11. Окно **Почта Windows**, меню **Доставить почту**

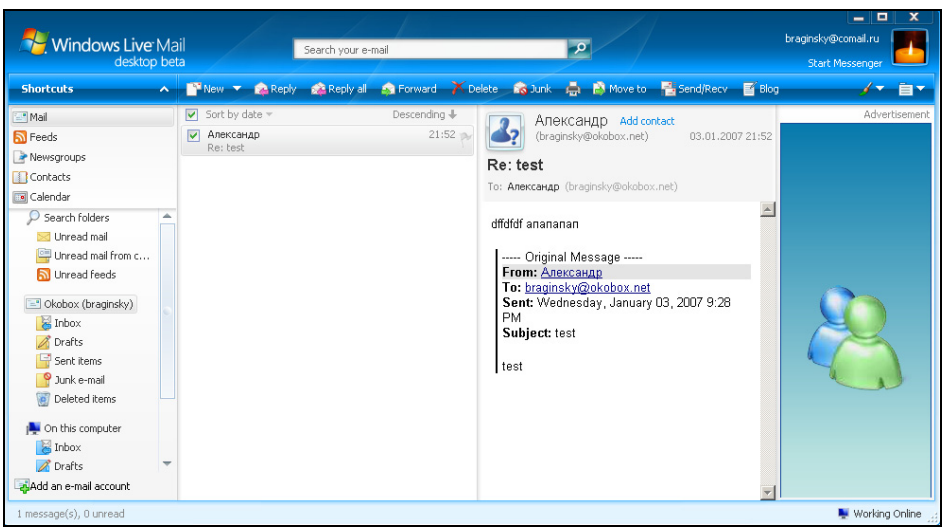


Рис. 3.12. Окно **Windows Live Mail**

Существует много почтовых программ. Со временем, когда вы в совершенстве будете знать Почту Windows, возможно, у вас появится желание попробовать другие программы, например, проходящую пока тестирование почтовую программу Windows Live Mail (рис. 3.12).

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 Evolution — почтовый клиент и ежедневник.

Рис. 3.13. Окно **Помощник по установке Evolution**

При первом запуске программы вы увидите окно **Помощник по установке Evolution** (рис. 3.13). Нажимая кнопку **Далее**, переходя от окна к окну, которые будет выводить Помощник по установке Evolution, вы можете настроить программу. Настройка практически всех почтовых клиентов очень похожа.

Настроив Evolution и запустив программу, вы увидите ее окно (рис. 3.14), откуда 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 сочетаний клавиш:

- **Основной режим** — <Ctrl>+<1>;
- **Контакты** — <Ctrl>+<2>;
- **Календари** — <Ctrl>+<3>;
- **Задачи** — <Ctrl>+<4>;
- **Заметки** — <Ctrl>+<5>.

Через меню программы **Правка | Параметры** доступны настройки, которые вам могут потребоваться после работы **Помощника по установке Evolution** (рис. 3.15).

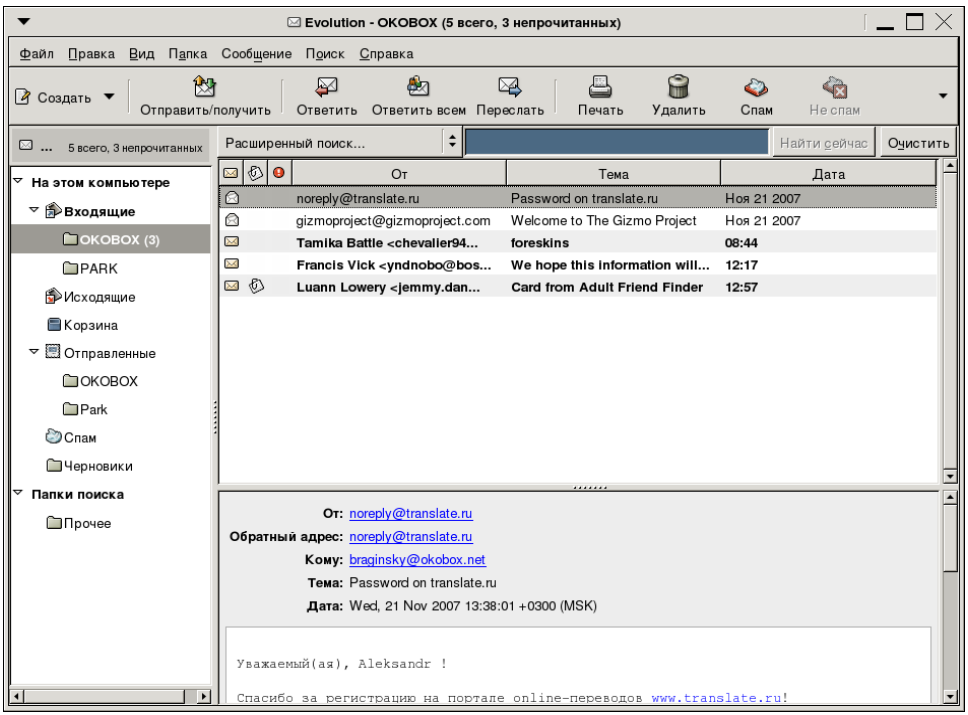


Рис. 3.14. Окно программы Evolution

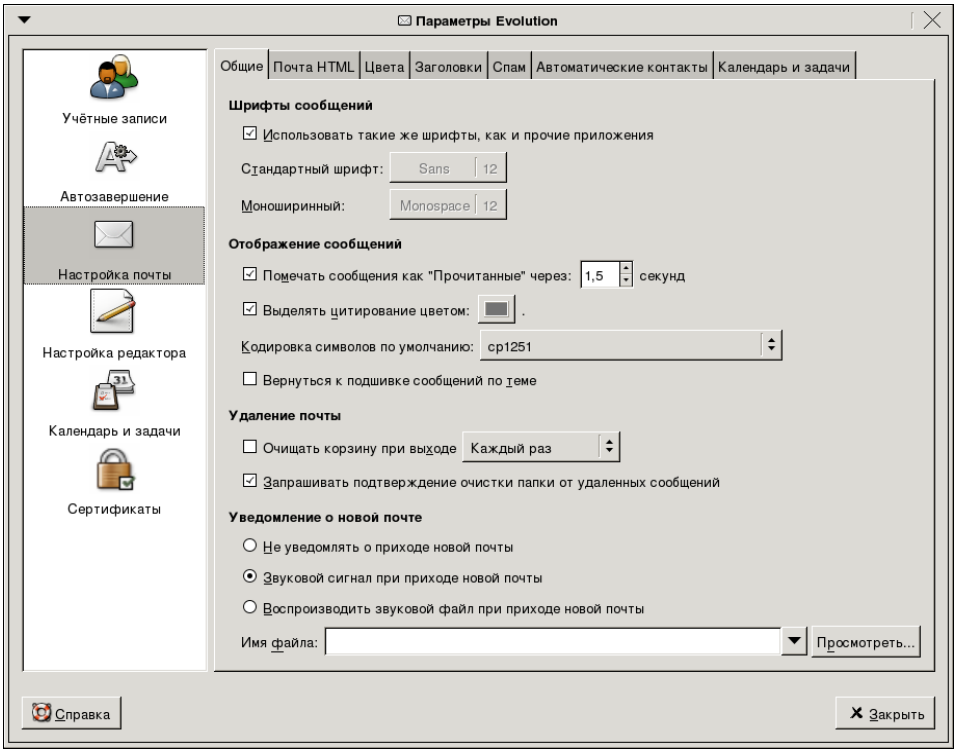


Рис. 3.15. Окно **Параметры Evolution**

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

Эта программа (рис. 3.16) тесно интегрирована в систему сервисов Windows Live, как и Windows Live Mail.

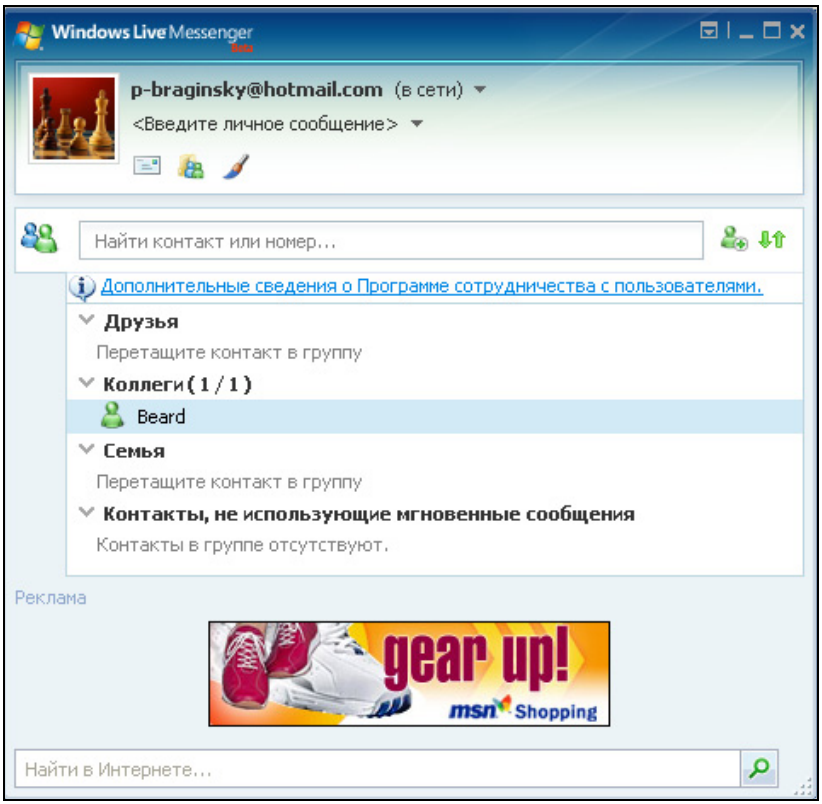


Рис. 3.16. Окно **Windows Live Messenger**

Windows Live Messenger позволяет обмениваться текстовыми сообщениями (рис. 3.17), 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/**.

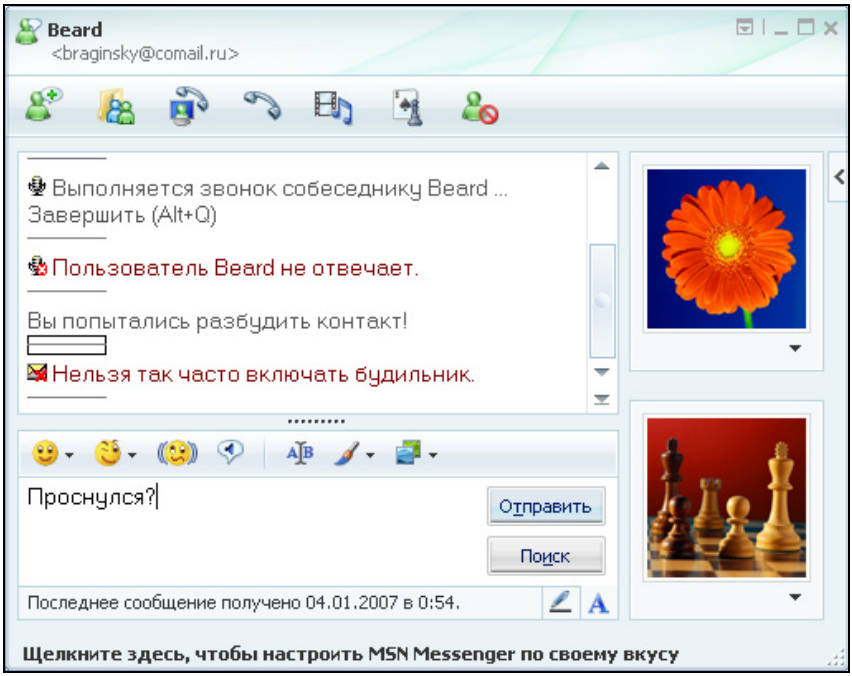


Рис. 3.17. Окно **Windows Live Messenger**: сеанс связи

Rambler ICQ

Эта программа (рис. 3.18) 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 Rambler.ru.

Возможности программы аналогичны Windows Live Messenger, функциональность программы основана на интеграции с несколькими сервисами, включая электронную почту и персональные блоги.

Рис. 3.18. Окно **Rambler ICQ**

Skype

Эта программа (рис. 3.19) 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, 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 **Яндекс Деньги**.

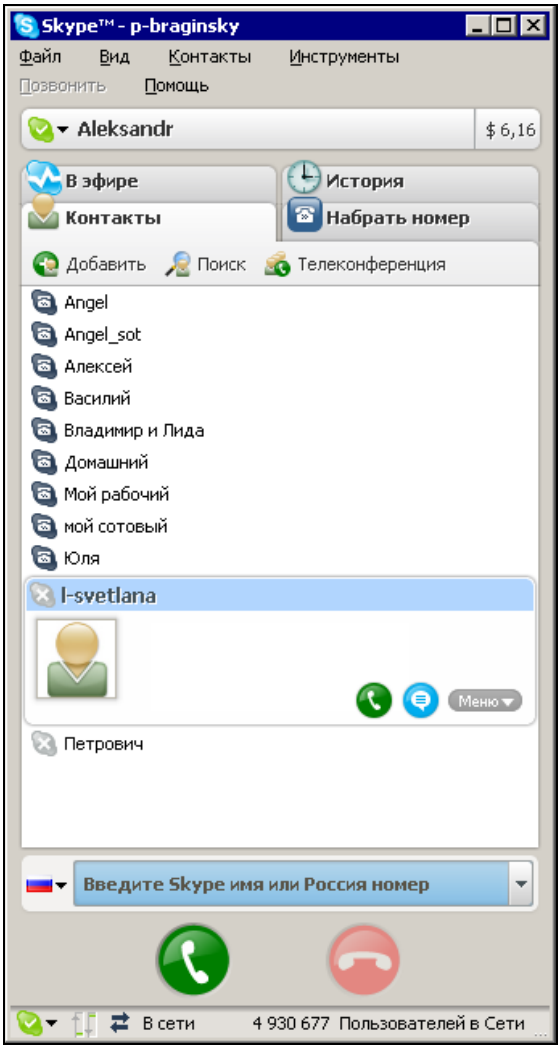


Рис. 3.19. Окно программы Skype

QIP Infium

Пожалуй, эта программа (рис. 3.20) заслуживает особого внимания (**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 предла-

гает звонки по Москве и Петербургу бесплатно... И обмен сообщениями, и голосовое общение доступны через эту программу. Возможны звонки на стационарные телефоны. Как и в Skype, возможно использование USB телефонного оборудования. Пока QIP Infium существует только в бета-версиях, но уже для большинства пользователей работает полноценно.

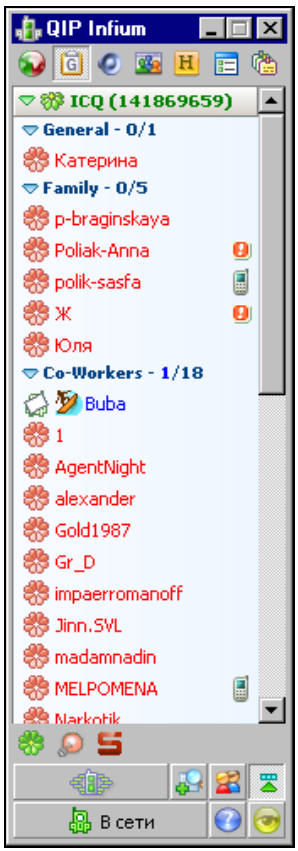


Рис. 3.20. Окно **QIP Infium**

COMILFON

Существуют программы, которые предназначены исключительно для голосового общения и звонков на обычные телефоны. Одна из таких программ — COMILFON (рис. 3.21) (**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.

Рис. 3.21. Окно **COMILFON**

На сайте **www.comilfon.ru** есть подробные объяснения по вопросам использования программы.

Telphin

Еще одна программа для голосового общения (рис. 3.22). 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 дополнительный аккаунт через другого оператора связи, например, SIPNET.

Рис. 3.22. Окно **Telphin**

Поискав 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 полюбившихся программах, но под управлением другой операционной 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. 3.23 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.

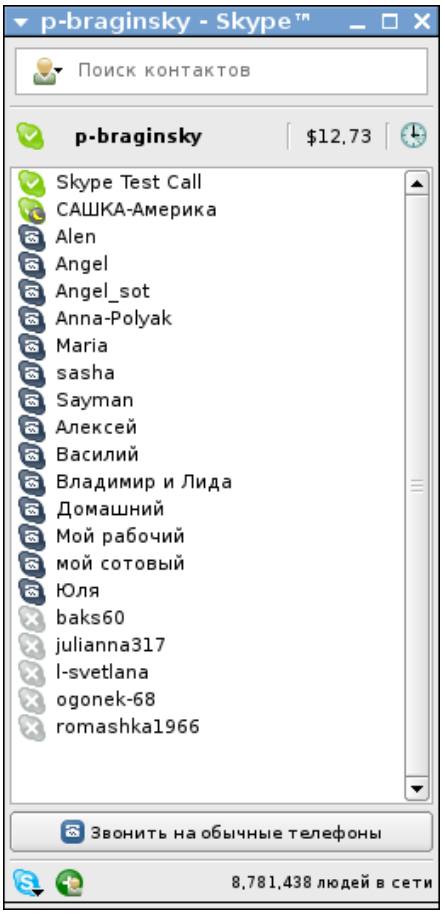


Рис. 3.23. Окно программы Skype для Linux

Чем больше будет пользователей Linux, тем больше полнофункциональных программ будет для этой операционной системы. Но основные возможности Skype — текстовое и голосовое общение через Интернет, звонки на стационарные и мобильные телефоны — присутствуют и в этой версии. Программа входит в дистрибутив Mandriva Linux.

Ekiga

Ekiga разработана специально под ОС Linux для голосового и видеообщения, обмена мгновенными сообщениями (рис. 3.24). Доступна программа по адресу в Интернете: **http://www.gnomemeeting.org**.

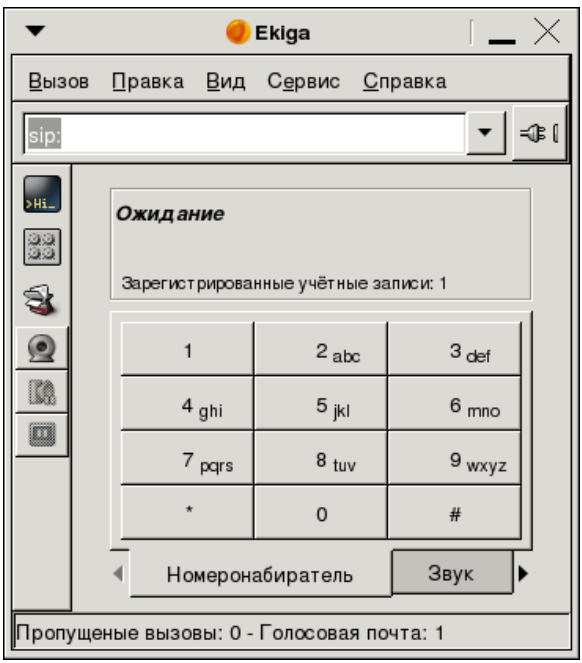


Рис. 3.24. Окно **Ekiga**

Программа входит в большинство дистрибутивов системы и имеет следующие возможности:

- совместимость с протоколом SIP;
- возможность одновременной регистрации нескольких учетных записей;
- 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;
- журнал звонков;
- возможность блокирования администратором некоторых настроек;
- поддержка видеоконференций;
- автоопределение устройств;
- гибкое конфигурирование звуковых оповещений;
- совместимость оконными менеджерами KDE и GNOME;
- руководство пользователя;
- перевод на множество языков.

Gaim — Pidgin

Gaim — это программа мгновенного обмена сообщениями (рис. 3.25). В Gaim поддерживается множество протоколов на основе модулей, включающих AIM, ICQ, Yahoo!, MSN, Jabber, IRC, Napster, Gadu-Gadu и Zephyr.

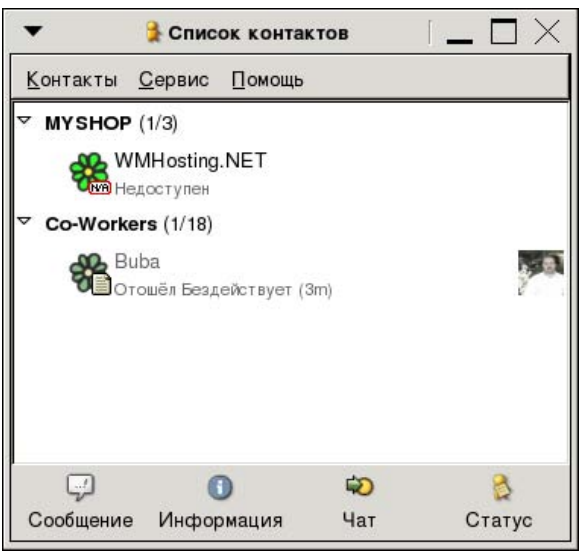


Рис. 3.25. Окно программы Gaim

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**.

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 г., 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 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, поставленные для достижения этих 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). То есть современная техника, становящаяся все более доступной, позволяет включать ее в компьютерные сети. Если есть возможность просматривать Web-страницы, то кто-то эти страницы делает. Обладатель обычного персонального компьютера в наше время в состоянии создать Web-страницу, сложность которой будет зависеть от фантазии создателя.

Любой современный персональный компьютер позволяет организовать Web-сервер. Если этот сервер включен в локальную сеть, то просматривать его страницы сможет любой пользователь этой сети.

Компьютерные сети уже давно стали средой общения единомышленников посредством электронной почты, чатов, различных программ мгновенной передачи сообщений. Многие пользователи компьютеров создают персональные страницы в Интернете, используя бесплатные или платные площад-

ки 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 общение еще на один уровень. 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 видеоинформации).

Каждый желающий может стать режиссером, оператором, сценаристом, актером, композитором, писателем при создании произведений для публикации в сети.

Технические подробности

Говорить о создании Web-сервера мы сейчас не будем. Об этом много сказано на страницах в Интернете и просто в справке Windows. Сейчас поговорим только о том, как включить в Web-страницу видеоинформацию, как настроить передачу этой информации в Интернет. В программе ConquerCam вы сможете разобраться самостоятельно. Да она и не позволяет передавать в Интернет динамическое изображение. Только статические картинки, хотя и обновляемые при нажатии кнопки **Обновить** в браузере Internet Explorer, доступны при использовании этой программы. Совсем другое дело — Кодировщик Windows Media 9 Series. С помощью этой бесплатной программы вы

можете передавать на свою страницу в Интернете видеоинформацию в режиме реального 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 предварительно записать видеосюжет 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 **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 **Вставка | Веб-компонент**, а в открывшейся форме — **Дополнительные элементы | Элемент ActiveX**.
9. Нажмите кнопку **Далее**.

10. В открывшемся списке найдите **Windows Media Player** и нажмите кнопку **Готово**. Ячейка увеличится до размеров окна Windows Media Player, имеющего в данном случае минимальный размер.

11. Теперь щелкните правой кнопкой мыши 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.

    Остальные параметры можно устанавливать по своему желанию.

> ***Примечание***
>
> Если предполагается, что страница будет помещена на сервер, где будет находиться и Кодировщик Windows Media 9 Series, то следует учесть, что на одном компьютере будут работать два сервера. Один — основной, для отображения страниц сервера, его адрес и порт будут указываться в адресной строке браузера. Другой сервер — дополнительный, для трансляции видеопотока. Его адрес должен быть указан в свойствах 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**.

13. Сохраните страницу, как Proba_video.htm в каталог Web-сервера.

14. Проверьте, что при открытии страницы 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. Нажмите 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 укажите выбранный порт (3333). Если у вас есть сомнения в том, что на вашем компьютере этот порт свободен, можно с помощью кнопки **Найти свободный порт** 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 необходимое значение. 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 опцию **Сохранить копию потока вещания** и указать файл, в который поток будет сохранен, во время прямой трансляции будет создана копия сеанса в виде файла, который вы сможете воспроизводить по запросу пользователей. Это требует дополнительных настроек, но в них после 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. Выберите кодирование только с выбранных устройств и нажмите кнопку **Далее**.
10. На следующем экране введите информацию о заголовке, авторе и другую текстовую информацию или оставьте все как есть. Снова нажмите 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. 3.26).

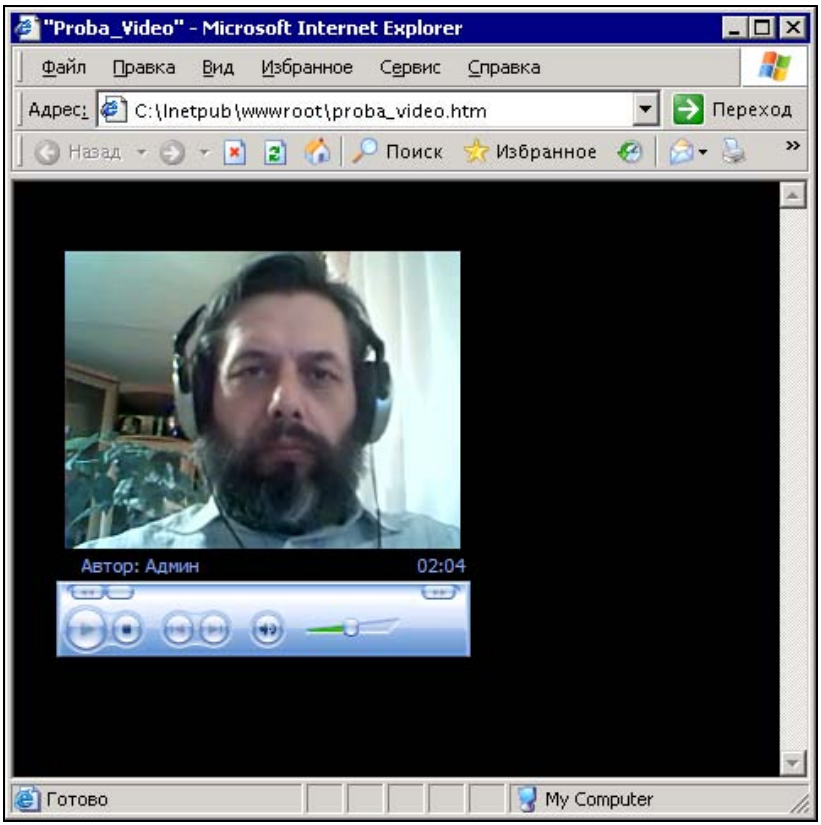


Рис. 3.26. Окно браузера с только что созданной страницей

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 применялось 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 видеоинформацию с дисков или созданную самостоятельно, то процедура настройки не будет очень сильно отличаться от описанной. Иногда, разве что, придется поэкспериментировать немного.

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. 3.27).

Через меню **Вид | Плейлист** откройте окно **Плейлист** (рис. 3.28), в котором через меню **Управление | Поиск сервисов** запустите поиск **Shoutcast TV**.

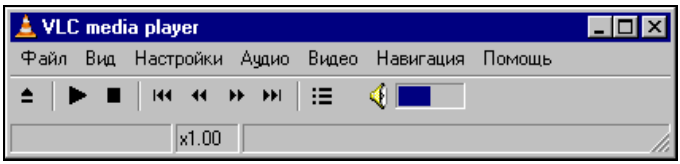


Рис. 3.27. Окно **VLC media player**

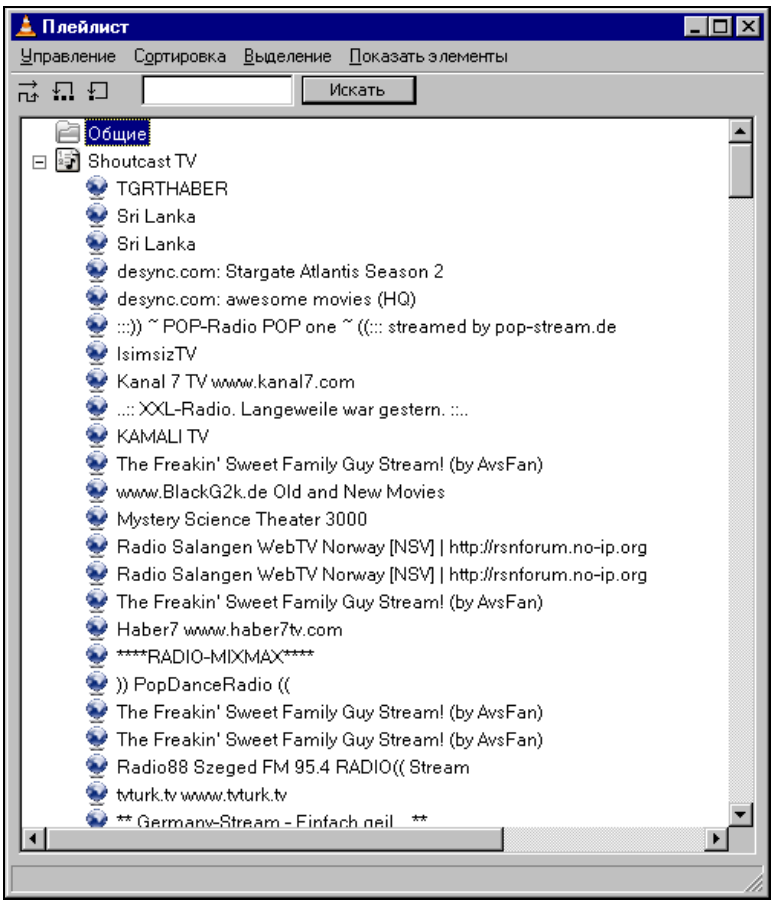


Рис. 3.28. Окно **Плейлист**

Выберите любой из найденных потоков, щелкнув на строке кнопкой мыши. Начнется воспроизведение потока на вашем компьютере.

Теперь запустите **Мастер вещания/кодирования** (рис. 3.29) из меню **Файл**.

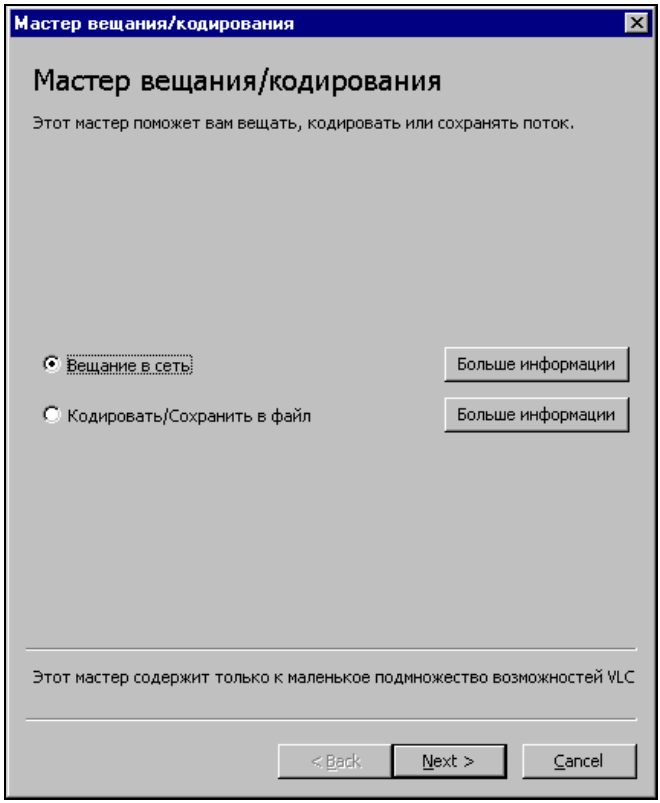


Рис. 3.29. Окно **Мастер вещания/кодирования**

Выберите переключатель **Вещание в сеть** и нажмите кнопку **Next**. Откроется окно **Мастер вещания/кодирования** на странице **Ввод** (рис. 3.30).

Выберите в этом окне строку потока, который уже воспроизводится, и нажмите кнопку **Next**.

Откроется окно **Мастер вещания/кодирования** на странице **Вещание** (рис. 3.31), в котором можно выбрать метод рассылки потока. Вариант **RTP Unicast** позволяет направить поток избирательно на определенный компьютер в сети. При этом необходимо указать его IP-адрес в поле **Адрес**. Вариант

RTP Multicast позволяет вещать на всю сеть. К сожалению, параметры нашей сети могут не совпадать с теми, что предусмотрены для этого метода вещания. Вариант **HTTP** тоже позволяет вещать на всю сеть. На компьютере-приемнике необходимо будет указать IP-адрес передающего компьютера.

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 команду **Открыть URL**, указав прием по UDP или HTTP и IP-адрес компьютера-передатчика и порт 8080.

В окне плейлиста появятся строки с информацией о принимаемых потоках (рис. 3.32), а на экране VNC и в динамике появится передаваемая информация (рис. 3.33).

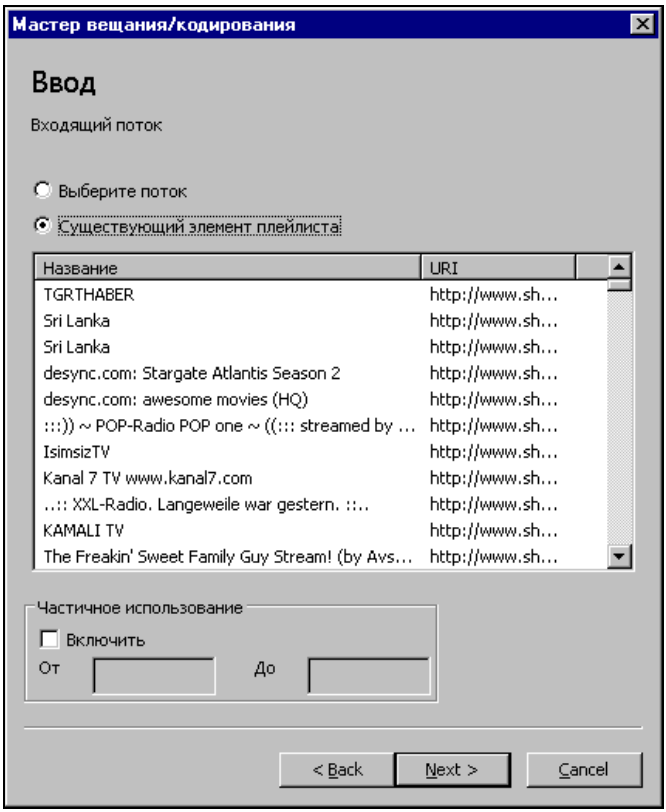


Рис. 3.30. Окно **Мастер вещания/кодирования**, страница **Ввод**

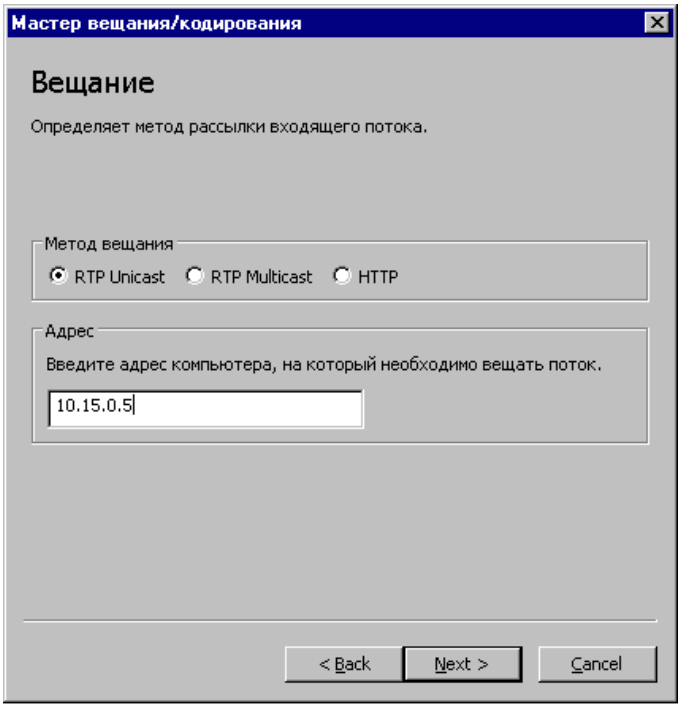


Рис. 3.31. Окно **Мастер вещания/кодирования**, страница **Вещание**

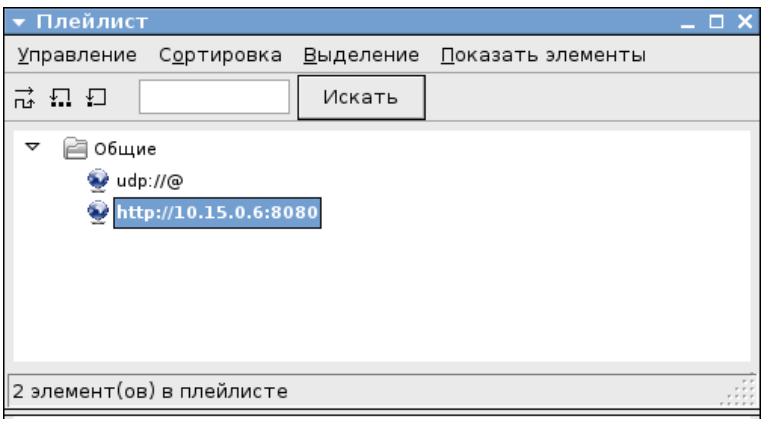


Рис. 3.32. Окно **Плейлист** (в Linux)

Если вместо потока из Интернета указать устройства самого компьютера, такие как Web-камера, например, то в сеть можно посылать изображение,

передаваемое этой камерой (рис. 3.34). Конечно, возможна передача видео из сохраненных файлов. Практически все, что необходимо для организации простой теле/радиостанции, имеется в VLC.

Интерфейс VLC можно выбрать по своему усмотрению в настройках программы. Один из вариантов интерфейса показан на рис. 3.34.

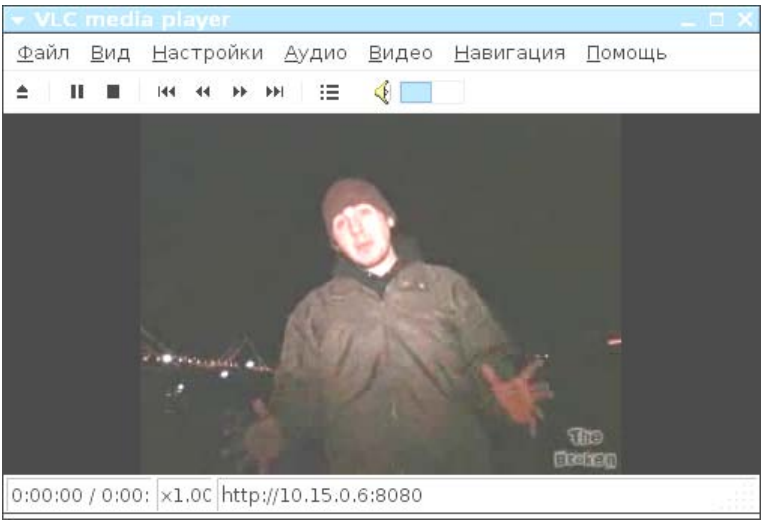


Рис. 3.33. Окно **VLC media player** (в Linux)

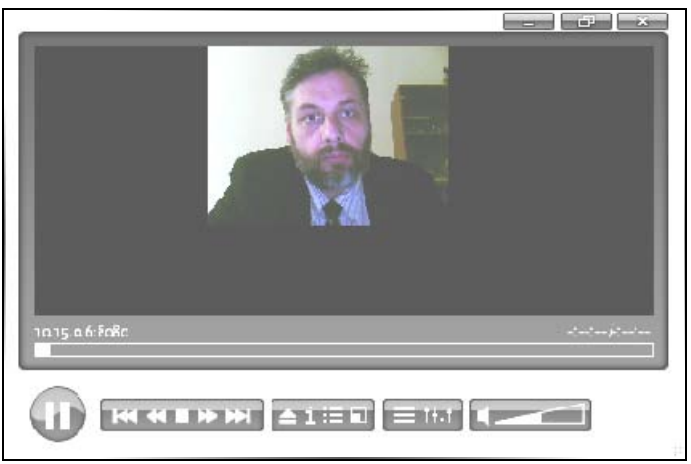
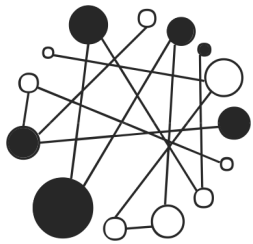


Рис. 3.34. Окно **VLC media player** (в Linux). Изображение от Web-камеры

Глава 4



Виртуальные компьютеры в домашней сети, создание сети на одном компьютере

Интерес к виртуальным технологиям в последние годы все более и более растет. Причем не только у специалистов, работающих в крупных сетях, где виртуализация помогает повысить эффективность использования оборудования и просто площади, на которой размещены серверы и компьютеры. Виртуальные технологии все более интересуют домашних пользователей. Если у вас есть желание посмотреть на работу различных операционных систем, но недостаточно средств и места для размещения компьютеров, где эти операционные системы смогут работать, можно воспользоваться виртуальными компьютерами. Для создания виртуального компьютера достаточно установить виртуальную машину. В ней вы можете создать неограниченное число виртуальных компьютеров, которые при необходимости можно сохранить на обычных CD- или DVD-носителях.

Создав виртуальный компьютер, вы можете включить его в вашу сеть на таких же правах, как обыкновенную реальную машину. Обращаясь к такому компьютеру по сети, вы не обнаружите никаких признаков того, что этого компьютера на самом деле нет. Он есть, но только он виртуальный. В этой книге мы рассматриваем только простую одноранговую сеть, но, установив виртуальный компьютер, вы можете попробовать создать сервер, поэкспериментировать с ним. Если файлы виртуального компьютера сохранены вами на диске, то в случае непоправимых проблем можно быстро восстановить компьютер из резервной копии. Если у вас нет желания создавать сервер, то и виртуальные рабочие станции могут вам послужить полигоном для их углубленного изучения. Нет опасности, что, выполнив некорректные действия, вы приведете систему к краху, и потребуется новая ее установка. Резерв-

ная копия позволит вам восстановить виртуальный компьютер уже настроенным в считанные минуты.

В этой главе мы обратим внимание на виртуальные машины, которые можно установить совершенно бесплатно. Компания VMware выпускает целую линейку продуктов для виртуализации компьютеров, причем два таких продукта совершенно бесплатны. VMware Server позволяет создавать виртуальные компьютеры и работать с ними, а VMware Player обеспечивает запуск созданных виртуальных компьютеров на любой рабочей станции. Возможностей этих двух программ для нас более чем достаточно.

Загрузить VMware Server и VMware Player можно по адресам в Интернете:

- **http://www.vmware.com/download/server/**;
- **http://www.vmware.com/products/player/**.

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 репозиториев 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 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 программы устанавливаются без проблем, но затем, при попытке запуска установленной программы, система просит выполнить конфигурацию программы для работы с имеющимся ядром. В процессе конфигурации система просит указать расположение 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. Рас-

смотрим решение для Mandriva Linux, для других дистрибутивов Linux действуйте по аналогии.

Откройте утилиту установки и удаления программ (рис. 4.1). В левой части окна **Управление программами** в разделе **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-cpp.

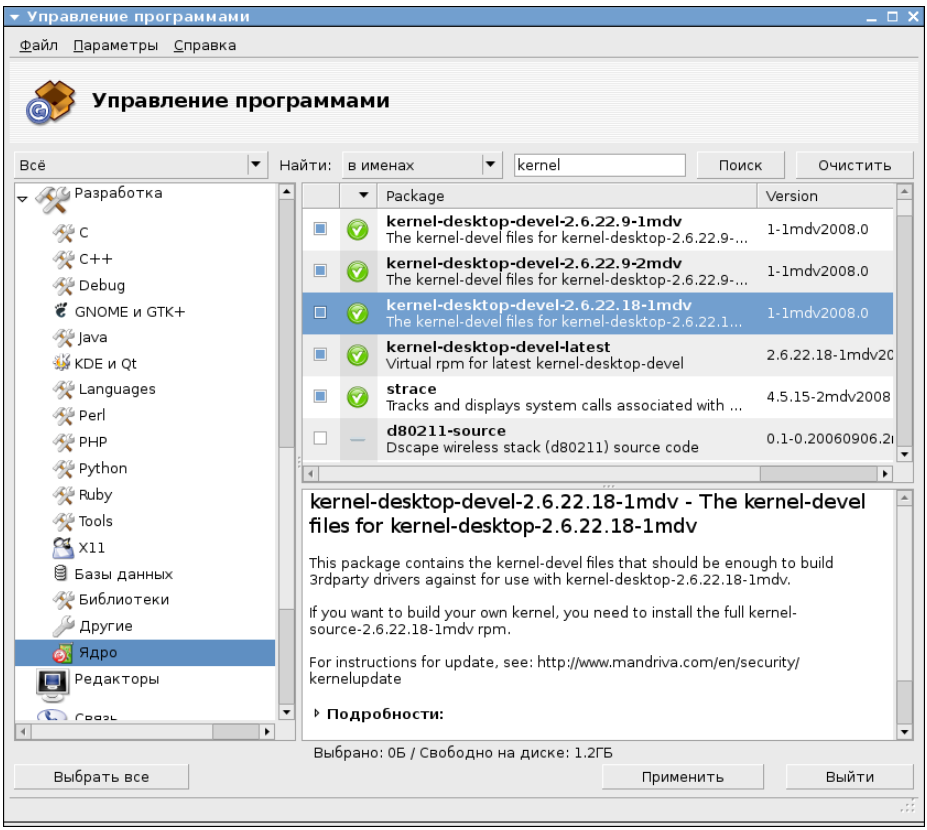


Рис. 4.1. Окно **Управление программами**, раздел **Ядро**

После добавления недостающих компонентов установка и конфигурация VMware Server и VMware Player пройдут без проблем.

В листинге 4.1 приведен вывод на экран в окне Терминала процесса конфигурации VMware Player с пояснениями, выделенными курсивом.

Листинг 4.1. 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 клавишу <Enter>

What directory contains your desktop menu entry files? These files have a
.desktop file extension. [/usr/share/applications] Нажимаем клавишу <Enter>

In which directory do you want to install the application's icon?
[/usr/share/pixmaps] Нажимаем клавишу <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 клавишу <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 клавишу
<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/phystrack.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/dbllnklst.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 клавищу <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]#
```

Конфигурация завершена.

Теперь, щелкнув правой кнопкой мыши на рабочем столе, выбираем команду **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. 4.2).

Рис. 4.2. Окно **VMware Player**

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.

В Windows процесс установки VMware Player и VMware Server проблем не вызывают, поэтому далее будем рассматривать работу с уже установленными программами. Единственно, о чем следует предупредить, — это необходимость в Windows установить компонент операционной системы **Службы IIS** (рис. 4.3).

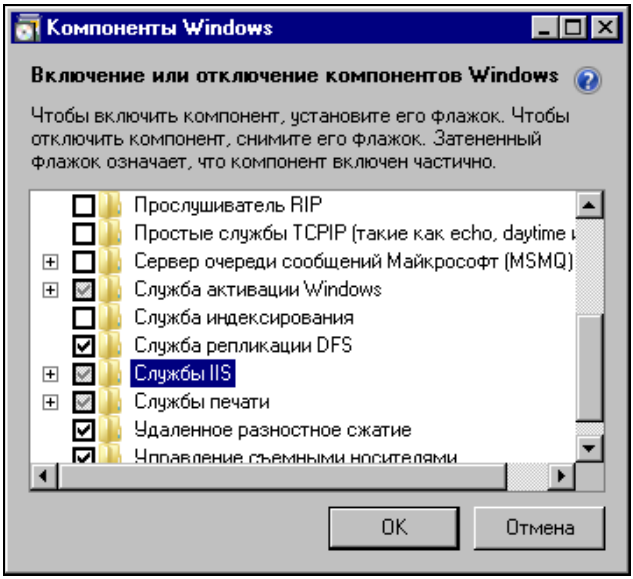


Рис. 4.3. Окно **Компоненты Windows**

Виртуальные технологии в нашей сети

Необходимые программы определили, с установкой разобрались. Рассмотрим теперь применение этих программ с пользой для нас и нашей сети 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

Brouser appliance — так называется виртуальный компьютер, предназначенный для посещения Интернета. Его операционная система — Ubuntu Linux —

вирусным заражениям практически не подвержена, 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 Brouser 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.

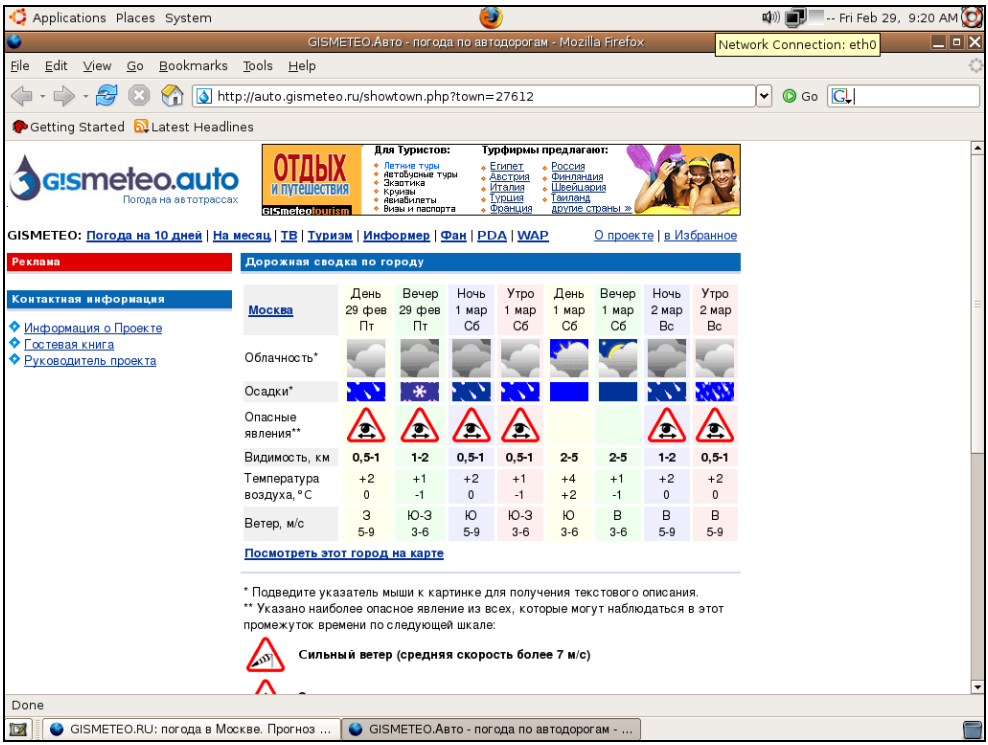


Рис. 4.4. Окно виртуальной машины Ubuntu Linux, запущенной в VMware Server, установленной на базовом компьютере Windows Vista Home Premium

Теперь запустите VMware Player или VMware Server. Откройте сохраненную виртуальную машину. Система Brouser appliance настроена таким образом, что после загрузки сразу откроется окно интернет-браузера Firefox. Сеть уже

настроена. Доступ в Интернет Brouser appliance получит через базовую машину с применением преобразования адресов (NAT). Никакие маршрутизаторы вам не потребуются. Все необходимые устройства созданы в виртуальной машине. Виртуальный компьютер включен в собственную подсеть, которая не имеет прямого выхода в вашу сеть. На рис. 4.4 показано окно запущенной виртуальной машины в программе VMware Server. Никаких дополнительных настроек не выполнялось. Единственное действие, которое выполнил автор после загрузки виртуальной системы, — это ввел в адресную строку браузера адрес сайта **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.

Виртуальная сеть

Попробуем настроить виртуальную машину с 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 Brouser appliance у нас уже настроены 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. 4.5), 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.

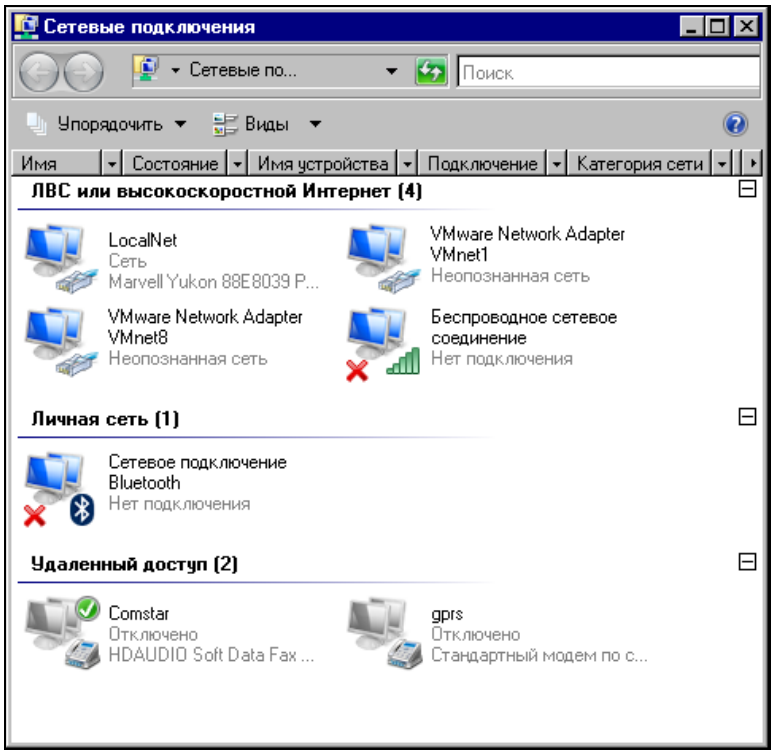


Рис. 4.5. Окно **Сетевые подключения**

Откройте **Virtual Network Editor** (Менеджер виртуальных сетей) с помощью **Пуск | Программы | VMware | VMware Server | Manager Virtual Networks**. В окне **Virtual Network Editor** на вкладке **Summary** (рис. 4.6) показаны адаптеры и сервисы, которые на них работают.

- **VMnet0 (Bredget)** — 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 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.

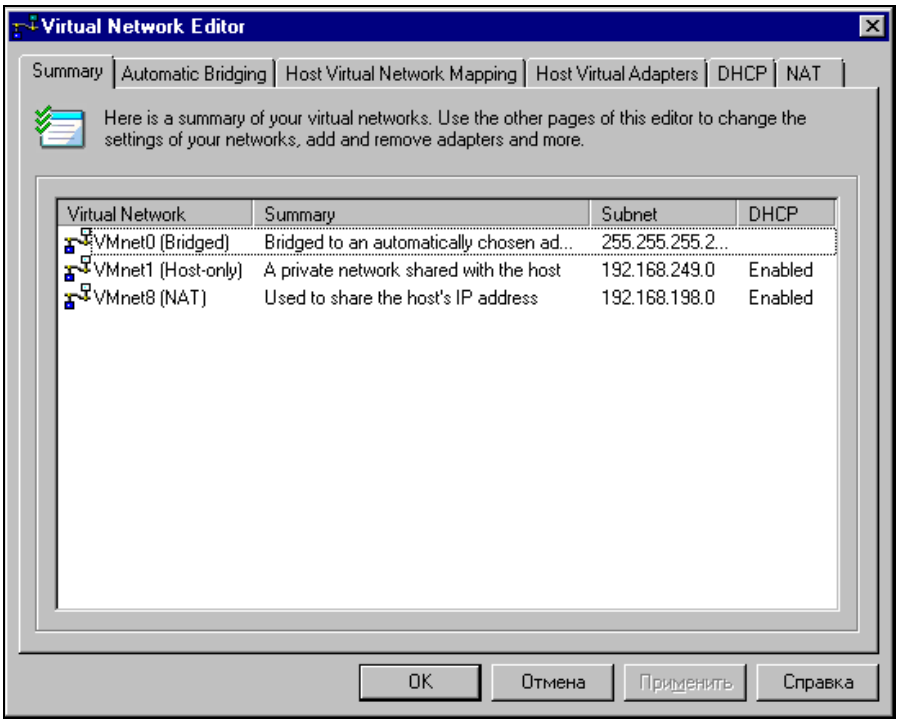


Рис. 4.6. Окно **Virtual Network Editor**, вкладка **Summary**

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 слу-

чай пролистайте вкладки окна **Virtual Network Editor** и запомните или запишите увиденные настройки. Хотя, вернуть настройки по умолчанию можно, переустановив VMware Server.

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 рисунке (рис. 4.7).

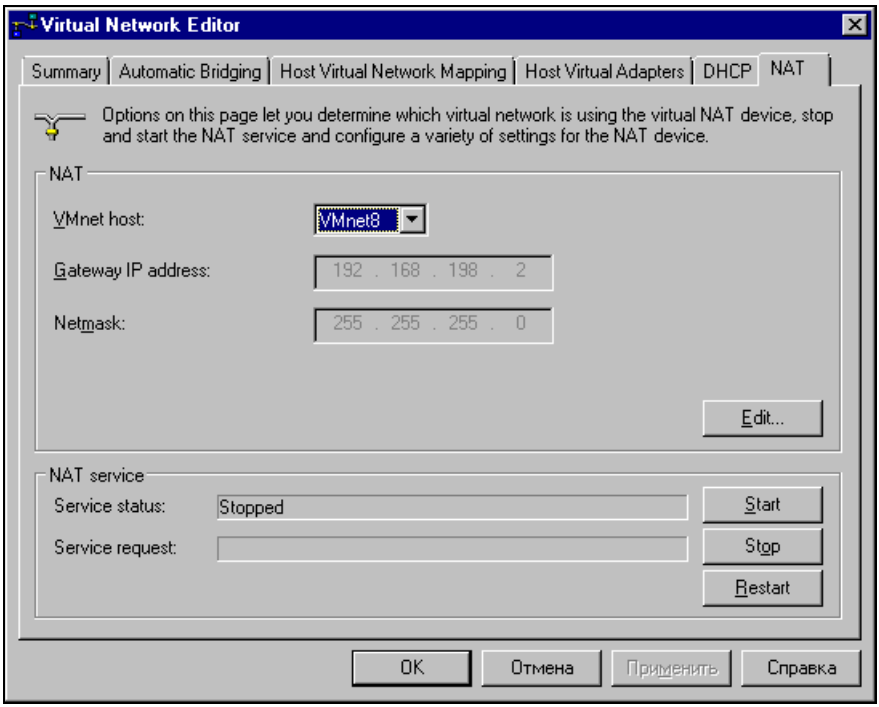


Рис. 4.7. Окно **Virtual Network Editor**, вкладка **NAT**

2. Перейдите на вкладку DHCP (рис. 4.8). Нажмите последовательно кнопки **Stop** и **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. 4.9). Выделяя каждую из имеющихся в окне строк, нажимайте кнопку **Disable**, а затем **Применить**. Этим действием мы отключим не требующиеся в нашем слу-

чае адаптеры. При желании их можно удалить совсем, если вы не планируете их использование в дальнейшем. Для этого следует нажимать кнопку **Remove** вместо **Disable**.

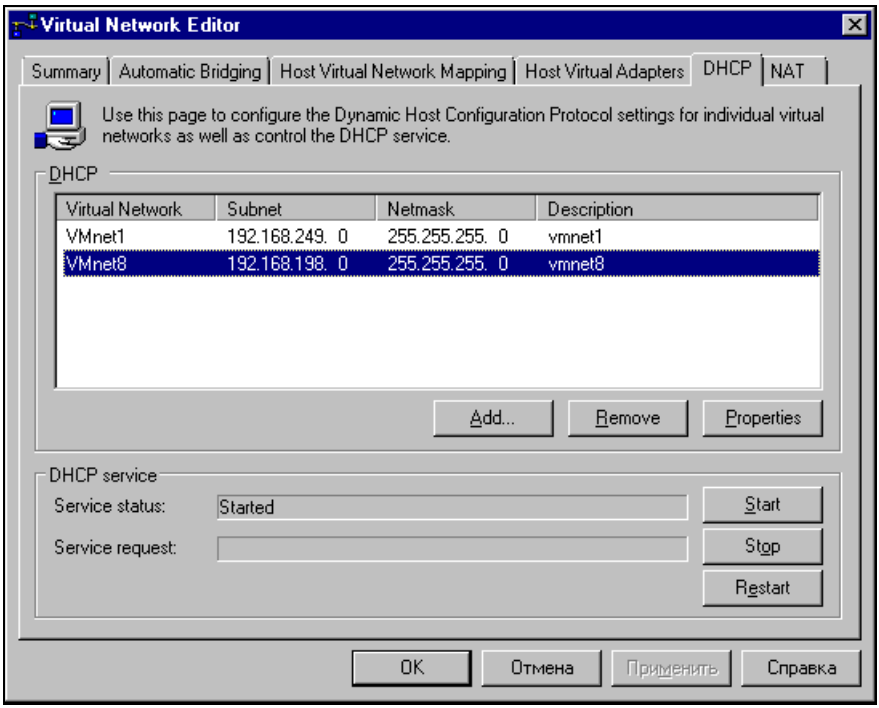


Рис. 4.8. Окно **Virtual Network Editor**, вкладка **DHCP**

4. На вкладке **Host Virtual Network Mapping** в выпадающем списке поля **VMnet0** (рис. 4.10) следует выбрать сетевой адаптер, через который базовый компьютер подключен к вашей сети.
5. И, наконец, на вкладке **Automatic Bridging** (рис. 4.11) ничего менять не надо. Флажок **Automatically choose an available physical network adapter to bridge to VMnet0** (Автоматический выбор доступного физического сетевого адаптера для моста на VMnet0) уже снят автоматически после выбора конкретного адаптера на предыдущей вкладке.

Сеть настроена. Остается запустить VMware Server Console (рис. 4.12), подключив ее к локальному серверу VMware Server (Local host), и поправить конфигурацию виртуальной машины.

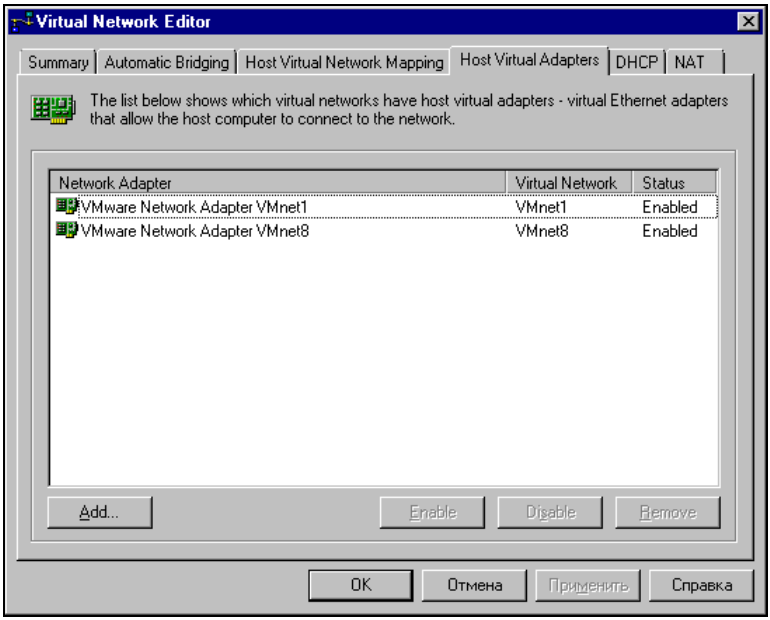


Рис. 4.9. Окно **Virtual Network Editor**, вкладка **Host Virtual Adapters**

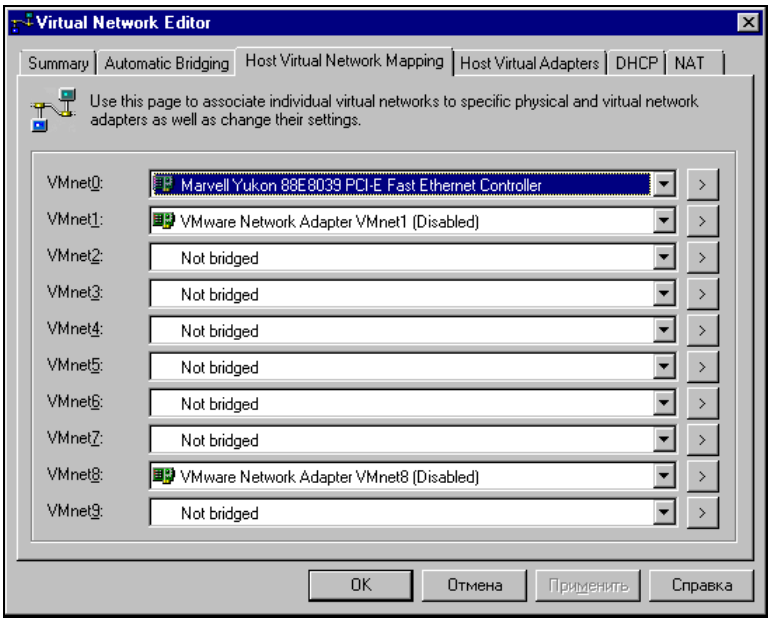


Рис. 4.10. Окно **Virtual Network Editor**, вкладка **Host Virtual Network Mapping**

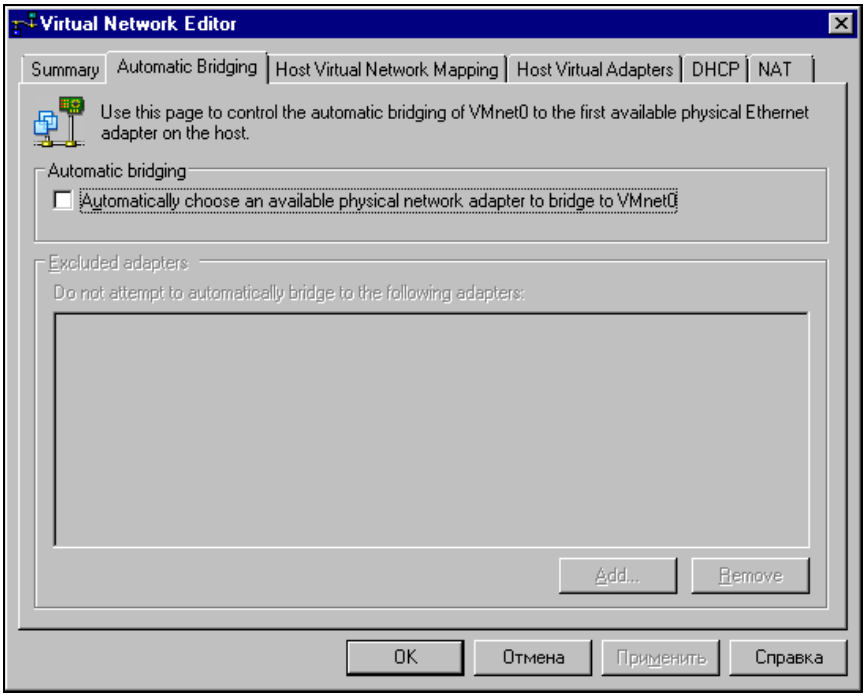


Рис. 4.11. Окно **Virtual Network Editor**, вкладка **Automatic Bridging**

Откройте окно **Virtual Machine Setting**, выбрав в левой части окна команду **Edit virtual machine settings** (Редактировать установки виртуальной машины).

В открывшемся окне (рис. 4.13) установите переключатель **Bridged: Connected directly to physical network** (Мост: подключен к физическому сетевому адаптеру).

Все. Настроена и сеть, и виртуальная машина. Теперь включите виртуальный компьютер командой **Start this virtual machine** (см. рис. 4.12) 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. 4.14). Если ответов на `ping` нет, то проверьте все настройки, описанные ранее.

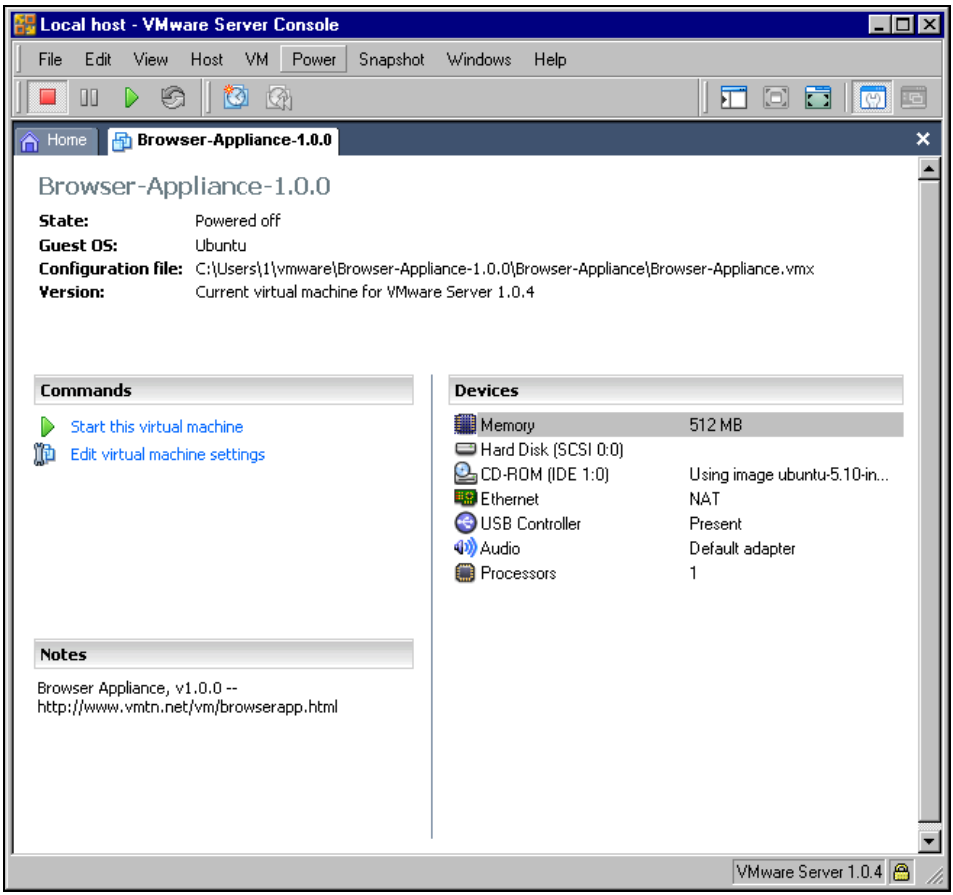


Рис. 4.12. Окно **Local host - VMware Server Console**

Если на виртуальном компьютере установлены все необходимые для работы в сети пакеты, через обозревателя сети можно будет увидеть доступные ресурсы (рис. 4.15). 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.

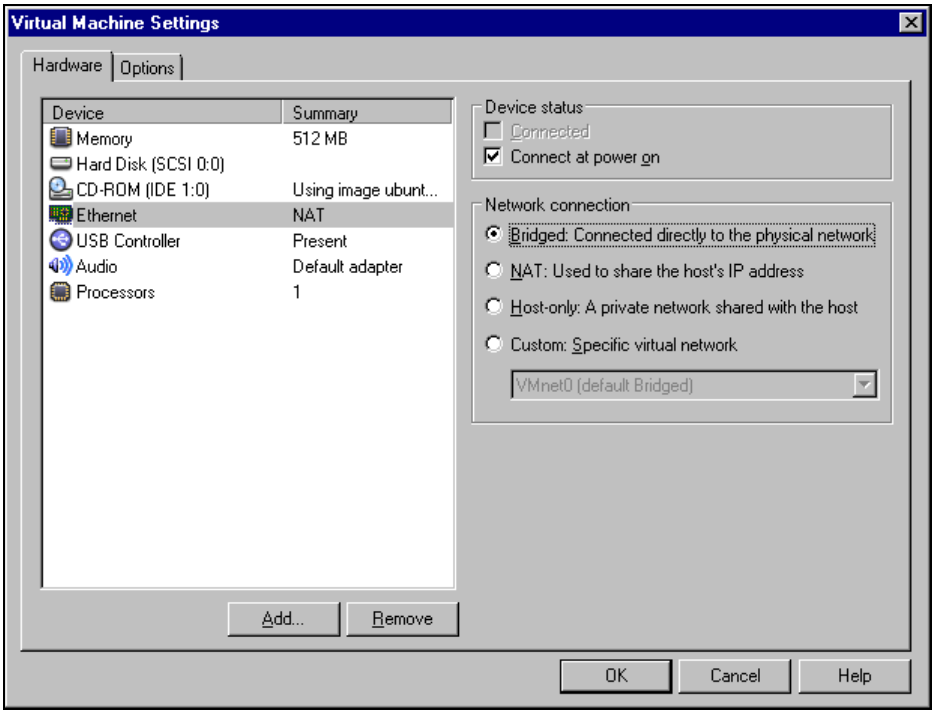


Рис. 4.13. Окно **Virtual Machine Settings**

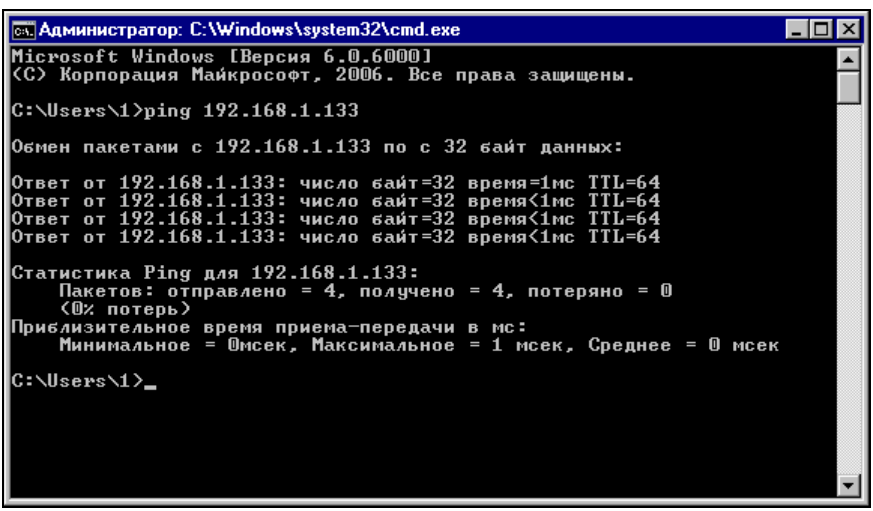


Рис. 4.14. Окно командной строки для выполнения команды `ping`

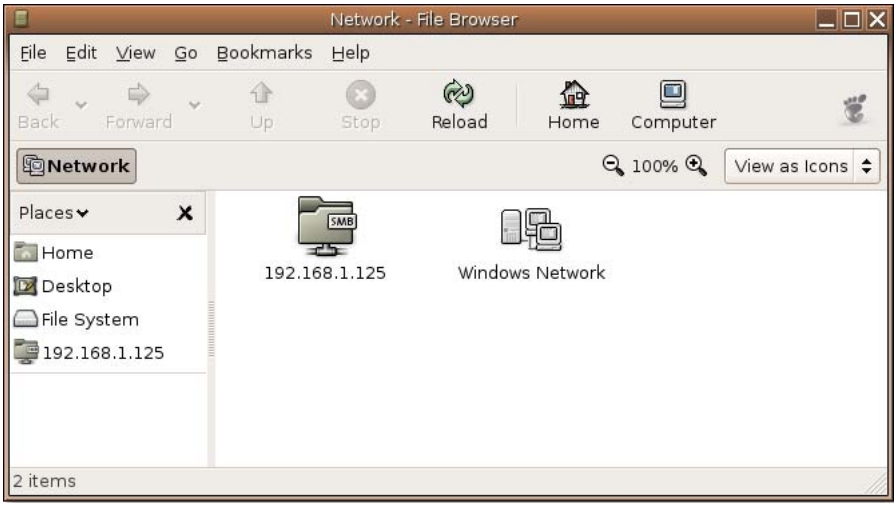


Рис. 4.15. Окно **Network - File Browser**

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.

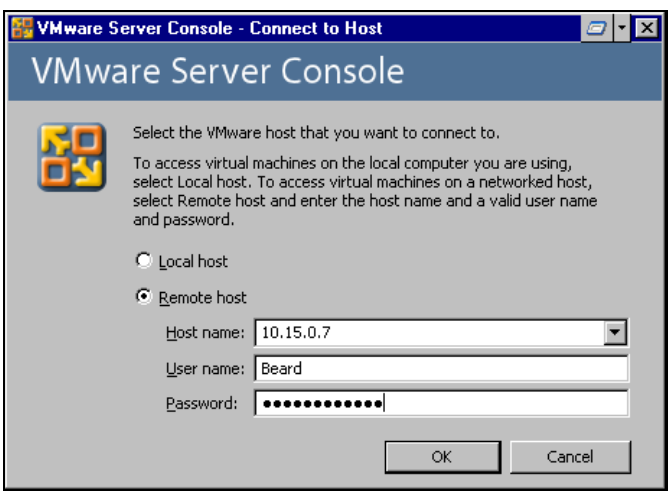


Рис. 4.16. Окно **VMware Server Console - Connect to Host**

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.

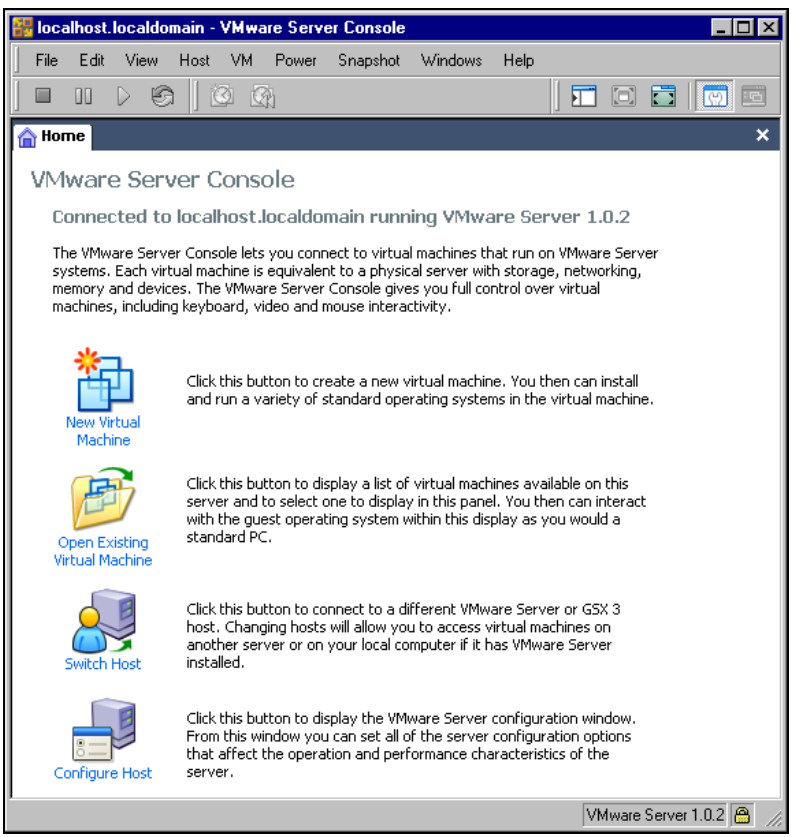


Рис. 4.17. Окно **VMware Server Console**

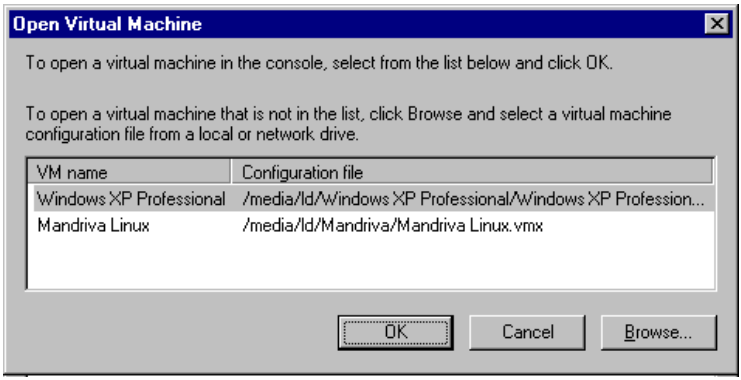


Рис. 4.18. Окно **Open Virtual Machine**

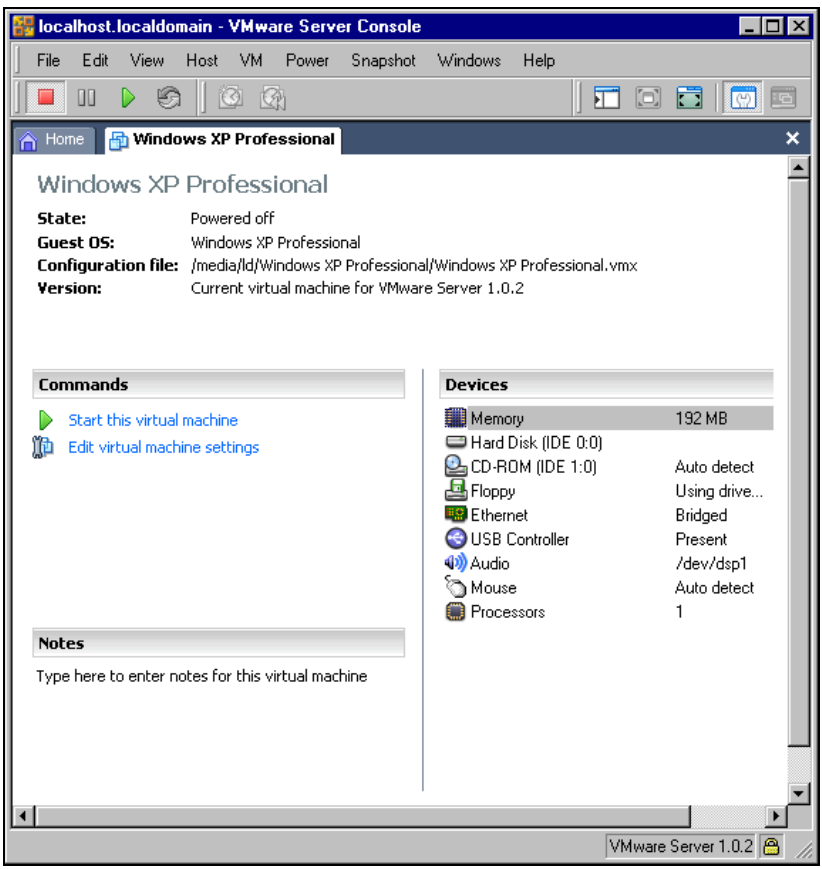


Рис. 4.19. Окно **VMware Server Console**, вкладка **Windows XP Professional**

При попытке подключения к удаленному компьютеру (Remote host) необходимо ввести его имя или IP-адрес, имя и пароль пользователя удаленного компьютера (рис. 4.16).

После ввода регистрационных данных откроется консоль управления виртуальным сервером на удаленном компьютере (рис. 4.17). 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. 4.18) необходимо выбрать одну из существующих виртуальных машин. Выбираем Windows XP и нажимаем кнопку **OK**.

Теперь в окне (рис. 4.19) **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. 4.20).

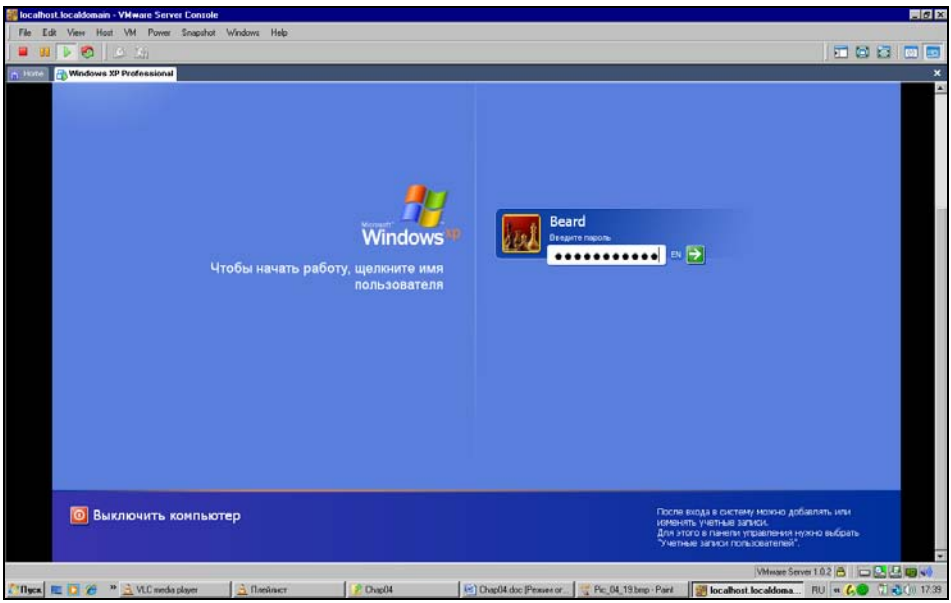


Рис. 4.20. Окно **VMware Server Console**, вкладка **Windows XP Professional**: экран входа в систему

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.

Рабочий стол виртуального компьютера может не помещаться в окне консоли управления на экране локального компьютера (рис. 4.21). С помощью полос прокрутки можно перемещать виртуальный рабочий стол в окне.

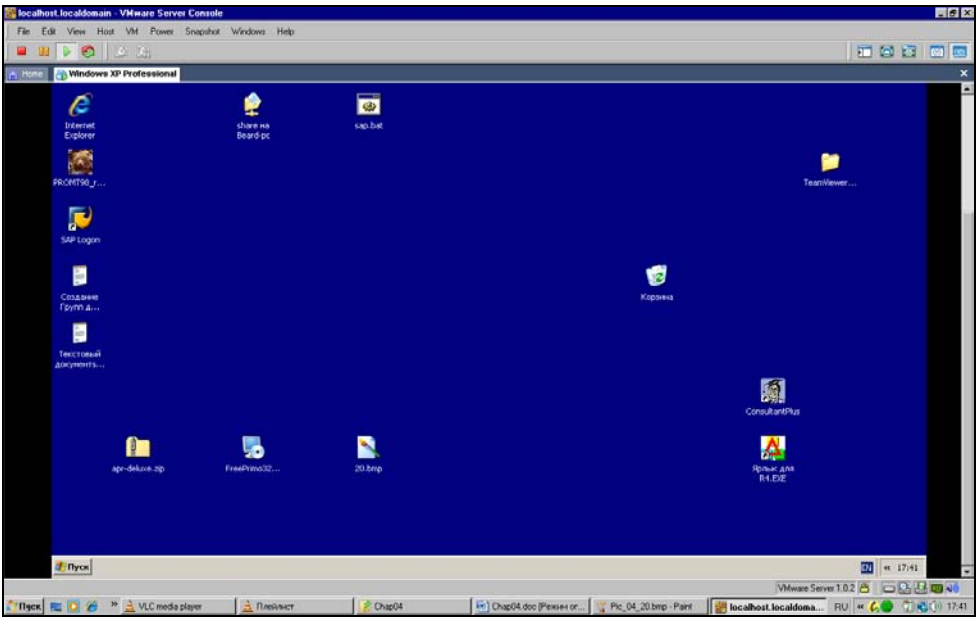


Рис. 4.21. Окно **VMware Server Console**, вкладка **Windows XP Professional**: экран загруженной системы

Как и любой реальный компьютер, виртуальная машина работает в сети (рис. 4.22). 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. 4.23). 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.

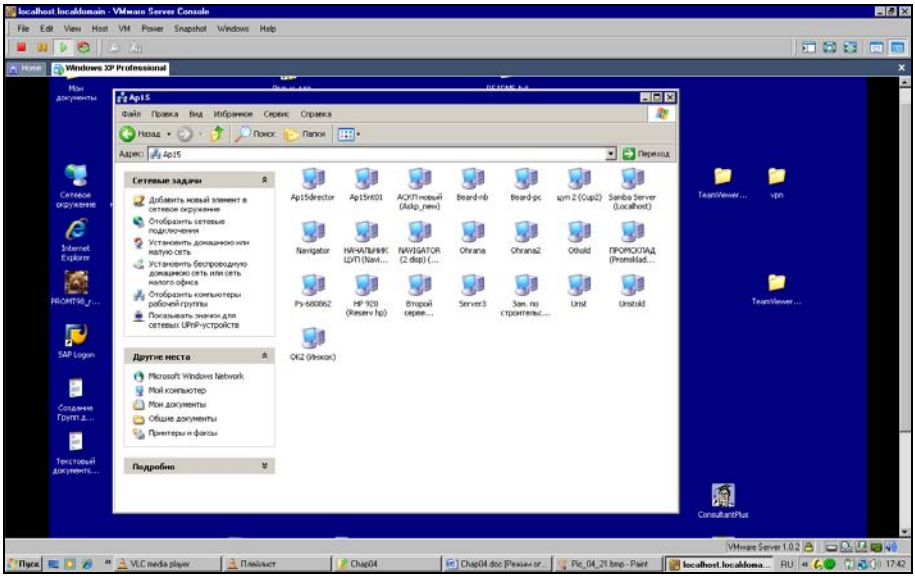


Рис. 4.22. Окно **VMware Server Console**, вкладка **Windows XP Professional**: экран загруженной системы и **Сетевое окружение**

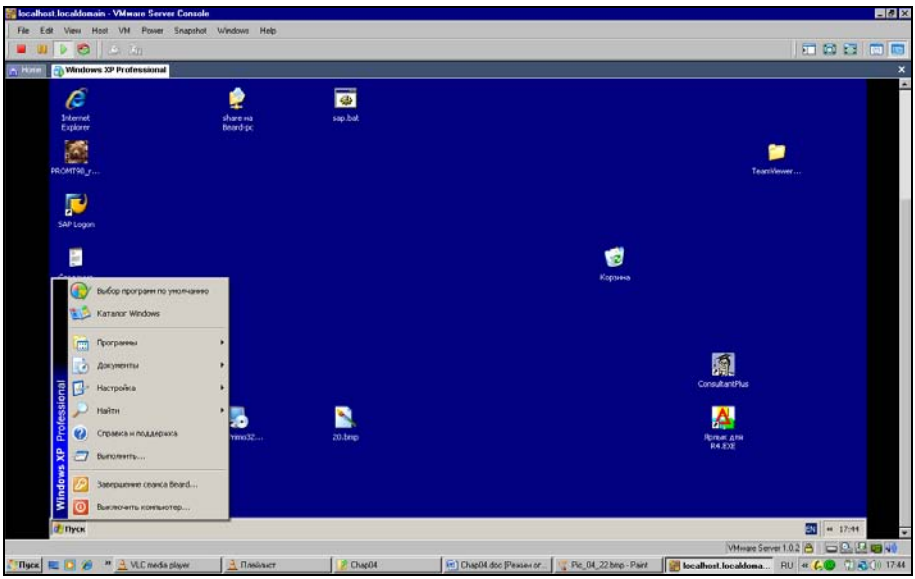


Рис. 4.23. Окно **VMware Server Console**, вкладка **Windows XP Professional**: экран загруженной системы, выключение

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 Windows. А часто под другими 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 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 операционкой. 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. То есть результаты работы в одой 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 спросит вас о необходимости создания нового уникального идентификатора виртуального компьютера (рис. 4.24). 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.

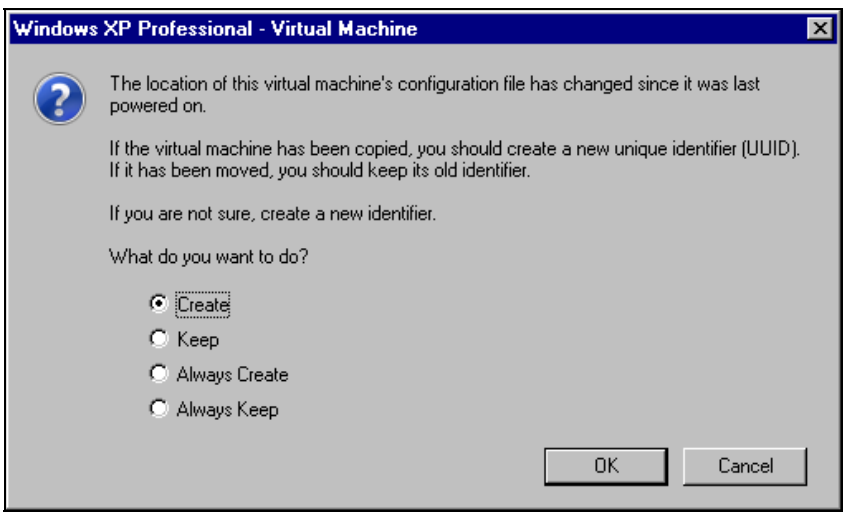


Рис. 4.24. Окно **Windows XP Professional - Virtual Machine**: создание нового уникального идентификатора

Виртуальные серверы разрабатываются не только VMware. Есть также бесплатная разработка у Microsoft. Возможно, вам эта программа понравится.

Устанавливаем Microsoft Virtual Server 2005 R2

Выбор этого сервера 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 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/windowsserversystem/virtualserver/downloads.aspx**. Для загрузки необходимо ввести данные регистрации в Windows Live (**http://www.windowslive.ru/**). С помощью VSMT можно преобразовать физические машины в VM, а виртуальные машины VMware VM — в совместимые с Virtual Server. Большинство пользователей Windows сможет без значительных проблем установить и освоить этот продукт.

Перед установкой виртуального сервера следует проверить, установлен ли у вас в системе компонент Internet Information Servises Manager из состава Internet Information Servises (IIS). Если компонент не установлен, то установите его. 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 инсталляции 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.

После установки виртуального сервера в окне браузера откроется страница с информацией о результатах установки (рис. 4.25)

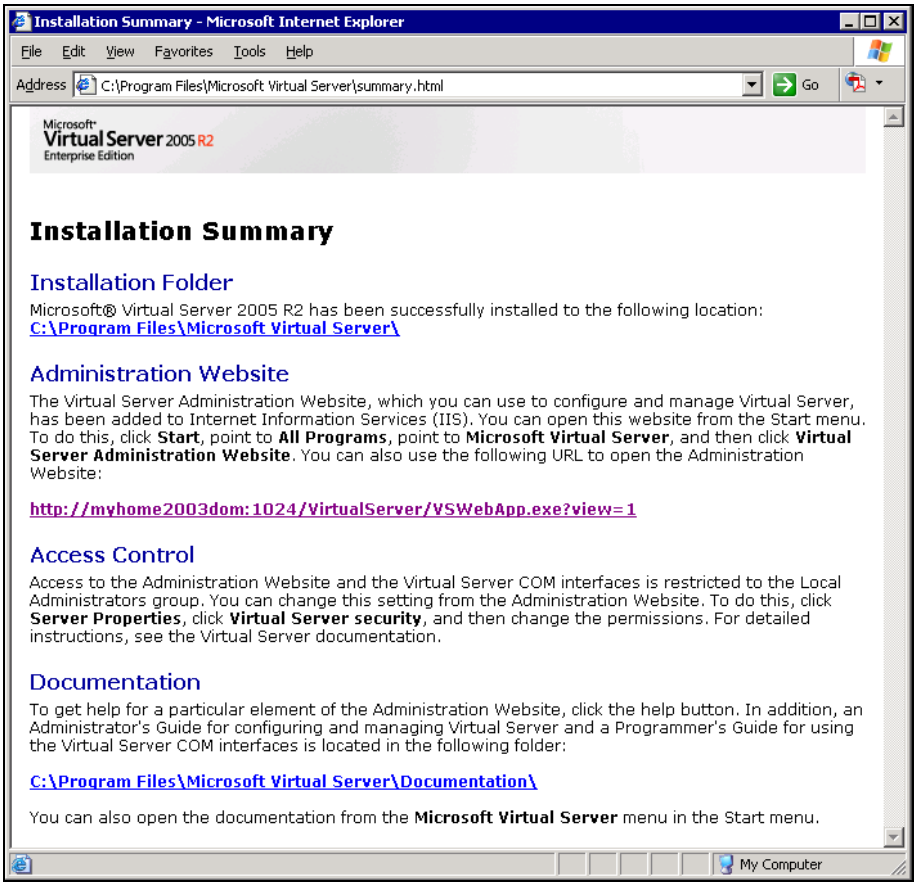


Рис. 4.25. Окно браузера с Installation Summary

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 | Создать), вы попадете в интерфейс создания новой виртуальной машины (рис. 4.26).

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 **OK**. В процессе создания виртуальной машины программа предложит отключить автозапуск CD-ROM. Автозапуск будет мешать подключению дисковода к виртуальной машине.

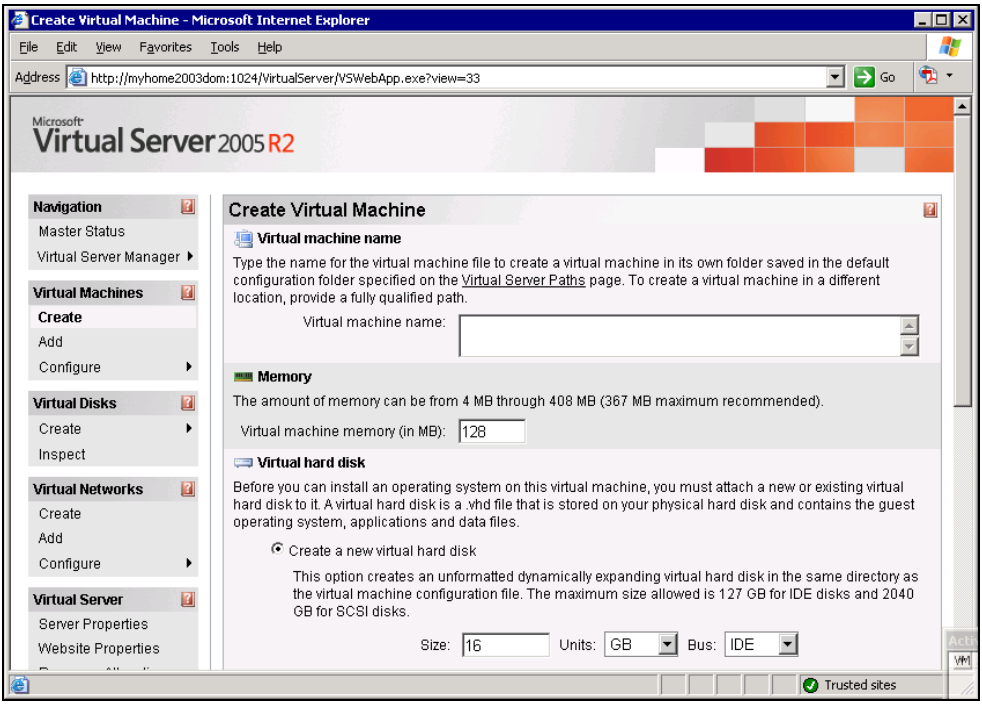


Рис. 4.26. Окно браузера
с открытым разделом **Create Virtual Machine**

После создания виртуальной машины перейдите в меню **Master Status** (Страница состояния сервера) (рис. 4.27).

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 через меню **Пуск** запустить Virtual Machine Remote Control (рис. 4.28).

Пользуясь этим окном, вы сможете провести установку системы, а в дальнейшем просто работать в системе, производя необходимые настройки сервера (рис. 4.29).

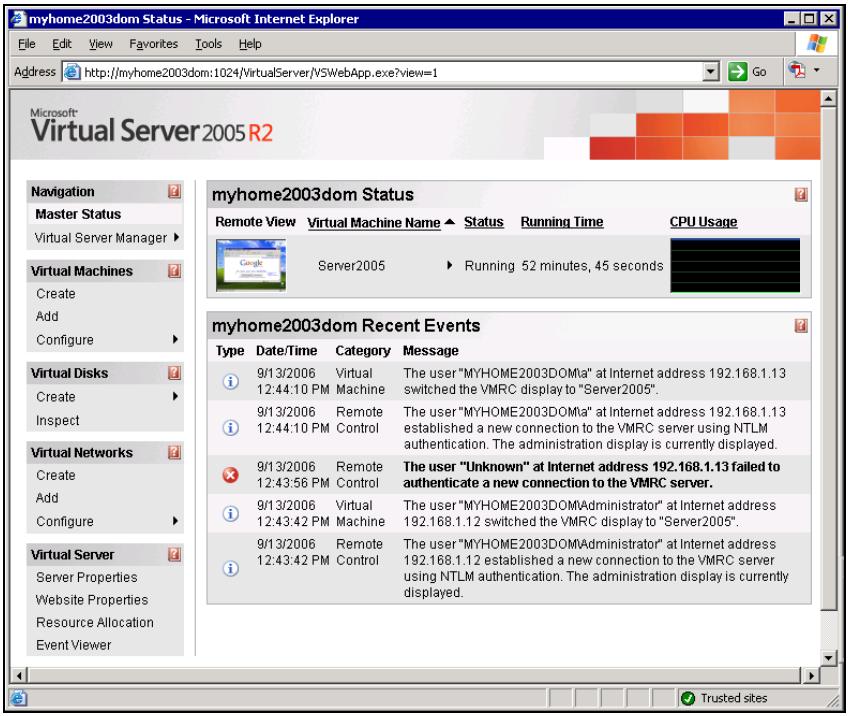


Рис. 4.27. Окно браузера с информацией о Virtual Machine Status

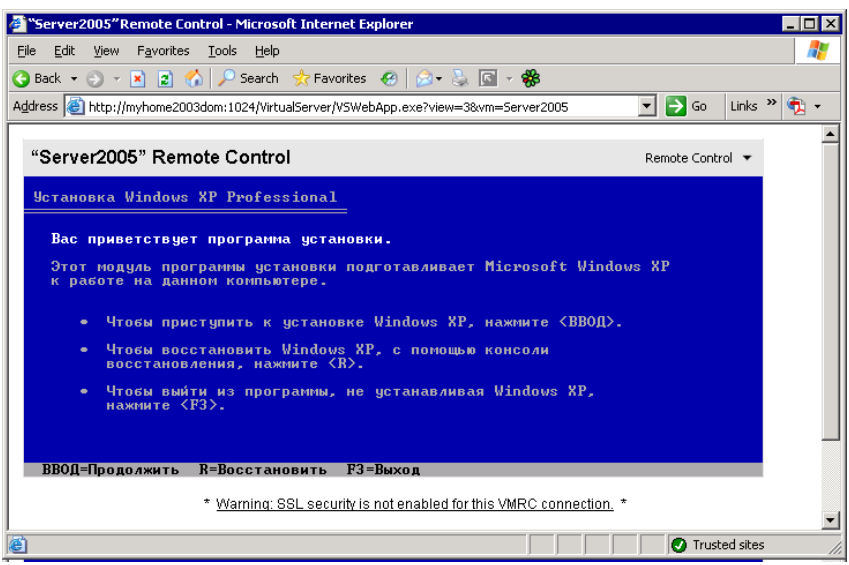


Рис. 4.28. Окно браузера Virtual Machine Remote Control: установка системы

Рис. 4.29. Окно браузера Virtual Machine Remote Control: система установлена

Учитывая виртуальность сервера, вы можете создавать любое мыслимое число виртуальных машин, сохранять удачные, уничтожать непонравившиеся вам и запускать несколько виртуальных машин одновременно. При этом Virtual Machine Remote Control позволит переключаться между созданными машинами.

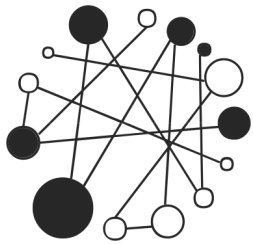
Создав более одного виртуального сервера, вы сможете подключаться с клиентского компьютера к любому из них. Установив на виртуальный сервер серверную версию операционной системы, вы можете осваивать варианты настройки сервера, применив впоследствии полученный опыт.

Возможно, что вам будет интересно прочитать некоторые подробности о виртуальном сервере Microsoft. Это можно сделать на страницах **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. Тогда можно заранее создать необходимые виртуальные машины, перенести их на физические машины, где они должны работать, а запускать их можно с помощью VMware Player.

Есть, конечно, определенные неудобства при работе с удаленной виртуальной машиной. Нет возможности напрямую использовать CD-привод или флэш-карты. Но такие неудобства существуют и при удаленной работе с физическими машинами. 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. Возможности удаленной работы с компьютерами нашей сети мы рассмотрим в следующей главе.

Глава 5



Работа с удаленными компьютерами

По опыту автора, этот вопрос волнует пользователей ПК с тех пор, как персональные компьютеры перестали быть редкой роскошной игрушкой. То есть более двадцати лет. Получив в свое распоряжение компьютер и средства для подключения к сети, пользователи ПК ищут способы взаимодействия с компьютерами своих друзей или коллег. Даже когда единственным средством коммуникации были телефонные сети, уже разрабатывались программы для удаленного управления компьютерами, для совместной работы на них посредством обычных аналоговых модемов. В компьютерной литературе прошлых лет можно найти немало вариантов реализации этой идеи. Были разработаны различные программы терминального доступа, которые требовали большого опыта в настройке модемов и немало сил от начинающих пользователей для освоения самих программ. Время идет. Совершенствуются программы, операционные системы, сами компьютеры и сервисы в Интернете, предназначенные для решения задач удаленного управления, администрирования и взаимодействия компьютеров. Еще в *главе 1* мы создали простую сеть. Современные компьютеры в пределах этой сети без особого труда можно заставить обмениваться файлами. Получив доступ в Интернет, можно использовать программы для общения между компьютерами *(см. главу 3)*. С помощью виртуального сервера можно работать с виртуальной машиной, установленной на компьютере, подключенном к сети *(см. главу 4)*. Но нам всегда хочется большего! Мы хотим подключиться к компьютеру своего друга в другой сети, поработать на своем домашнем компьютере из интернет-кафе или со своего ноутбука, находясь далеко от дома, хотим из дома поработать на своем рабочем компьютере, подключиться к компьютеру друга — начинающего пользователя ПК, находящегося в другом городе, и оказать ему помощь. Не слишком ли многого мы хотим? Да, нет. Это лишь малая часть того, что позволяют нам делать современный персональный компьютер и

сеть. Правда, сеть теперь будем понимать в более широком смысле, чем только наша домашняя сеть. Можно объединить нашу домашнюю сеть с другой компьютерной сетью. Эта другая сеть может быть такой же домашней в вашем доме или сетью вашего предприятия, находящейся в десятках километров от вас.

Смешанная сеть

Комбинированные сети, состоящие из нескольких мелких сетей и/или имеющие выход в Интернет и связанные чрез эту глобальную сеть, называют *смешанными*. К смешанным сетям можно отнести и сеть, состоящую всего из двух компьютеров, связанных не кабелем или двумя беспроводными адаптерами, а посредством другой сети, например, Интернета. Теоретические основы работы смешанных сетей значительно сложнее, чем обычных локальных. Но современное программное обеспечение, сервисы в Интернете, само оборудование достигли такого уровня совершенства, что создание смешанной сети зачастую под силу рядовому пользователю ПК с пытливым умом и, как говорят, "прямыми" руками.

Один из вариантов смешанной сети показан на рис. 5.1. Две локальных сети, имеющих выход в Интернет, соединены защищенным каналом VPN (Virtual Private Network, виртуальная частная сеть). Установлена связь между компьютером администратора, находящимся в сети № 1, и сервером сети № 2. Реально канал связи, конечно, проходит в Интернете, но для пользователей и компьютеров этот канал выглядит так, как будто проложен отдельный кабель. Никакой связи между этим каналом и Интернетом нет. Это значит, что канал защищен со стороны Интернета, а связь через него абсолютно безопасна.

На рисунке в сети № 2 один из компьютеров обозначен, как сервер. В нашей сети такого компьютера еще не было, но мы уже знакомы с DHCP- и DNS-серверами. В больших сетях есть выделенные компьютеры, предназначенные для управления всей сетью, учета пользователей сети, обеспечения безопасного доступа в сеть только зарегистрированным в ней пользователям и компьютерам. В этой книге мы не рассматриваем такие сети, но надо сказать, что сервером может быть любой из ваших компьютеров, если он предоставляет другим компьютерам в вашей сети или сети, связанной с вашей сетью, какие-либо услуги (сервисы).

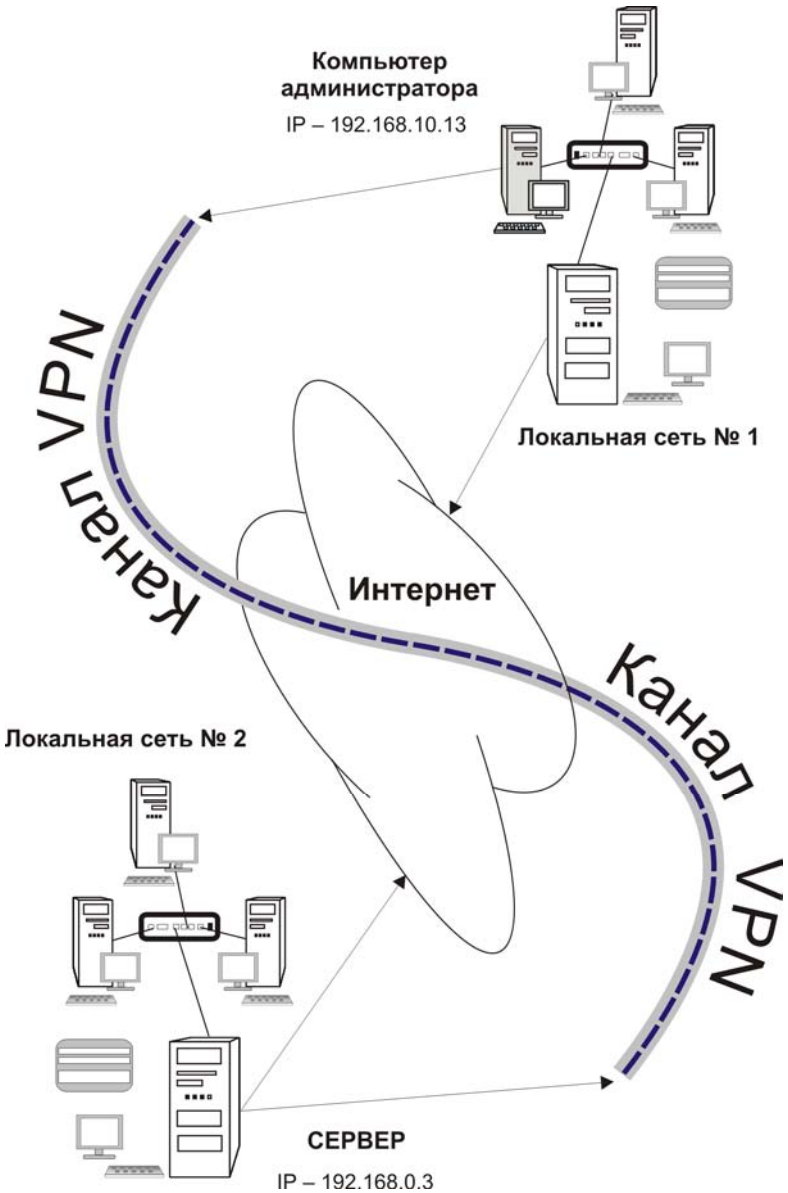


Рис. 5.1. Связь двух сетей через Интернет

Например, компьютер, предоставляющий общее подключение к Интернету, можно назвать сервером общего доступа в Интернет, а компьютер, на котором расположен каталог или каталоги общего доступа, — это файловый сер-

вер. Как видите, все достаточно просто. В области знаний о компьютерных сетях применимо старое, но верное до настоящего времени анекдотичное определение ученого человека.

> ***Чем отличается ученый человек от неученого?***
>
> Ученый в какой-либо области знаний или деятельности человек знает, что и как называется, а неученый делает все то же самое, но не знает, как это называется.

Это не значит, конечно, что не надо знать термины, относящиеся к компьютерным сетям, и их значение. Вполне вероятно, что сами для себя вы сможете сделать многое, но сеть — явление коллективное. А общаясь с себе подобными, следует говорить на одном языке. Иначе, как при строительстве Вавилонской башни, люди перестанут понимать друг друга, и общее коллективное дело станет невозможным.

Еще один термин, который еще не упоминался ранее в книге, — VPN. Как и виртуальные компьютеры, частные виртуальные сети получают все большее распространение, объединяя разделенные расстоянием офисы организаций в единую сеть. Теория VPN достаточно сложна, но практическая реализация такой сети вполне возможна даже для не обладающего соответствующим дипломом человека. Важно лишь найти соответствующее вашим задачам программное обеспечение и выполнить необходимые для решения этих задач условия.

Безграничное расширение домашней сети

Итак, наша задача — связать две сети или два компьютера через Интернет таким образом, чтобы для пользователя создавалась иллюзия работы в обычной локальной сети. На первый взгляд задача очень сложна, но, если выполняются некоторые необходимые условия, она вполне выполнима.

Для того чтобы, не обладая специальными знаниями, получить положительный результат, необходима возможность экспериментировать. Эксперименты проще проводить в ограниченном небольшом пространстве. Поэтому создание VPN мы начнем с нашей локальной сети. Создадим виртуальную сеть между двумя стоящими рядом компьютерами. Вполне возможно, что, имея опыт работы с виртуальными компьютерами, вы найдете применение таким сетям и в вашей сети. А если нет, то опыт создания такой миниатюрной сети

станет основой для создания настоящей VPN, которая может соединить компьютеры, удаленные друг от друга на неограниченное расстояние.

Приступим.

OpenVPN

Среди различных способов организации связи с сетью есть один, который становится все более популярным и распространенным. Используя его, некоторые провайдеры предоставляют доступ в Интернет своим клиентам VPN (Virtual Private Network, виртуальная частная сеть). Способов реализации VPN существует на сегодняшний день великое множество. Но нас, с точки зрения самостоятельного создания, может интересовать не слишком сложный в настройках, но полезный для организации подключений типа "точка — точка" вариант. В сети автора давно и успешно применяется средство под названием OpenVPN. Это открытая и бесплатная разработка, начавшая свое развитие в Linux, но имеющая версию и для Windows.

Организация доступа к локальной сети или удаленному компьютеру посредством OpenVPN позволяет решить задачу доступа пользователя к своим файлам и принтерам. При этом в сетевом окружении будут необходимые папки, а для печати документов можно использовать принтер, подключенный к удаленному компьютеру, к которому осуществлено подключение через VPN. Задержки передачи информации между компьютером удаленного пользователя и сетью не повлияют на скорость обычной работы с документами. В зависимости от скорости передачи информации через применяемое подключение к Интернету будут более или менее значительными время копирования файлов и время печати документа. Само по себе соединение устанавливается достаточно быстро даже при использовании выхода в Интернет через обычный модем. У автора соединение устанавливается в течение сорока секунд. При этом удаленный компьютер находится на расстоянии более 50 км от места подключения. Единственное условие, которое должно быть соблюдено, — это наличие у рабочей станции, с которой осуществляется доступ к сети, реального (пусть даже динамически выделяемого) IP-адреса, а у компьютера, через который подключена к Интернету локальная сеть, должен быть постоянный IP-адрес, выделенный поставщиком услуг Интернета. Правда, есть возможность обойти второе условие, воспользовавшись определенными сервисами в Интернете. Применение VPN позволяет предоставить доступ к файлам и принтерам удаленного компьютера, использовать про-

граммы для связи между двумя компьютерами и совместной работы пользователей, такие как Конференц-зал Windows (рис. 5.2). Для работы этой программы требуется наличие одноранговой сети или VPN.

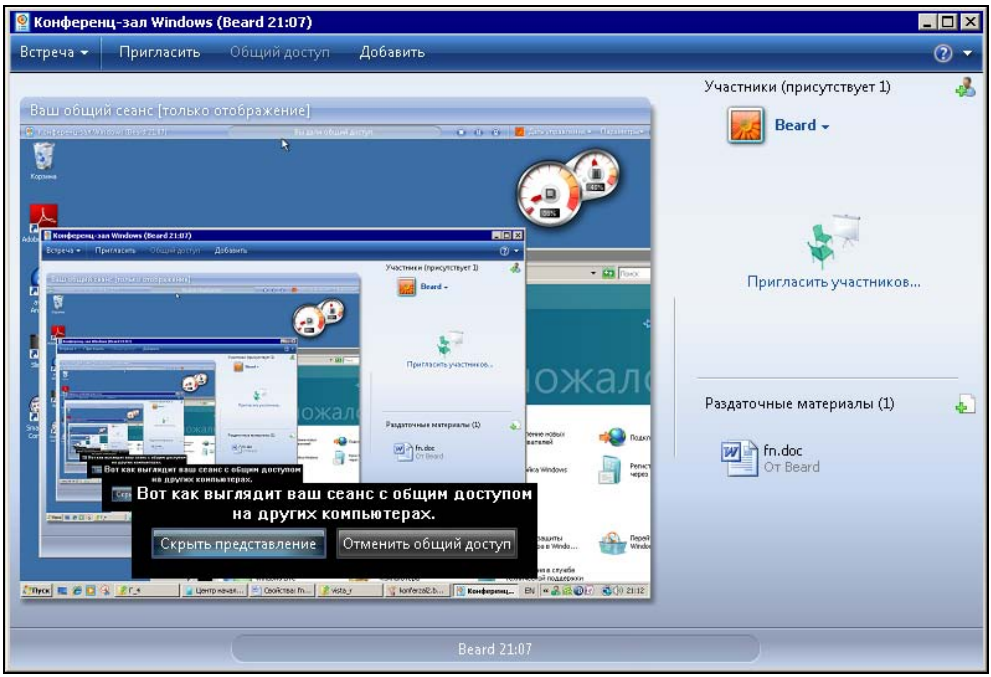


Рис. 5.2. Окно **Конференц-зал Windows**

Конференц-зал Windows позволяет не только общаться, но и предоставлять для использования файлы, программы, осуществлять доступ к рабочему столу. Аналога этой программы для Linux по сведениям, имеющимся у автора, нет, но есть другие межплатформенные разработки, которые совместно с программами мгновенного обмена сообщениями могут применяться для работы через VPN. Пример такой программы будет рассмотрен в этой главе.

Методы шифрования, применяемые для организации VPN, не позволят постороннему перехватить передаваемую информацию, пароли и получить доступ к сети или удаленному компьютеру.

OpenVPN можно найти по адресу в Интернете: **http://openvpn.sourceforge.net**. Получить последнюю версию программы можно на странице **http://openvpn.net/index.php/downloads.html**. Для загрузки доступны версии для Linux и

Windows. В некоторых дистрибутивах есть встроенные средства для настройки OpenVPN, например, в Mandriva Linux.

Настройка OpenVPN в Windows

Серверная и клиентская части программы ничем не отличаются, кроме нескольких строчек в файле конфигурации программы.

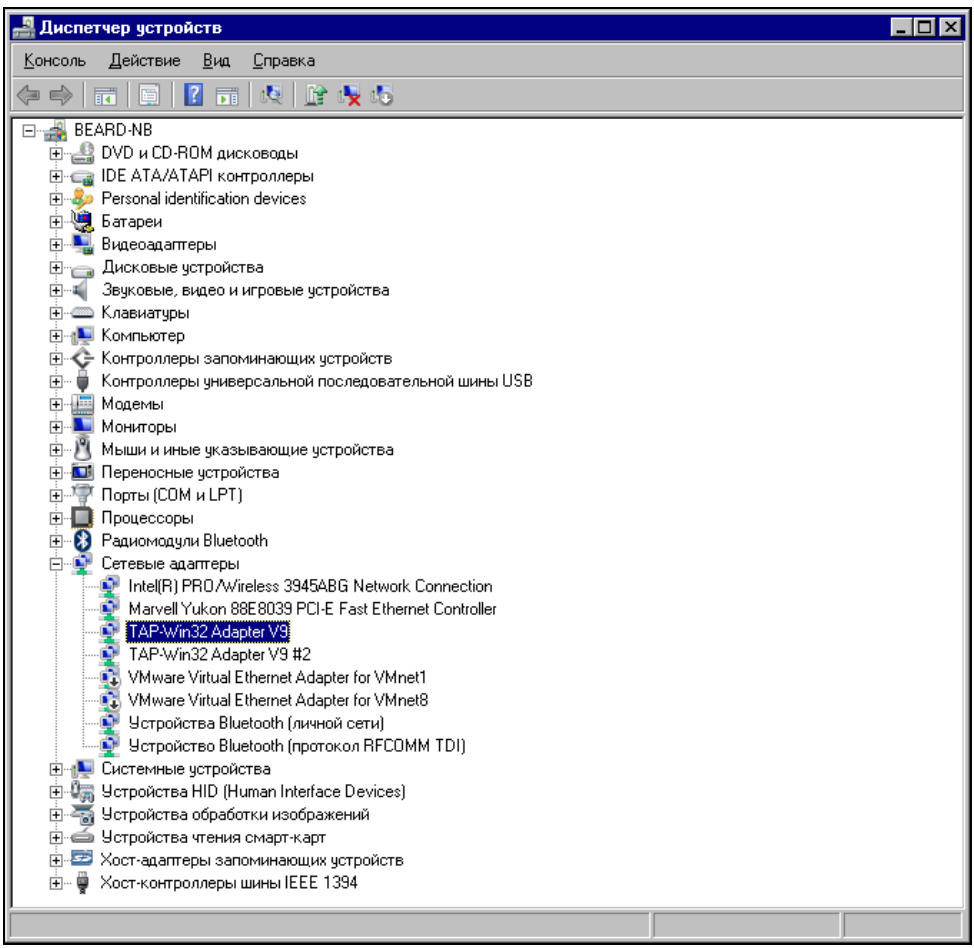


Рис. 5.3. Окно **Диспетчер устройств**.
Новые адаптеры в перечне оборудования компьютера

В режиме сервера программа может быть запущена в качестве службы. После установки программы будет создан виртуальный сетевой адаптер. При необходимости можно создавать дополнительные сетевые адаптеры, для этого следует выполнить последовательно **Пуск | Программы | OpenVPN | Utilities | Add a new Tap-Win32 virtual Ethernet adapter**. В данном примере созданы два новых виртуальных сетевых адаптера (рис. 5.3) и соответствующие им два новых сетевых подключения, которые следует переименовать, как показано на рис. 5.4, в VPN1 и VPN2 для удобства написания этих имен в файлах конфигурации.

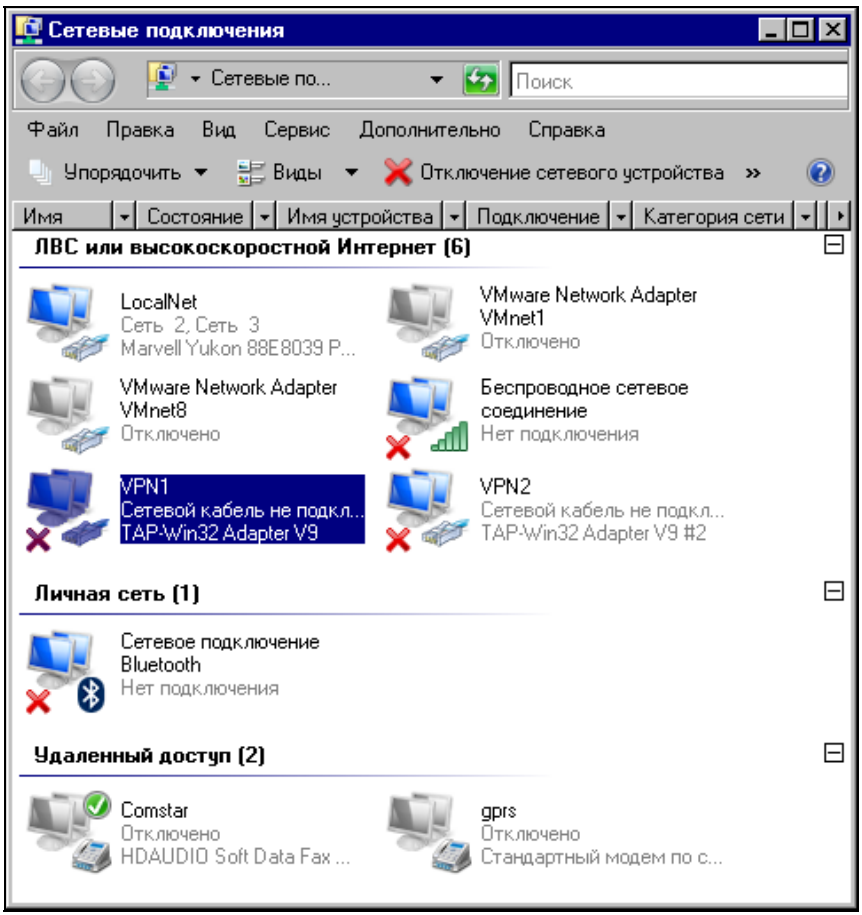


Рис. 5.4. Окно **Сетевые подключения**.
Новые сетевые подключения VPN1 и VPN2

Это необходимо и потому, что программа работает в режиме командной строки, где короткие имена предпочтительны.

Файлы конфигурации для сервера и клиента в самом простом варианте приведены в листингах 5.1 и 5.2.

Листинг 5.1. Файл конфигурации client.ovpn для клиента OpenVPN

```
# имя компьютера, к которому осуществляем доступ
remote Beard-NB
# порт, через который осуществляется связь (любой свободный)
port 35000
# указание на роль компьютера в VPN
proto tcp-client
dev tap
ifconfig 192.168.116.3 255.255.255.0
dev-node VPN1
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

Листинг 5.2. Файл конфигурации server.ovpn для сервера OpenVPN

```
port 35000
proto tcp-server
dev tap
ifconfig 192.168.116.1 255.255.255.0
dev-node VPN1
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

В обоих файлах имя сетевого подключения (dev-node) — VPN1. Сетевые подключения настройки не требуют, их параметры устанавливаются самой программой. Так, в клиентском файле есть строка

```
ifconfig 192.168.116.3 255.255.255.0
```

Эта строка устанавливает IP-адрес для подключения VPN 192.168.116.3, а маску подсети 255.255.255.0. Файлы должны иметь расширение ovpn. При этом в контекстном меню этих 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`). Указывать можно как имя, так и IP-адрес. При указании имени должна быть обеспечена его связь с IP-адресом одним из доступных способов. Это может быть указание DNS-сервера, который разрешит имя в адрес, а может быть и просто запись в файле C:\Windows\system32\drivers\etc\Hosts. Запись в этом файле — просто строка, содержащая IP-адрес и имя компьютера через пробел после адреса. В описываемом примере строка в файле Hosts выглядит так:

```
192.168.1.125  hp-admin
```

Адрес в файле Hosts отличается от адреса в файле конфигурации. Это связано с тем, что адрес основного сетевого адаптера не совпадает с адресом адаптера, созданного программой OpenVPN.

Если до вашего компьютера `ping` не доходит, хотя по вашему мнению все настроено правильно, убедитесь, что в настройках брандмауэра или файервола указаны правила, разрешающие двухсторонний обмен данными по протоколу ICMP. С предустановленной системой Windows Vista нередко прилагается программа Norton Internet Security, имеющая в своем составе брандмауэр с довольно строгими настройками по умолчанию. На рис. 5.5 приведено окно **Norton Internet Security** на странице **Общие правила**. В нем выделено правило для исходящих ICMP, скорректированное для двунаправленной работы.

OpenVPN-сервер, запущенный на сервере сети, ожидает попыток подключения извне. При удачной попытке сетевое подключение **VPN** активизируется (рис. 5.6). При этом в окне командной строки последней строчкой появляется запись `Listening for incoming TCP connection on [undef]:35000`, сообщающая, что сервер ожидает входящие подключения на порту 35000.

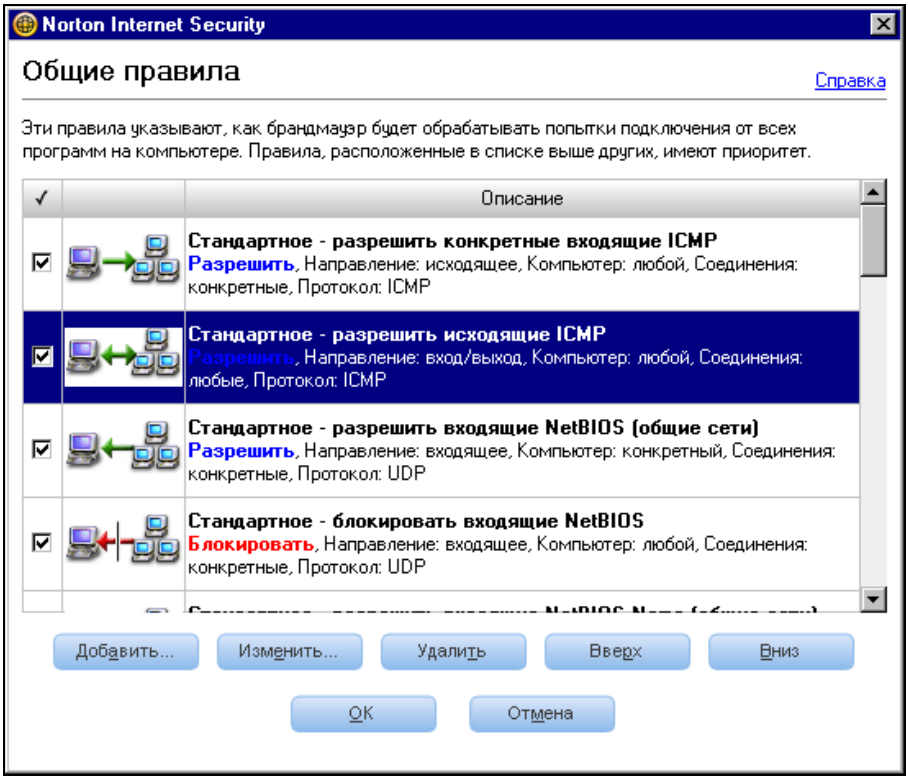


Рис. 5.5. Окно **Norton Internet Security**, страница **Общие правила**

Слегка забегая вперед, скажем, что при установлении входящего подключения запись в последней строке будет иной — "Initialization Sequence Completed" ("Инициализация завершена").

Запуск OpenVPN-сервера в окне командной строки требуется только на этапе настройки программы. После завершения всех настроек можно запустить службу OpenVPN Service в окне **Службы** (рис. 5.7), которое можно открыть по пути **Панель управления | Администрирование | Службы**. Если для этой службы установить автоматический запуск, то сервер будет запускаться сразу после включения компьютера.

Клиентская часть программы запускается на компьютере, с которого мы хотим получить доступ к серверу. OpenVPN-клиент после запуска предпринимает попытки определить доступность сервера по его имени, если оно указано в файле конфигурации. Как только сервер обнаружен, создается канал связи через виртуальные сетевые адаптеры. В последней строке окна ко-

мандной строки появляется запись "Initialization Sequence Completed" ("Инициализация завершена") — рис. 5.8.

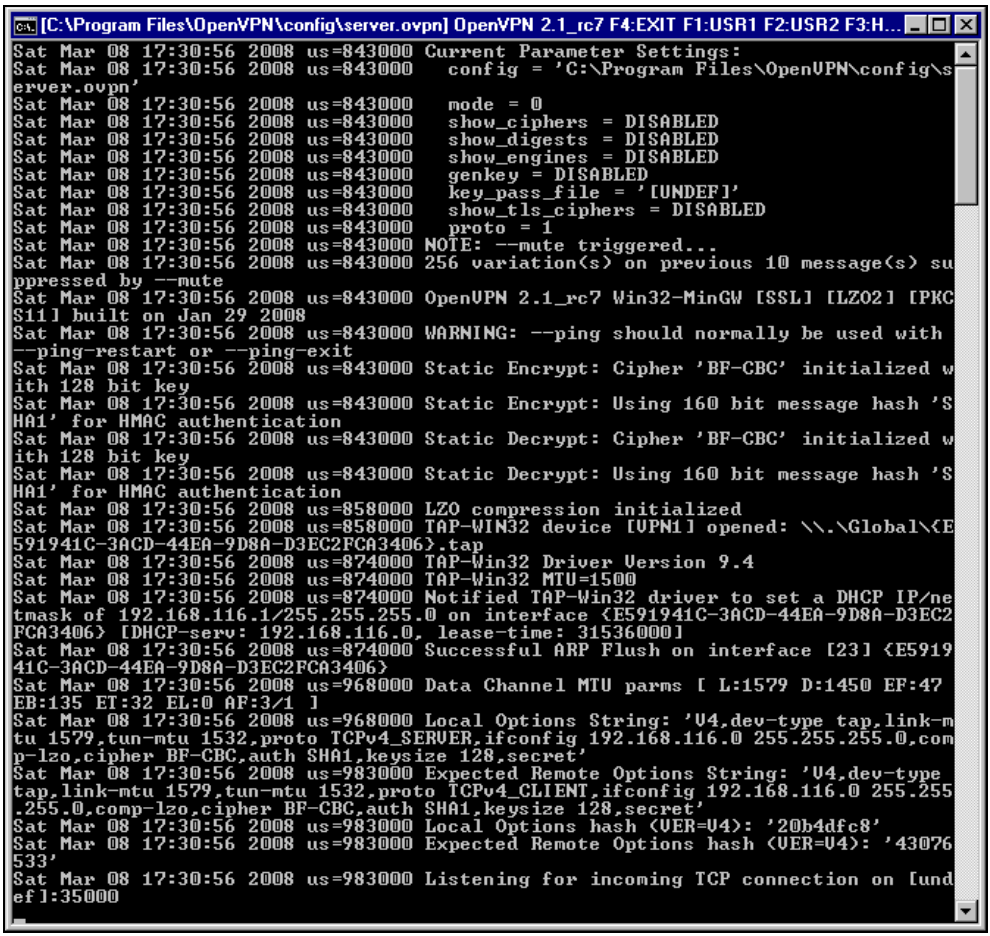


Рис. 5.6. Окно командной строки для Server OpenVPN

Для обеспечения защищенности этого канала применяется шифрование. Для того чтобы сервер мог определить "своего" при подключении, применяется файл ключа (key.txt), который должен быть сформирован средствами самой программы на одном из компьютеров и передан на другой любым доступным способом. Кроме того, связь осуществляется через выбранный вами порт, номер которого указывается в файлах конфигурации (параметр `port`).

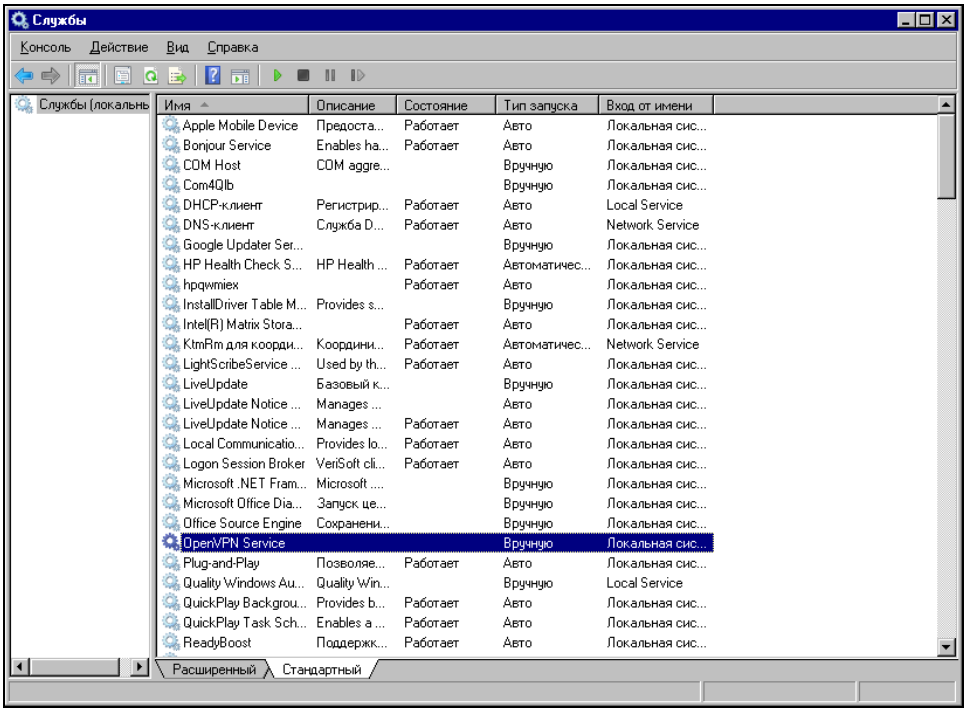


Рис. 5.7. Окно **Службы**

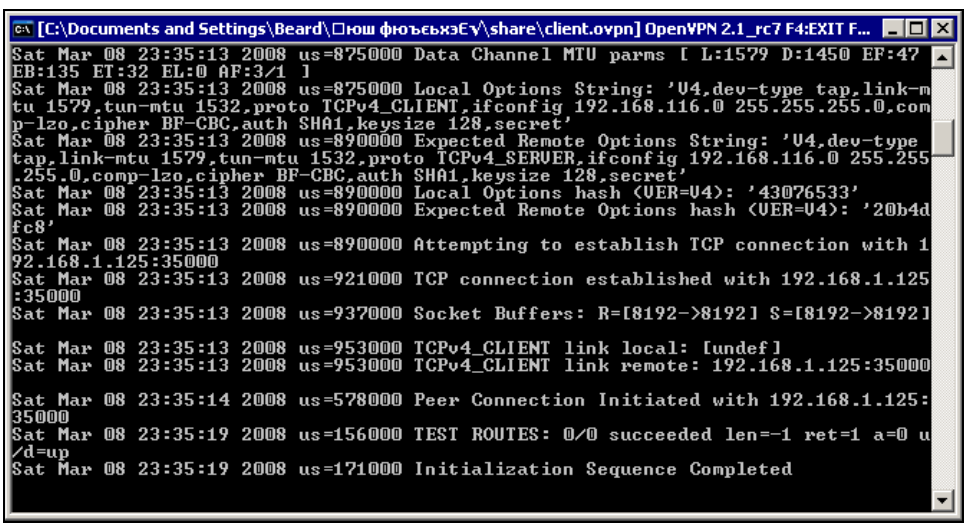


Рис. 5.8. Окно командной строки для Client OpenVPN

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.

Сообщение клиентской программы `mute triggered` обозначает, что попытки связи неудачны и программа ожидает изменений в настройках. Например, если был недоступен адрес сервера по его имени, а вы внесли верную запись в файл Hosts (не закрывая OpenVPN), программа возобновит попытки установления связи.

При установившейся связи в сетевом окружении удаленного компьютера появится сервер. Для входа на него потребуется ввести имя пользователя и пароль, допустимые в сети.

Для успешного соединения следует проконтролировать выполнение еще двух условий:

- локальный IP-адрес удаленной рабочей станции и сервера должен принадлежать подсети, которой не принадлежат адреса виртуальных адаптеров, созданных OpenVPN;
- имя рабочей группы, к которой принадлежит удаленная рабочая станция должно совпадать с именем домена или рабочей группы сервера.

Первое из этих условий обеспечивает однозначность поиска компьютера-сервера программой-клиентом. Невыполнение этого условия приведет к невозможности установления связи с удаленной сетью, а OpenVPN не сообщит вам никакой информации о причинах неудачи.

Второе условие обеспечивает появление компьютеров, находящихся в локальной сети, в сетевом окружении удаленной рабочей станции.

При достаточном качестве связи пользователь получит практически все те же возможности, что и при работе в локальной сети.

Поскольку в каждой сети, в том числе и в вашей, настройки доступа к ней могут иметь свои особенности, без экспериментов вам не обойтись, и для тонкой настройки придется обратиться к справке по OpenVPN и справочной системе Windows. Но применение OpenVPN позволит вам достаточно быстро провести настройки подключения, если они возможны в ваших условиях. Когда подключение установлено, скорость передачи информации по этому каналу будет ниже, чем при прямом соединении. Дополнительные преобразования информации, шифрование и дешифрование требуют и дополнительного времени. Но для обычной работы в сети скорость связи вполне достаточна, особенно, если рабочая станция подключена к Интернету через

быстрый канал связи. Автору удалось установить такое соединение через dial-up. При этом для работы с документом Word его требовалось скопировать на рабочую станцию, но печать на один из принтеров сети проходила нормально. Более того, этот принтер был подключен к рабочей станции во время соединения. Для ускорения процесса подключения желательно, чтобы драйвер принтера был уже установлен на удаленной рабочей станции.

Можно обеспечить несколько подключений к серверу, запустив на нем несколько экземпляров OpenVPN-сервера. Каждый из экземпляров должен быть связан со своим виртуальным сетевым подключением. Виртуальные подключения могут создаваться средствами OpenVPN в любом необходимом количестве. Это позволяет для каждого подключения применять свой ключевой файл, что повышает защищенность сети.

Описанный ранее пример подключения предназначен только для первого опыта его организации. В нем предполагается прямое соединение двух компьютеров перекрестным кабелем или через концентратор (хаб, коммутатор). Реальное соединение, которое будет описано далее, лучше организовывать после удачного завершения первого эксперимента по связи между двумя компьютерами. Для реальной связи через Интернет с локальной сетью потребуется более кропотливая работа. Приведем пример реально работающей пары компьютеров, связанных через VPN. Само собой разумеется, что на оба компьютера необходимо установить OpenVPN. Имя виртуальному сетевому адаптеру следует присвоить короткое, латинскими буквами. Можно использовать имя программы OpenVPN.

Теперь рассмотрим случай создания VPN-канала в другую удаленную сеть, которая, вполне возможно, существует у вас на работе. При необходимости администратор сети сможет выполнить описанные далее настройки для обеспечения вашего доступа в сеть или, при небольшой модификации настроек, к вашему компьютеру на работе.

В этом примере описаны настройки для двух компьютеров. Один из них — ноутбук, который работает и в локальной сети, и вне ее. Другой — вспомогательный сервер под управлением Windows Server 2003, через который локальная сеть имеет выход в Интернет. Подключение к Интернету осуществлено через ADSL-модем. При этом сеть имеет единственный внешний адрес 81.195.117.138. Внутренние адреса ЛВС принадлежат подсети 192.168.115.0. Постоянный адрес ноутбука в данном случае значения не имеет, поскольку при подключении к Интернету через обычный модем он получает динамически выделяемый адрес. Конкретное значение этого адреса тоже не имеет значения и в настройках соединения не применяется. В файлах конфигурации

OpenVPN виртуальным сетевым адаптерам присваиваются адреса 192.168.116.1 — для сервера и 192.168.116.2 — для ноутбука (удаленной рабочей станции). На рис. 5.9 схематично показана организация подключения к локальной сети через Интернет с использованием виртуальной частной сети.

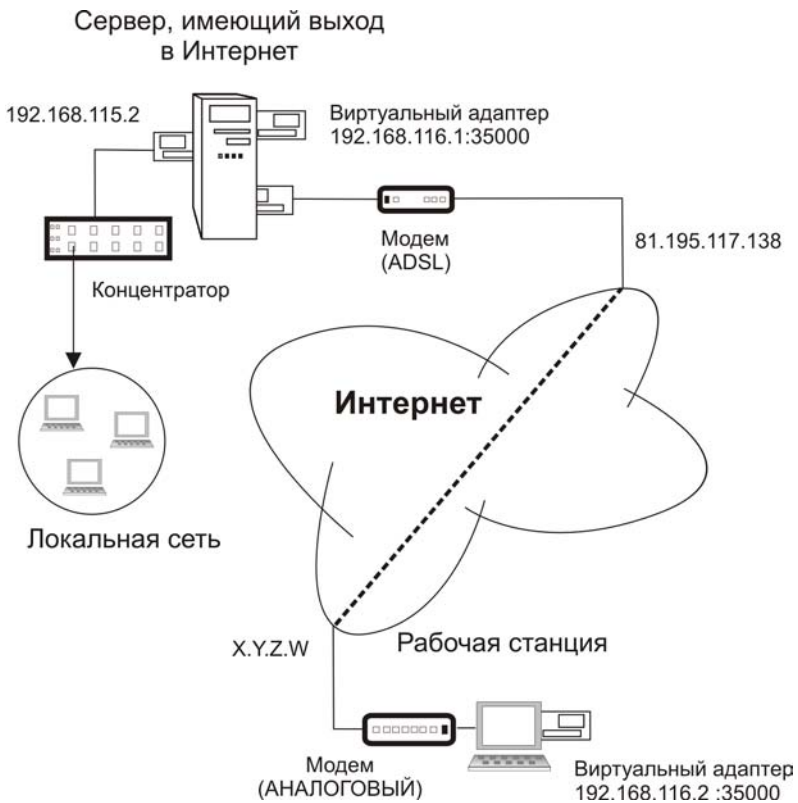


Рис. 5.9. Схема подключения к ЛВС через Интернет с применением VPN

Прежде всего, необходимо обеспечить возможность ответа сервера на команду `ping`. Иногда администраторы намеренно запрещают эту возможность, пытаясь максимально обезопасить сеть от проникновения в нее извне. Но в нашем случае именно такое проникновение и готовится. При этом защищенность сети не ухудшается, если не считать возможности простого обнаружения вашего компьютера (сервера) из Интернета. Ответ компьютера на команду `ping`

запрещается, если включен брандмауэр и выключен параметр протокола ICMP (Internet Control Message Protocol) **Запрос входящего эха** (рис. 5.10).

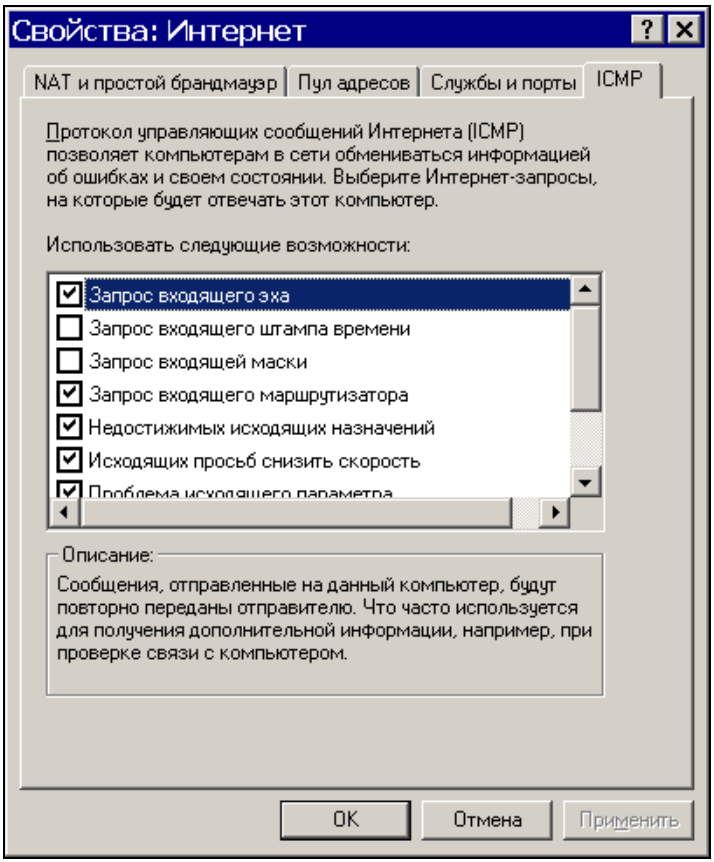


Рис. 5.10. Свойства интерфейса "Интернет". Настройка ICMP **Запрос входящего эха**

Компьютер с несколькими сетевыми подключениями (соответственно и несколько сетевых адаптеров) может иметь различные настройки брандмауэра для каждого из них. Тем более это относится к компьютеру, на котором настроено преобразование сетевых адресов (NAT). Поэтому, настраивая параметры сетевых подключений, будьте внимательны. Случайная ошибка при установке параметров подключений к катастрофе не приведет, но заставит помучиться в поисках причин неудачи.

Когда вы убедились, что `ping` до сервера проходит нормально, а время ответа не превышает 300 мс, а разброс значений этого времени невелик (не более 50%), то можно продолжать настройки. Если время ответа больше, работа с удаленной рабочей станции с ресурсами локальной сети будет очень медленной. Но иногда достаточно даже медленной связи для выполнения необходимых процедур администрирования. Связь будет очень неустойчивой, если ответы на `ping` будут нерегулярными. Если среди строчек ответов на экране появляется "Превышено время ожидания", то следует искать причины нарушения качества связи или выбрать другое время для подключения.

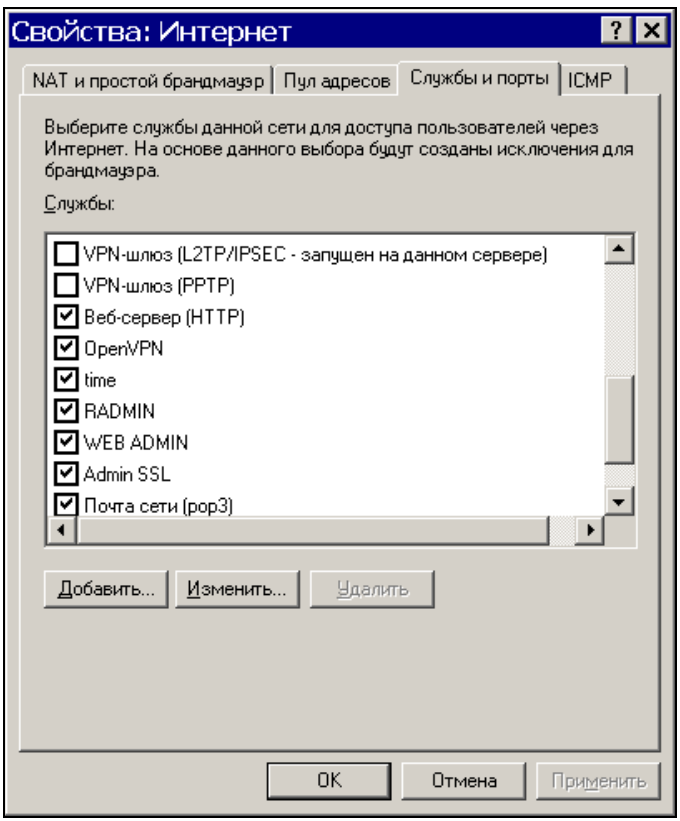


Рис. 5.11. Маршрутизация и удаленный доступ. Свойства интерфейса

Защищенный канал связи, создаваемый в Интернете, работает через порт, который мы зададим в файлах конфигурации OpenVPN. Это значит, что на

всем протяжении этого канала (рабочая станция — сервер провайдера 1— интернет-сервер провайдера 2 — сервер локальной сети) этот порт должен быть открыт. В примере показано применение порта 35000, но можно выбрать любое значение, не используемое на вашем сервере. Если есть сомнения в том, что выбранный вами порт открыт на каком-либо участке предполагаемого канала, его можно изменить. Если на сервере ЛВС не применяется какой-нибудь из известных сервисов, например, POP3, то можно использовать стандартный для этого сервиса порт 110. Скорее всего, он будет открыт на всем протяжении канала VPN. Для того чтобы открыть этот порт на вашем сервере, следует настроить свойства интерфейса, подключенного к Интернету в оснастке **Маршрутизация и удаленный доступ**.

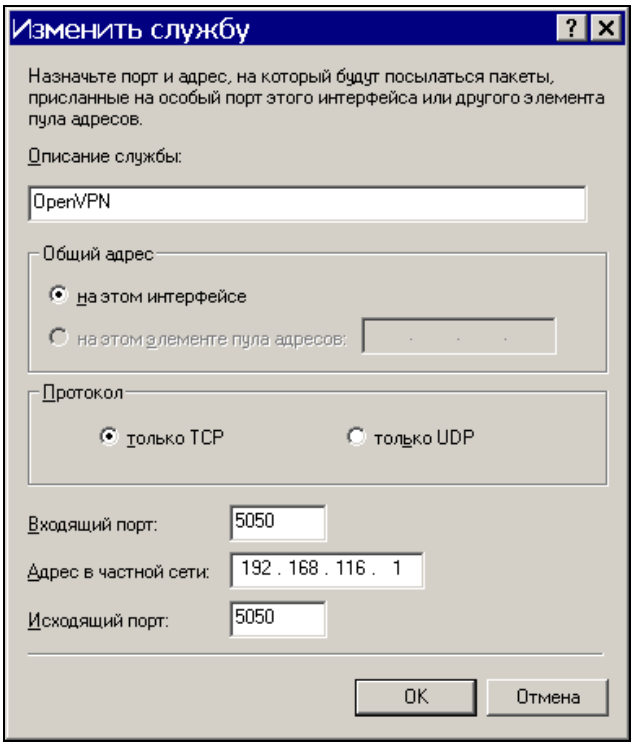


Рис. 5.12. Маршрутизация и удаленный доступ. Свойства интерфейса: изменение службы

На рис. 5.11 показано окно свойств интерфейса с перечнем служб, доступных из Интернета. На рис. 5.12 показано окно изменения свойств службы с указа-

нием номеров входящего и исходящего портов. Можно задать эти значения разными. В этом случае соответствующие значения должны быть указаны в файлах конфигурации на удаленной рабочей станции (значение для входящего порта) и на сервере (значение для исходящего порта).

Открыв используемый порт, необходимо настроить маршрутизацию IP-пакетов, передаваемых через Интернет. Это также делается в оснастке **Маршрутизация и удаленный доступ** (рис. 5.13), где необходимо указать статические маршруты. Один маршрут уже был указан, когда настраивался доступ к Интернету для пользователей сети. Теперь следует добавить еще два (один для основного, другой для виртуального сетевого адаптера).

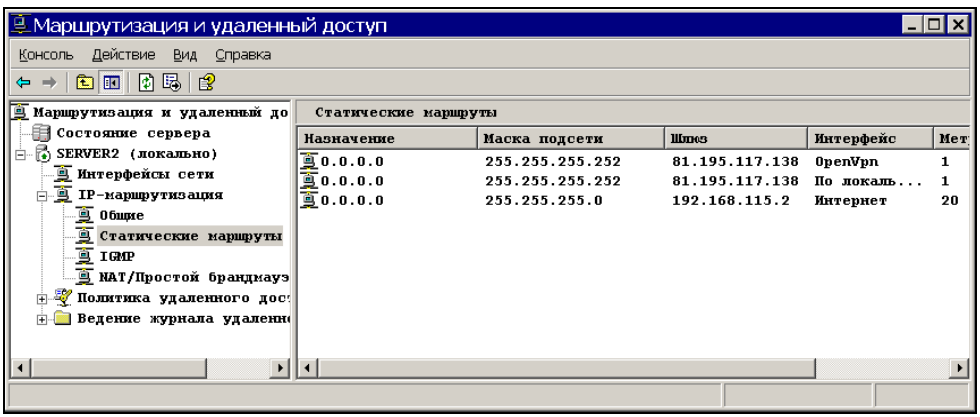


Рис. 5.13. Маршрутизация и удаленный доступ. Статические маршруты

В дальнейшем может потребоваться подключение других пользователей через VPN. Для этого нужно создать несколько виртуальных адаптеров по числу создаваемых каналов и присвоить им имена с различными суффиксами. При этом для каждого канала следует запускать свой экземпляр OpenVPN-сервера, а в файле конфигурации каждого экземпляра указать соответствующее имя адаптера. При этом выбранный вариант маршрутов изменять не потребуется.

Создадим файлы конфигурации (см. листинги 5.3 и 5.4).

Эти файлы могут быть такими же, как и при проведении экспериментов с локальными машинами. Важно указать правильные значения IP-адресов и портов.

Создадим файл секретного ключа с помощью пункта меню программы **Generate a static OpenVPN key** (Создать статический ключ) и поместим одну копию на OpenVPN-сервере, другую — на OpenVPN-клиенте в папку с файлами конфигурации программы. Можно использовать и те файлы, что применялись на локальных машинах. Важно, чтобы на обеих машинах были копии одного и того же файла.

На рабочей станции обычно специальных настроек не требуется. Должна быть установлена программа OpenVPN, а в папку с конфигурационными файлами программы помещены файл конфигурации клиента и секретный ключ.

Теперь можно запустить OpenVPN-сервер и попытаться установить подключение с рабочей станции, с доступом к Интернету. Хорошо, если для проведения пробного подключения есть второй телефон. К сожалению, подключение dial-up по той же линии, к которой подключен ADSL-модем, не всегда бывает достаточно хорошего качества, но, может быть, вам повезет, и вы сможете для эксперимента использовать одну телефонную линию.

На рабочей станции устанавливаем соединение с Интернетом через обычный модем и запускаем OpenVPN с использованием локального (клиентского) файла конфигурации. Программа делает несколько попыток соединения, и, если все настроено верно, соединение устанавливается. Вы можете определить момент установки соединения по сообщению "Initialization Sequence Completed". В противном случае проверяем настройки и качество соединения.

После установления VPN-соединения откройте сетевое окружение на рабочей станции. Вы должны увидеть компьютер, к которому производилось подключение. Попытка открыть этот компьютер и получить доступ к ресурсам может оказаться неудачной, если для доступа к компьютеру требуется сертификат, а на рабочей станции его нет. Установите для входящего подключения на сервере проверку подлинности по имени пользователя и паролю. Это можно сделать на вкладке **Проверка подлинности** в окне свойств подключения. При работе в локальной сети может быт включена проверка подлинности по смарт-карте или сертификату, но при доступности сведений о компьютере проверяется подлинность самого компьютера. В нашем случае связь оказывается односторонней. Удаленная рабочая станция не имеет постоянного IP-адреса, OpenVPN установила связь и идентифицировала клиента по своему секретному ключу, а сервер теперь хочет проверить подлинность пользователя или компьютера при попытке доступа к его ресурсам.

В этом случае можно установить проверку подлинности по имени пользователя и паролю (MD5-Challenge).

Можно, конечно, установить и настроить центр сертификации на сервере Windows Server 2003. Но это тема отдельного разговора.

Подключение к рабочим станциям сети

Если вам удалось подключиться к серверу сети или к компьютеру, имеющему непосредственное подключение к Интернету, то можно начинать настройку доступа к любой рабочей станции сети (рис. 5.14). Эта возможность позволяет любому пользователю (если вы настроили для него доступ) подключиться из дома к своему рабочему компьютеру. В нашей сети второй сервер, имея непосредственное подключение к Интернету, обладает реальным IP-адресом в Интернете. Другие компьютеры сети имеют только внутренние адреса. Тем не менее, есть возможность обеспечить доступ к этим компьютерам через VPN. Это возможно, потому что обращение к компьютерам происходит не только по IP-адресу, но и с использованием определенного порта. Если на стороне OpenVPN-клиента в файле конфигурации указать порт, отличающийся от того, который был применен для связи с сервером, а на сервере, подключенном к Интернету, создать маршрут к рабочей станции в локальной сети, на которой имеется этот же номер порта, то связь OpenVPN-клиента осуществится именно с этой рабочей станцией. То есть, используя перенаправление портов, можно, меняя номер порта на клиенте, подключаться к различным серверам OpenVPN, находящимся в локальной сети. Если для подключения к Интернету вашей сети используется маршрутизатор, то существует возможность подключения к любому компьютеру вашей сети по выбору. Если применяется брандмауэр, то необходимо разрешить связь из Интернета по этому номеру порта.

Настройте доступ по выбранному порту к рабочей станции, создав еще одну службу, подобно тому, как показано на рис. 5.11, адресовав ее на соответствующий рабочей станции IP-адрес и указав выбранный для работы порт. Следует указать так же статические маршруты (рис. 5.12) к рабочим станциям. Указывать их надо для интерфейса, подключенного к Интернету. Шлюз — адаптер, смотрящий в локальную сеть, назначение — IP-адрес рабочей станции в сети, маска подсети — 255.255.255.255.

Можно заранее настроить возможность доступа к нескольким рабочим станциям, выбрав для них различные номера портов.

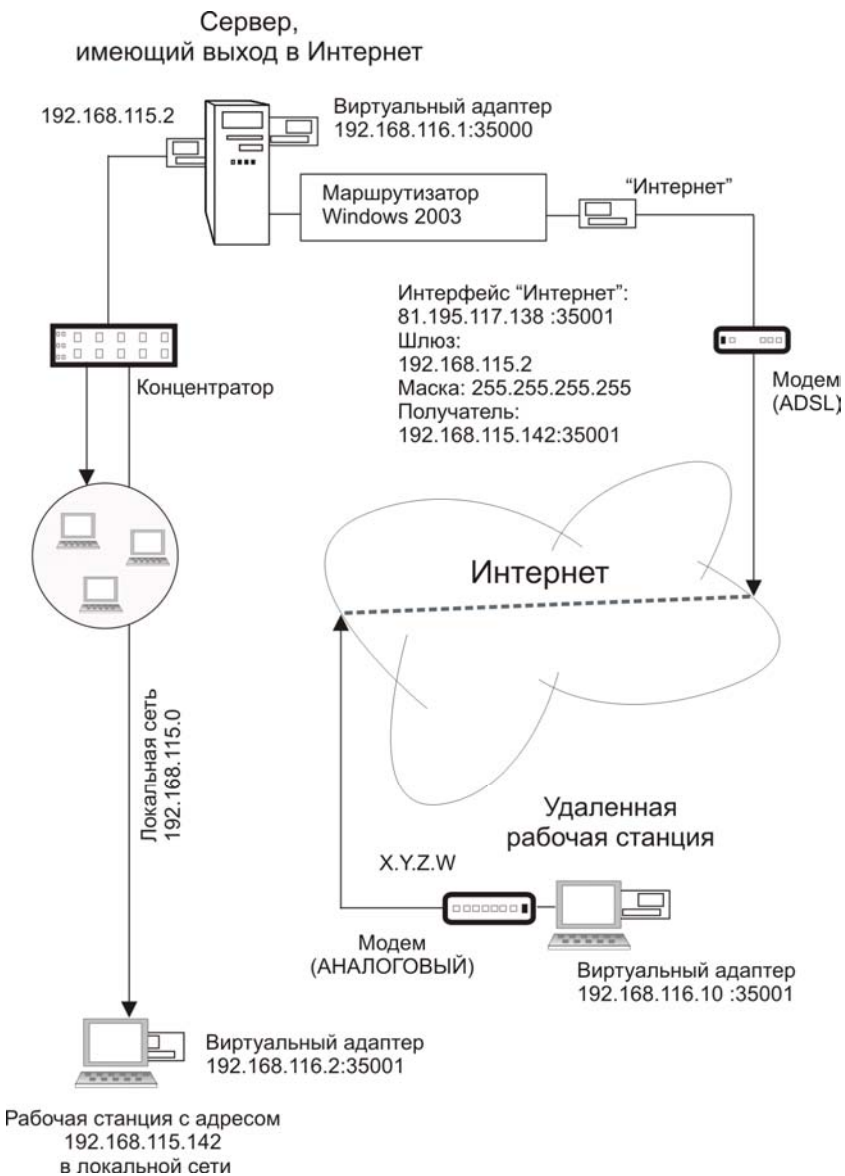


Рис. 5.14. Схема подключения к рабочей станции

Если при организации удаленного доступа пользователя к своей рабочей станции подготовить отдельный ключевой файл, то кроме этого пользователя никто не сможет подключиться к его рабочей станции. Аналогично, этот пользователь не сможет подключиться к другим рабочим станциям и серверам.

При подготовке нескольких подключений следует дать понятные имена ключевым файлам, самим подключениям и файлам конфигурации для исключения путаницы.

Если ваш компьютер (рабочая станция) поддерживает работу с несколькими сетевыми адаптерами, то можно одновременно подключиться к рабочей станции в локальной сети и к серверу. Несмотря на то, что в файлах конфигурации клиентов будет указано одно и то же имя удаленного компьютера, соответствующее IP-адресу сервера, подключение будет происходить к соответствующим рабочим станциям. При этом в сетевом окружении они будут появляться под своими именами. То есть ваша работа на удаленной рабочей станции почти не будет отличаться от работы в локальной сети. Работу с несколькими виртуальными сетевыми адаптерами необходимо обязательно проверить в условиях, когда с одним адаптером все работает устойчиво. Если вместо сообщения "Initialization Sequence Completed" на экране будет появляться "Initialization Sequence Completed with Errors", когда установлено более одного виртуального адаптера, — работа с сетевыми ресурсами может быть затруднена или невозможна.

В файлах конфигурации могут быть предусмотрены параметры, позволяющие улучшить надежность VPN-соединения и уменьшить время его восстановления при сбоях. Подробное описание всех возможных параметров приведено на сайте разработчиков OpenVPN, а здесь приведем еще раз содержимое файлов конфигурации сервера и клиента с некоторыми изменениями (листинги 5.3 и 5.4).

Листинг 5.3. Файл конфигурации Local.ovpn для клиента OpenVPN

```
remote server # необходимо в файле Hosts указать IP-адрес
proto tcp-client
dev tap2
ifconfig 192.168.116.12 255.255.255.0
mssfix
dev-node den
secret den.txt
ping-restart 60
ping-timer-rem
persist-key
resolv-retry 86400
```

```
ping 10
comp-lzo
verb 4
mute 10
```

Листинг 5.4. Файл конфигурации Server.ovpn для сервера OpenVPN

```
port 35001
proto tcp-server
dev tap
ifconfig 192.168.116.142 255.255.255.0
dev-node <Имя подключения>
secret den.txt
ping 10
comp-lzo
verb 4
mute 10
```

В обоих файлах (один клиентский, другой серверный) один и тот же файл ключа (копия). При этом имя ключевого файла можно изменять.

Настройка сервера OpenVPN в Linux

Рассматривая установку OpenVPN для Linux, используем средства, которые допустимы в любых версиях Linux, основанных на кодах Red Hat. Это и Mandriva Linux, и ASPLinux, а также множество других распространенных дистрибутивов. В процессе установки проблем будет меньше, если система изначально установлена в варианте для сервера. В других вариантах установки могут требоваться дополнительные пакеты. Часть проблем, возникающих во время установки, рассмотрена в этом описании. Мы начнем установку OpenVPN с получения архива с исходными кодами программы. Убедитесь, что у вас работает подключение к Интернету. Практически все операции мы будем выполнять в окне терминала, поэтому перед началом установки откройте окно терминала.

Чтобы получить права на выполнение операций с файлами и установку программ, введите команду `su` и после запроса системой введите пароль администратора компьютера.

Можно начинать установку.

Переходим в каталог, где будет храниться архив с исходным кодом программы. Для этого вводим команду:

```
cd /usr/local/sr
```

Вводим команду для получения файла с сервера OpenVPN:

```
Wget http://openvpn.net/release/openvpn-2.0.9.tar.gz
```

> ***Примечание***
>
> На момент написания этих строк последняя версия программы была openvpn-2.0.9. Проверьте на странице **http://openvpn.net/index.php/downloads.html** наличие более новых файлов и измените в командах номер версии на текущий.

Распаковываем полученный архив командой

```
tar zxvf openvpn-2.0.9.tar.gz
```

Запускаем инсталляцию:

```
cd openvpn-2.0.9
./configure
```

Вполне возможно, что в процессе инсталляции в окне терминала вы увидите следующее сообщение:

```
LZO library available from http://www.oberhumer.com/opensource/lzo/
configure: error: Or try ./configure –disable-lzo
```

Это значит, что в системе нет библиотеки lzo, с помощью которой происходит сжатие трафика в режиме реального времени.

Получаем необходимые файлы и устанавливаем их:

```
wget http://www.oberhumer.com/opensource/lzo/download/lzo-2.02.tar.gz
tar zxvf lzo-2.02.tar.gz
cd lzo-2.02
./configure
Make
make install
```

Возвращаемся в каталог openvpn-2.0.9 и продолжаем установку:

```
cd ../openvpn-2.0.9
./configure
Make
make install
```

На этом этап инсталляции пакета закончен.

Начинаем процедуру настройки программы.

Генерируем master CA сертификат/ключ (корневой сертификат и ключ)

```
cd easy-rsa
../vars
./clean-all
./build-ca
```

При генерации соглашаемся со всеми предложениями системы нажатием клавиши <Enter>. Только в строке, где необходимо указать имя сертификата, вводим это имя:

```
Common Name (eg, your name or your server's hostname) []: OpenVPN-CA
```

OpenVPN-CA — *имя CA-сертификата*.

Генерируем сертификат и ключ для сервера:

```
./build-key-server server
```

Также соглашаемся со всеми предложениями системы нажатием клавиши <Enter>. Только в строке, где необходимо указать имя сертификата, вводим это имя:

```
Common Name (eg, your name or your server's hostname) []: server
```

Далее на вопросы системы, где есть выбор `y/n`, отвечаем `y`.

Генерируем ключи клиентов (в этом примере два):

```
./build-key client1
./build-key client2
```

Также как и в предыдущем случае в строке, где требуется ввести имя ключа, указываем его:

```
Common Name (eg, your name or your server's hostname) []: client1
```

Генерируем параметры алгоритма шифрования Diffie Hellman командой

```
./build-dh
```

Теперь создадим каталог /etc/openvpn и перепишем в него сгенерированные ключи и конфигурационный файл сервера, который был установлен вместе с программой:

```
mkdir /etc/openvpn
cp ../sample-config-files/server.conf /etc/openvpn/
```

Редактируем конфигурационный файл сервера:

```
vi /etc/openvpn/server.conf
```

Строку

```
;push "redirect-gateway"
```

меняем на

```
push "redirect-gateway def1"
```

Строку

```
;push "dhcp-option DNS 10.8.0.1"
```

меняем на

```
push "dhcp-option DNS 10.8.0.1"
```

IP-адреса указываем для своей сети. Строку

```
;max-clients 100
```

меняем на

```
max-clients 10
```

Удаляем символы комментария в строках

```
;user nobody
;group nobody
```

Переписываем скрипт старта сервера и добавляем его в автоматический старт при загрузке:

```
cp /usr/local/src/openvpn-2.0.9/sample-scripts/openvpn.init
/etc/rc.d/init.d/openvpn
chkconfig --add openvpn
```

Запускаем OpenVPN:

```
service openvpn start
```

Редактируем файл конфигурации сервера:

```
vi /etc/sysctl.conf
```

Находим строку

```
net.ipv4.ip_forward = 0
```

и меняем ее на

```
net.ipv4.ip_forward = 1
```

Это необходимо, чтобы включилась маршрутизация пакетов между сетевыми адаптерами.

Клиентскую часть OpenVPN можно настроить в Windows. Нам понадобятся файлы сертификатов, созданные на сервере:

```
ca.crt
client1.crt
client1.key
```

На нашем сервере они лежат в папке /etc/openvpn. Копируем их оттуда любым способом на свою клиентскую машину. Далее создаем для примера на нашем диске C: папку vpn и копируем туда наши ключи.

Файл конфигурации клиента OpenVPN для данного случая будет выглядеть подобно приведенному в листинге 5.5.

Листинг 5.5. Файл конфигурации Local.ovpn для клиента OpenVPN при подключении к серверу под Linux

```
remote server # необходимо в файле Hosts указать IP-адрес
proto tcp-client
dev tap2
ifconfig 192.168.116.12 255.255.255.0 # заменить на IP-адрес в вашей сети
mssfix
dev-node den
secret den.txt
ca c:\\vpn\\ca.crt
cert c:\\vpn\\client1.crt
key c:\\vpn\\client1.key
persist-key
ping 10
comp-lzo
verb 4
mute 10
```

Настройка программ для работы в Linux требует внимания и настойчивости. Возможно, что трудности, которые вы встретите во время работы с Linux, покажутся вам непреодолимыми. Но терпение и настойчивость принесут свои плоды. В Mandriva Linux есть графический интерфейс для настройки OpenVPN-соединений. Но с его помощью без понимания работы программы настройка не проще, чем путем редактирования файлов конфигурации. К сожалению, литературы о OpenVPN на русском языке практически нет. Можно рекомендовать статьи в Интернете по следующим ссылкам:

- **http://www.securitylab.ru/analytics/240979.php**;
- **http://dedicatesupport.com/archives/8**;
- **http://www.cyberinfo.ru/3/2362_1.htm**;
- **http://torgsat.ru/nastroika_ss/open_vpn_ss/**;
- **http://www.opennet.ru/base/net/openvpn_x509.txt.html**;
- **http://wiki.kryukov.biz/wiki/Openvpn**.

В поисковиках можно найти ссылки на обсуждение настройки OpenVPN для различных систем.

На английском языке можно почитать инструкции по настройке OpenVPN на сайте разработчиков: **http://openvpn.net/index.php/documentation/howto.html**.

По адресу в Интернете **http://v3n.0x7.net/books/ENG/security/VPN.7.rar** можно загрузить семь книг о OpenVPN на английском языке.

Автор надеется, что в обозримом будущем ему удастся написать подробное руководство по настройке OpenVPN для использования в домашних сетях под управлением Windows и Linux.

Далее в этой главе рассмотрены средства, которые могут быть использованы для доступа к удаленному компьютеру как с применением, так и без применения OpenVPN.

Работаем на своем компьютере из любой точки мира

Вернемся к домашней сети, в которой находится ваш компьютер. Если для доступа к компьютеру на работе необходима помощь администратора сети,

если вы сами не являетесь ее администратором, то для обеспечения доступа к домашнему компьютеру из Интернета все действия вы можете выполнить самостоятельно. Вы можете настроить VPN-канал и/или использовать другие средства доступа к компьютеру. Для того чтобы обеспечить доступ к компьютеру из Интернета, необходимо обеспечить наличие внешнего IP-адреса и открыть необходимый порт для доступа извне. Протоколы TCP/IP позволяют единообразно настраивать доступ, независимо от применяемых средств. Всегда есть серверная и клиентская части программы. Клиентская часть должна иметь возможность найти в Интернете ваш компьютер, а серверная, которая установлена на вашем компьютере, должна иметь возможность принять запросы на определенных портах. Эти порты должны быть доступны клиентской части программы.

Некоторые провайдеры Интернета, предоставляя домашним пользователям доступ в Интернет, закрывают некоторые порты для доступа из Интернета. Это делается в целях обеспечения безопасности пользовательских компьютеров. Обычно именно по этим портам происходит большинство атак на компьютеры пользователей, которые не позаботились о безопасности своих машин. Закрыв отдельные порты, провайдеры исключают распространение многих вирусов в своих сетях. Конечно, для пользователей создаются определенные неудобства, такие, например, как невозможность создать на своем компьютере Web-сайт с использованием стандартных портов 80 и 8080. Но эти неудобства могут быть достаточно просто обойдены средствами, которые используем для обеспечения доступа к нашему компьютеру. Универсальность TCP/IP-протоколов позволяет обе задачи решить одними и теми же средствами. Совершенно не важно, какая операционная система установлена на вашем компьютере. В крайнем случае, если некоторые вспомогательные программы существуют только для Windows, а ваша основная ОС — Linux, вы можете установить их на виртуальную машину Windows, работающую на вашем компьютере.

DynDNS

Теперь рассмотрим сервис, предоставляемый сайтом **http://www.dyndns.com/** и позволяющий, получив символьный адрес в Интернете для вашего компьютера, направлять все запросы по этому имени на ваш компьютер. Даже если провайдер выдает вам динамический IP-адрес, вы всегда сможете найти его из Интернета. Запросы по закрытым провайдером портам могут быть перенаправлены на открытые, которые вы укажете. Вообще говоря, довольно много

компаний распространяют платные программы, которые, используя серверы этих компаний, могут обеспечить доступ к вашему компьютеру из Интернета. Мы рассмотрим вариант бесплатный.

Компания DynDNS в числе прочих предлагает услугу по связыванию внешнего IP-адреса вашего компьютера с символьным именем, которое зарегистрировано на сайте **http://www.dyndns.com/**. Если вы имеете зарегистрированное в Интернете имя, то можете использовать его, но можно и на сайте получить бесплатное доменное имя вида example.homeip.net, где имя третьего уровня example придумываете сами, а имен второго уровня вам предлагается на данный момент 89.

Для использования сервисов DynDNS необходимо зарегистрироваться на сайте. Бесплатно можно создать три доменных имени для сервиса Dynamic DNS. Имена можно связать с существующими статическими IP-адресами или скачав специальную программу-клиент с текущим динамическим IP-адресом. Если провайдер закрыл какой-либо порт, можно настроить серверную часть программы на работу с нестандартным портом, а при вводе адреса в клиентской части программы указать работающий порт через двоеточие после адреса.

Таким образом, сервисы DynDNS позволяют заставить DNS-серверы в Интернете разрешать символьные адреса ваших компьютеров в динамически присваиваемые IP-адреса.

Настраивая OpenVPN для работы с домашним компьютером, укажите в клиентской части программы вместо IP-адреса доменное имя, зарегистрированное на DynDNS, а клиентскую программу этого сервиса DynDNS Updater настройте на связь этого имени с текущим IP-адресом. Получить DynDNS Updater можно на странице **https://www.dyndns.com/support/**.

Теперь мы можем настроить доступ к компьютеру из Интернета, используя любые программы, которые предназначены для работы в локальной сети.

Терминальный доступ

Один из популярных способов удаленной работы на компьютере — терминальный доступ. К сожалению, не все операционные системы позволяют управлять ими таким способом. Из распространенных на сегодняшний день у пользователей ОС это Windows Vista Ultimate, Windows XP Professional, Windows 2000 Server, Windows Server 2003. Но доступ к ним возможен из

любых других систем, включая Linux. Используя сервисы DynDNS, можно применить программу Удаленный доступ к рабочему столу для доступа к своему компьютеру через Интернет.

Эту программу можно использовать и при работе через VPN. Если установлен канал виртуальной сети до удаленного компьютера, то Удаленный доступ к рабочему столу будет работать, как и в локальной сети, но через виртуальные сетевые адаптеры.

Как и при настройке OpenVPN, есть смысл "обкатать" подключение к удаленному рабочему столу на рядом стоящих компьютерах.

Пример

В данном примере виртуальная сеть настроена между компьютерами Beard-NB под управлением Windows Vista Home Premium и Beard-XP под управлением Windows XP Professional.

Запускаем программу Удаленный доступ к рабочему столу на компьютере Beard-NB (**Программы | Стандартные | Подключение к удаленному рабочему столу**) (рис. 5.15).

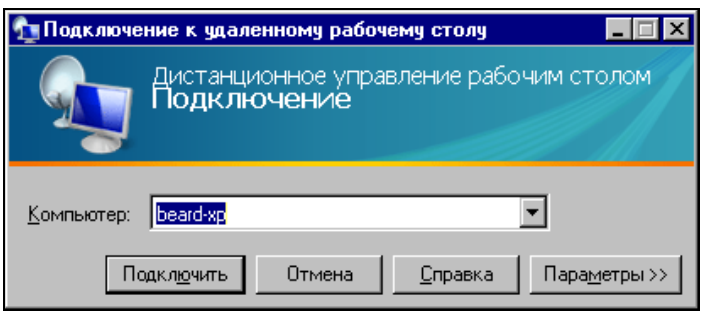


Рис. 5.15. Окно **Подключение к удаленному рабочему столу**: подключение

Нажав кнопку **Подключить**, мы вызовем окно **Безопасность Windows**, где необходимо ввести учетные данные пользователя удаленного компьютера, который имеет разрешение удаленного доступа (рис. 5.16).

Если данные введены верно, нажимаем кнопку **OK**. Откроется окно **beard-xp - Удаленный рабочий стол** (рис. 5.17).

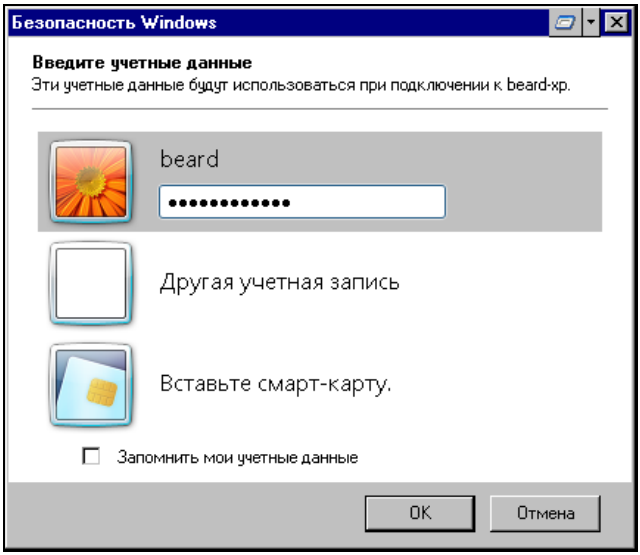


Рис. 5.16. Окно **Безопасность Windows**

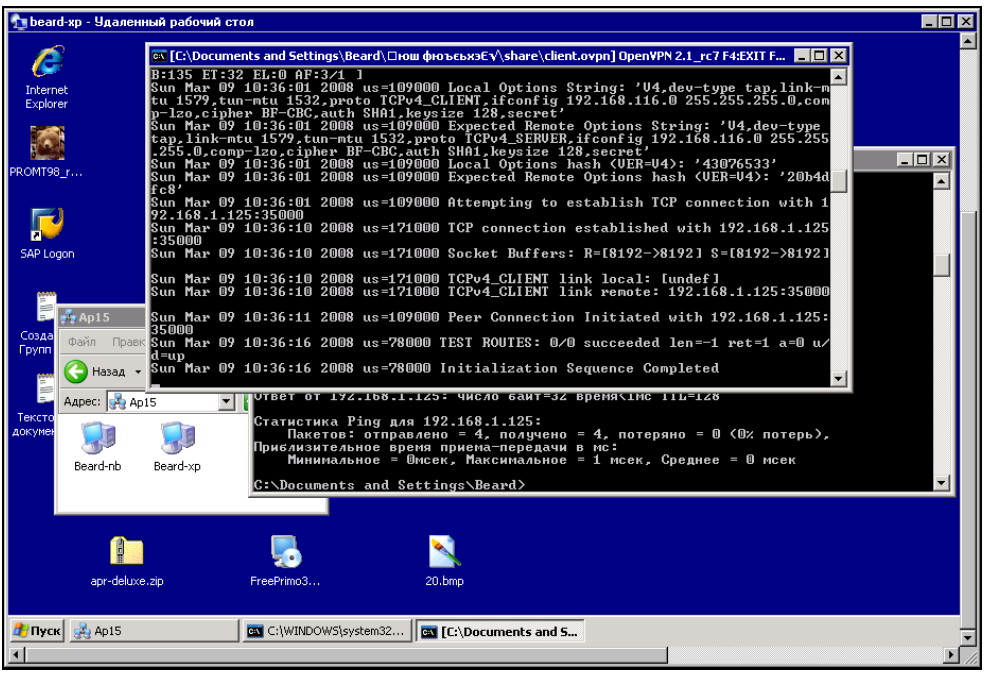


Рис. 5.17. Окно **beard-xp - Удаленный рабочий стол**

Попробуйте подключиться к рабочему столу, введя вместо имени IP-адрес виртуального адаптера. Если все работает, можно попробовать подключиться из Интернета.

Предупреждение

Вам не удастся подключиться через Интернет к компьютеру, находящемуся в вашей сети. Подключение возможно только из другой сети или отдельного компьютера, использующего другое подключение к Интернету.

На рис. 5.18 показано окно **okobox.homeip.net: 23333 - Удаленный рабочий стол**. Это рабочий стол компьютера, к которому выполнено подключение через Интернет с использованием сервиса DynDNS без организации VPN.

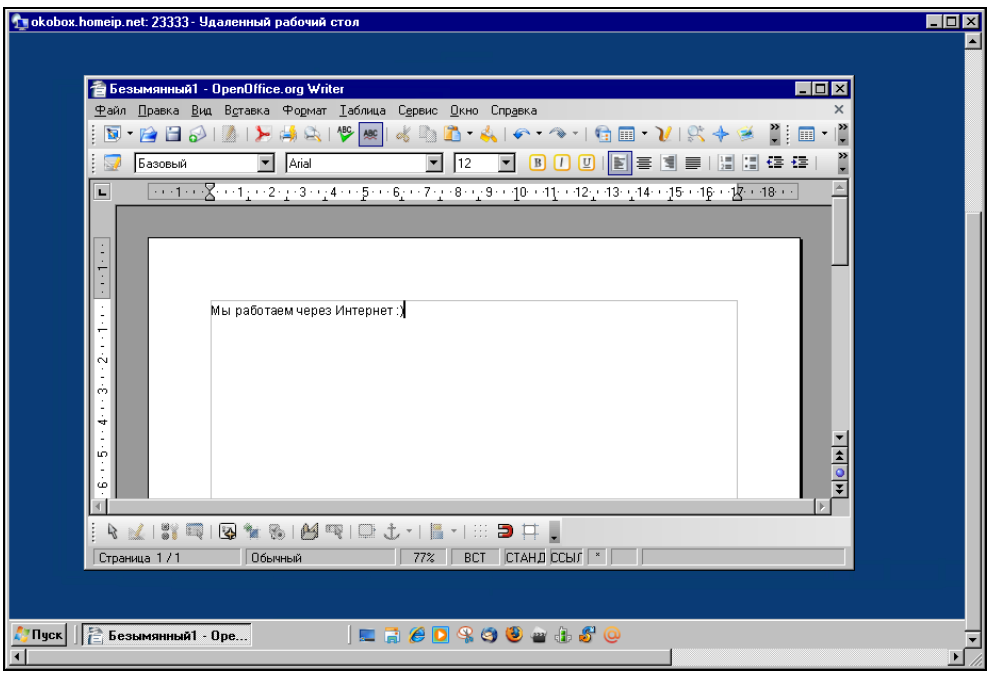


Рис. 5.18. Окно **okobox.homeip.net: 23333 - Удаленный рабочий стол**

На удаленном компьютере в целях безопасности изменен порт, на котором работает программа. При работе через OpenVPN в этом необходимости нет.

Подключение к удаленному рабочему столу Windows из Linux

В Linux есть встроенные средства для подключения к удаленному рабочему столу Windows. В различных версиях Linux интерфейсы управления такими подключениями отличаются, но в целом они похожи. Поэтому рассмотрим работу в Mandriva Linux, а в случае использования другой версии вы сможете самостоятельно найти аналогичные средства.

Итак, откройте **Центр управления Mandriva Linux | Онлайновое администрирование | Удаленное управление** (рис. 5.19).

В открывшемся окне **Центр управления Mandriva Linux** на странице удаленного управления (рис. 5.20) установите переключатель **Тип удаленного доступа** в значение **Терминальные службы Windows**.

В поле **Имя хоста Windows** введите IP-адрес удаленного компьютера или его имя. Остальные поля можно пока не изменять.

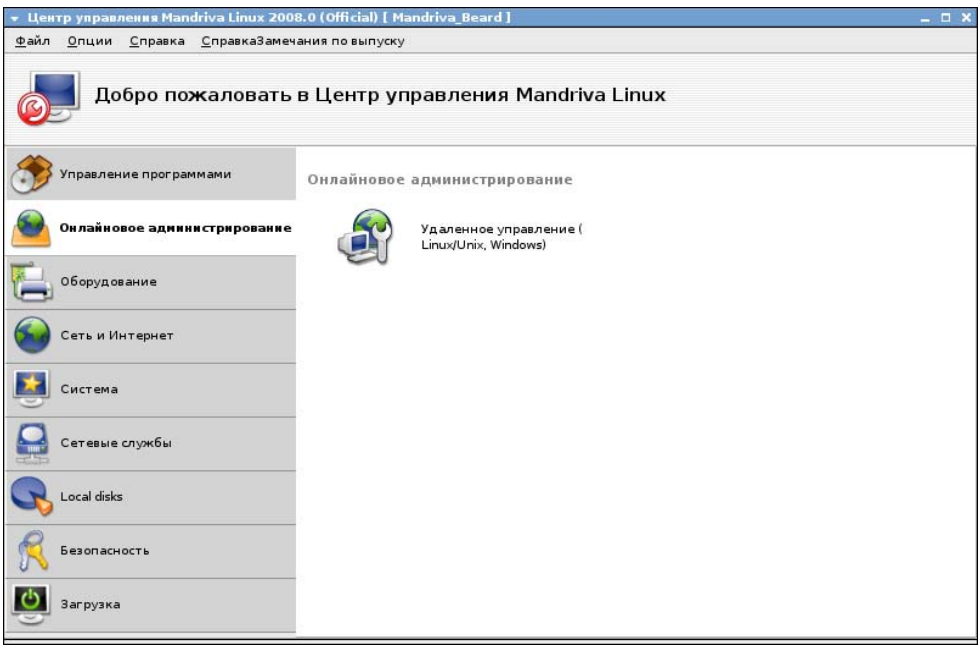


Рис. 5.19. Окно **Центр управления Mandriva Linux**, раздел **Онлайновое администрирование**

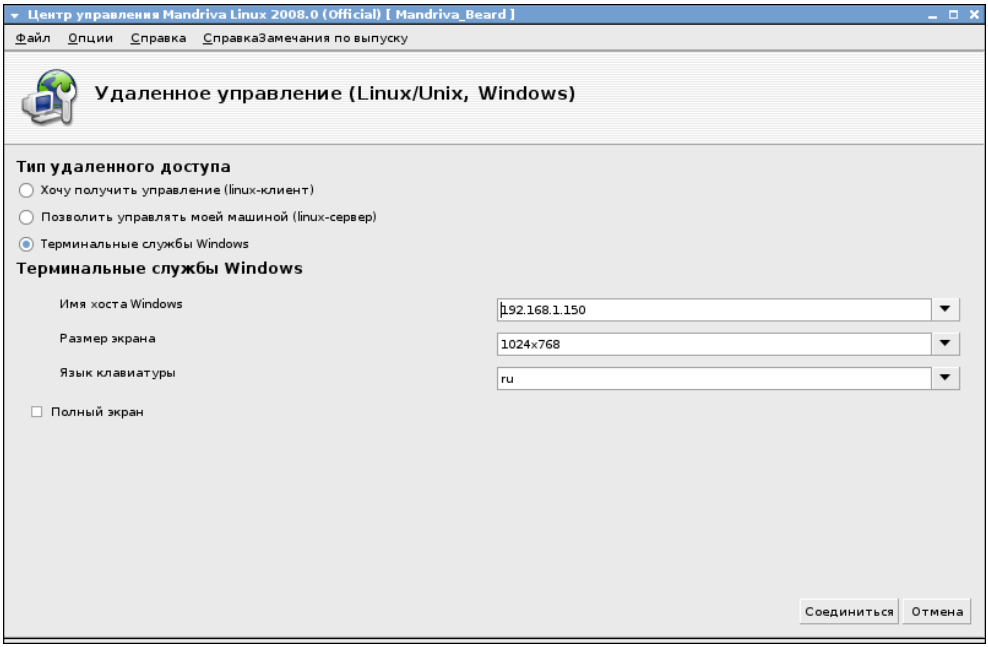


Рис. 5.20. Окно **Центр управления Mandriva Linux 2008.0**, страница **Удаленное управление (Linux/Unix, Windows)**

Нажмите кнопку **Соединиться**. Через несколько мгновений откроется окно **rdesktop <Имя_компьютера>** с окном **Вход в Windows** (рис. 5.21).

Все дальнейшие действия понятны — можно работать в Windows, подключившись из Linux.

Терминальный доступ широко используется администраторами сетей для удаленного управления серверами. В территориально распределенных организациях терминальный доступ позволяет сотрудникам удаленных офисов работать на компьютере, который находится в центре. Это удешевляет обслуживание компьютерной сети, делает более надежным хранение данных. Но и для домашнего компьютера и сети при наличии компьютера с операционной системой, поддерживающей терминальный доступ, тоже можно обнаружить немало выгод. Если на домашнем компьютере установлены дорогие программы, выполняются работы, требующие значительных ресурсов, то, используя простой легкий ноутбук, можно работать на домашнем компьютере, находясь вдали от дома. Вы всегда можете получить доступ к своей почте, органайзеру, привычным для вас программам и интерфейсам даже с чужого компьютера.

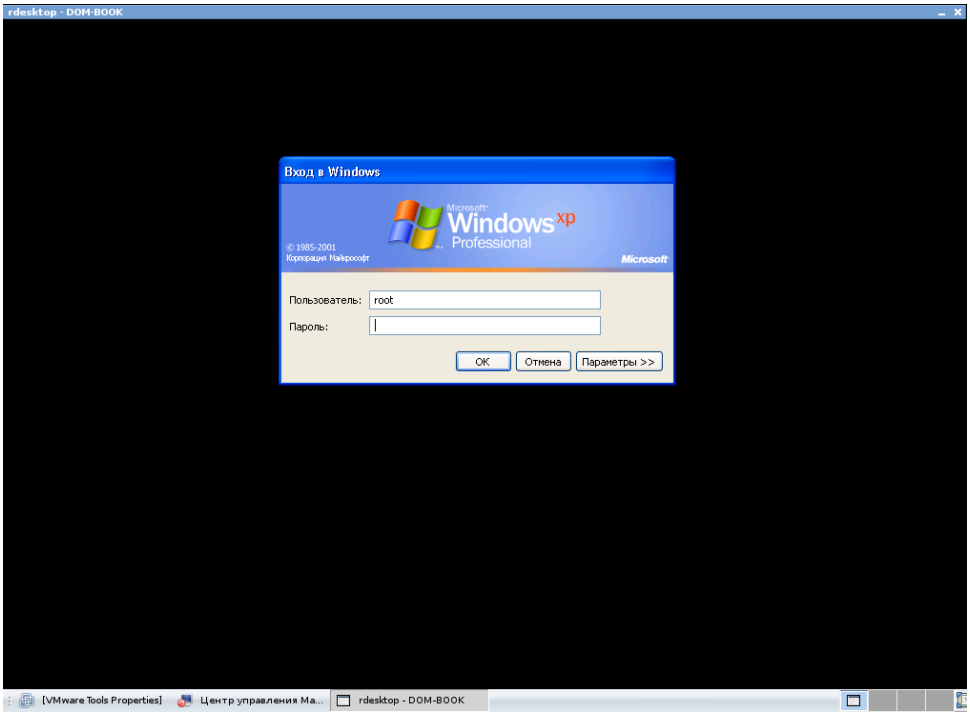


Рис. 5.21. Окно **rdesktop <Имя_компьютера>** с предложением войти в Windows

Но если на вашем компьютере домашняя версия Windows Vista или Linux, то Windows-терминал применить невозможно. В этих случаях придется использовать программы сторонних разработчиков. Есть целый класс программ, предназначенных для удаленного управления и администрирования компьютеров. Среди них есть весьма дорогие программы, но существуют и бесплатные. Независимо от цены, программы обладают различным быстродействием и различными дополнительными возможностями. Одну из этих программ мы рассмотрим подробно.

Программы удаленного управления и администрирования VNC

VNC (Virtual Network Computing) — это плотформо-независимая система удаленного доступа к рабочему столу. Точнее это целое семейство программ,

предназначенных для удаленного управления и администрирования компьютеров.

Программы, основанные на системе VNC, разрабатываются несколькими известными фирмами, а также, поскольку код системы открытый, множеством индивидуальных программистов. Вот наиболее известные реализации системы:

- RealVNC, исходная версия, **http://www.realvnc.com**;
- TightVNC — система, оптимизированная для узких каналов в Интернете, **http://www.tightvnc.com**;
- Ultr@VNC — система с дополнительными возможностями, такими как пересылка файлов, чат, драйвер видео, NT/AD-безопасность, **http://www.uvnc.com**;
- TridiaVNC — система, включающая средства работы в обход брандмауэров, **http://www.itivity.tridia.com/**;
- Win2VNC — система, реализующая один виртуальный рабочий стол на двух компьютерах, **http://sourceforge.net/projects/win2vnc**.

Все версии Linux содержат в своем составе VNC. Linux позволяет использовать в системе несколько рабочих столов, поэтому VNC, предназначенные для Linux, используют несколько портов. Обычно это диапазон 5900—5906. В Windows система не допускает создания нескольких рабочих столов. С появлением Windows Vista использование VNC для этой системы было затруднено, но уже через несколько месяцев после выхода новой ОС появились не только коммерческие, но и бесплатные реализации VNC. Одной из первых бесплатных версий VNC, пригодной для работы с Windows Vista, стала UltraVNC. При установке последней версии UltraVNC на компьютер под управлением Windows Vista установите подключение к Интернету. Вполне возможно, что когда книга попадет к читателям, дистрибутив программы будет содержать полный набор файлов, но во время написания этих строк для работы в Windows Vista программа использовала дополнения, которые закачивались на компьютер пользователя в процессе установки программы. Для Linux обычно подходящая версия VNC есть в дистрибутиве, а программы с расширенными возможностями можно получить из репозиториев системы.

Подключение "Windows — Windows"

Начнем рассмотрение работы VNC в среде Windows Vista и при подключении к удаленному рабочему столу в этой же системе. Windows Vista для до-

машних пользователей не содержит специальных средств для предоставления доступа к рабочему столу, и UltraVNC восполняет этот пробел.

Установка программы трудностей не вызывает. Важно только во время установки выбрать обе части программы — клиентскую (Viewer) и серверную (Server). Сервер UltraVNC может запускаться просто как программа, но можно и установить его в качестве службы. В последнем случае компьютер всегда будет готов к приему входящих подключений.

Итак, на двух компьютерах под управлением Windows Vista установлена программа UltraVNC. Оба компьютера входят в вашу сеть или между ними установлен VPN-канал, вам известен IP-адрес для доступа к удаленному компьютеру. Как вариант, на удаленном компьютере работает клиент DynDNS, и вы знаете доменное имя этого компьютера, а ваш компьютер имеет доступ в Интернет.

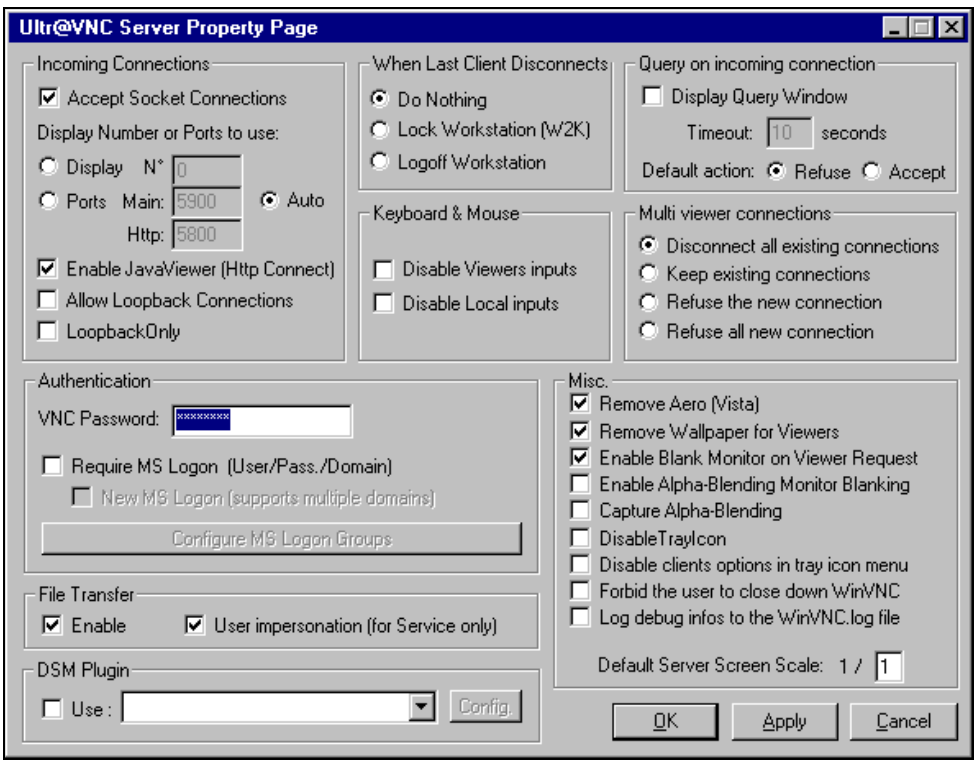


Рис. 5.22. Окно **Ultr@VNC Property Page**

Это достаточные условия для обеспечения возможности подключения к удаленному компьютеру через VNC.

После установки программы в главном меню появляются ярлыки для UltraVNC Server и UltraVNC Viewer. Создается также дополнительный ярлык Install WinVNC Service для установки сервера в качестве службы. При первом запуске Install WinVNC Service откроется окно **Ultr@VNC Property Page**, в котором можно установить свойства сервера (рис. 5.22).

При первом запуске программы нет смысла менять настройки, установленные по умолчанию. Важно только в разделе **Authentication** задать **VNC Password** — пароль для подключения к серверу, который должен будет ввести пользователь, выполняющий подключение к нему. Введя пароль, нажмите кнопки **Apply** (Применить) и **OK**. В системном трее появится значок с изображением глаза на синем фоне. Щелчком правой кнопкой мыши по этому значку вы можете вызвать меню, из которого есть доступ и к только что рассмотренному окну, и к другим настройкам и командам управления сервером.

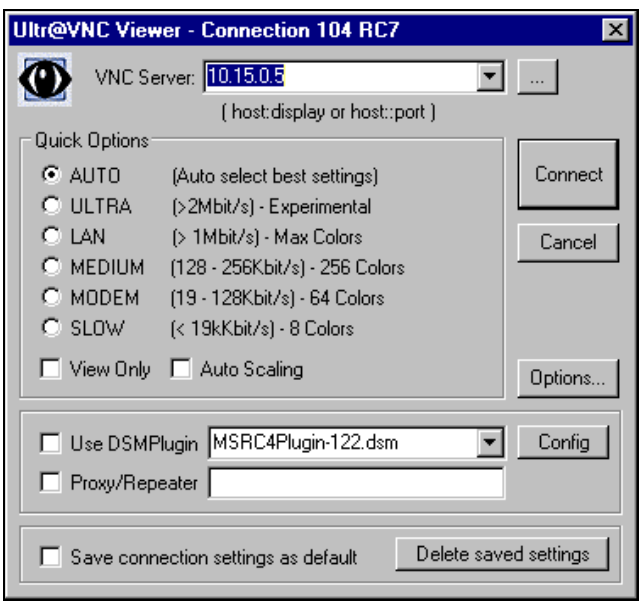


Рис. 5.23. Окно **Ultr@VNC Viewer - Connection 104 RC7**

Запустив UltraVNC Viewer, вы увидите окно **Ultr@VNC Viewer - Connection 104 RC7** (рис. 5.23), где необходимо только указать IP-адрес удаленного

компьютера, где запущен сервер VNC, или имя этого компьютера, по которому он доступен. Если используется нестандартный порт, то через двоеточие следует указать номер порта. При подключении через DynDNS номер порта необходимо указывать всегда, например, так: mycomp.webhop.net:5900.

Здесь тоже нет необходимости при первом включении изменять другие настройки. Постепенно, экспериментируя и читая материалы на сайте **http://www.uvnc.com** и другие материалы в Интернете, которые легко можно найти по ключевому слову VNC, вы, возможно, решите, что надо что-то изменить в настройках.

Остается нажать кнопку **Connect** (Подключиться).

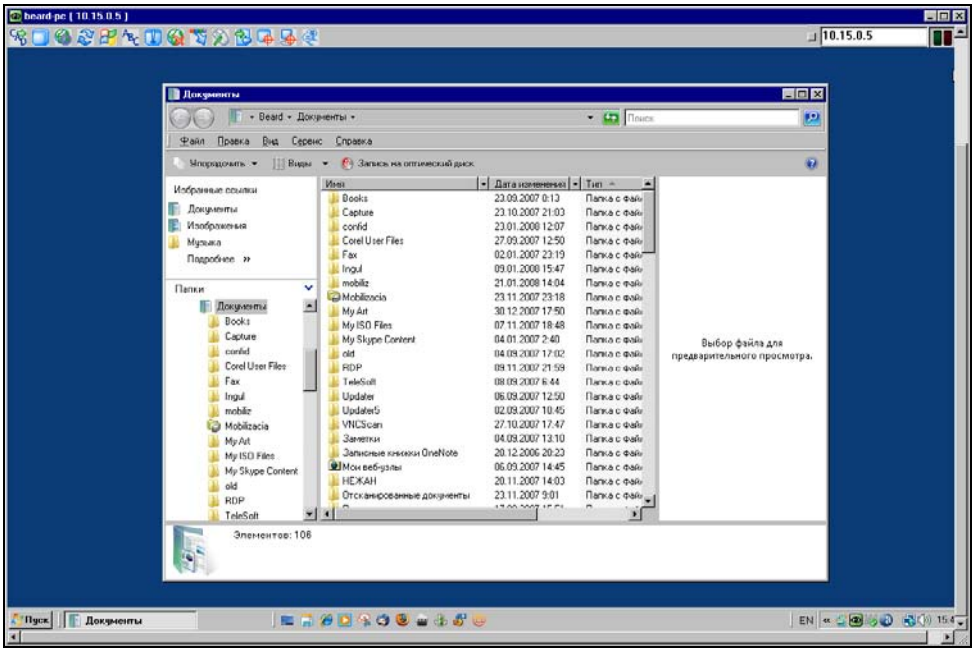


Рис. 5.24. Окно удаленного рабочего стола

Возможно, что подключение не будет выполнено... Проверьте, что все параметры настройки сервера и клиента оставлены по умолчанию, и повторите подключение. Важно, чтобы на удаленном компьютере был выполнен вход в систему. В противном случае клиент не может установить подключение. Убедитесь, что брандмауэр или файервол не запрещают подключение через

порт 5900. Если удаленный компьютер подключен к Интернету через ADSL-модем и маршрутизатор, убедитесь что установлено перенаправление (Port Forwarding) по этому порту на компьютер с сервером VNC.

Если все выполнено, как описано выше, после ввода пароля, запрошенного программой, вы увидите рабочий стол удаленного компьютера (рис. 5.23).

Теперь мы можем работать на удаленном компьютере, как у себя дома. Но программа имеет множество дополнительных возможностей. Наводя курсор на значки под заголовком окна (рис. 5.25), вы можете увидеть всплывающие надписи, поясняющие назначение кнопок.

Рис. 5.25. Кнопки для использования дополнительных функций UltraVNC

Рассмотрим назначение кнопок в порядке их расположения на рис. 5.25:

-  — послать на удаленный компьютер сочетание клавиш <Ctrl>+ +<Alt>+<Del>. Смысл этого действия понятен;
-  — включение полноэкранного режима работы с удаленным рабочим столом;
-  — вызов окна свойств подключения;
-  — обновление экрана. Иногда требуется при плохом качестве связи с удаленным компьютером;
-  — нажатие кнопки **Пуск** (Start) на удаленном компьютере;
-  — отправить любое сочетание клавиш на удаленный компьютер;
-  — показать статус подключения. Можно увидеть скорость соединения, использованный трафик;
-  — отключиться от удаленного компьютера;
-  — скрыть кнопки рассматриваемой панели;
-  — погасить экран удаленного компьютера. В Windows Vista через пару секунд экран включается самопроизвольно;

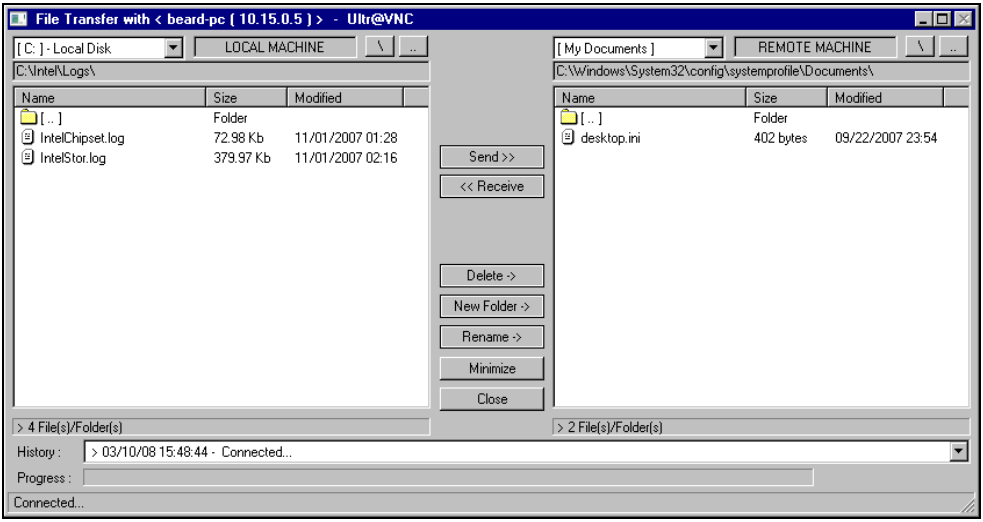


Рис. 5.26. Окно обмена файлами

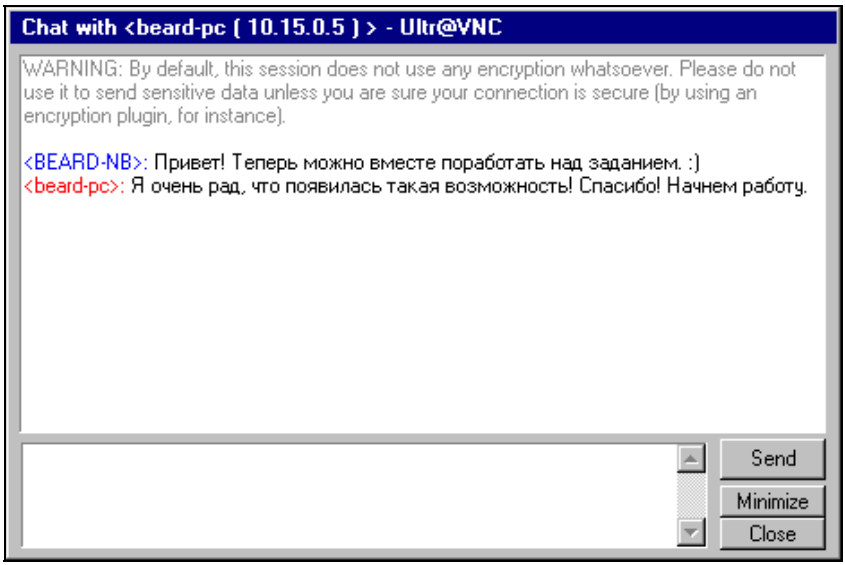


Рис. 5.27. Окно чата **Chat with *<имя_удаленного_компьютера>***

-  — открыть окно обмена файлами **File Transfer** (рис. 5.26). Очень полезная функция;

- — выбрать одно окно. Позволяет работать не со всем рабочим столом, а только с выбранным окном;
- — возврат к полному рабочему столу;
- — открыть окно чата с пользователем удаленного компьютера (рис. 5.27).

На взгляд автора, лучшего инструмента для доступа к удаленному рабочему столу и управления удаленным компьютером не существует на сегодняшний день. Во всяком случае среди бесплатных продуктов.

Подключение "Windows — Linux"

Как было уже сказано, большинство версий Linux имеют в своем составе VNC. Как и для UltraVNC, настройки по умолчанию подходят для большинства практических случаев.

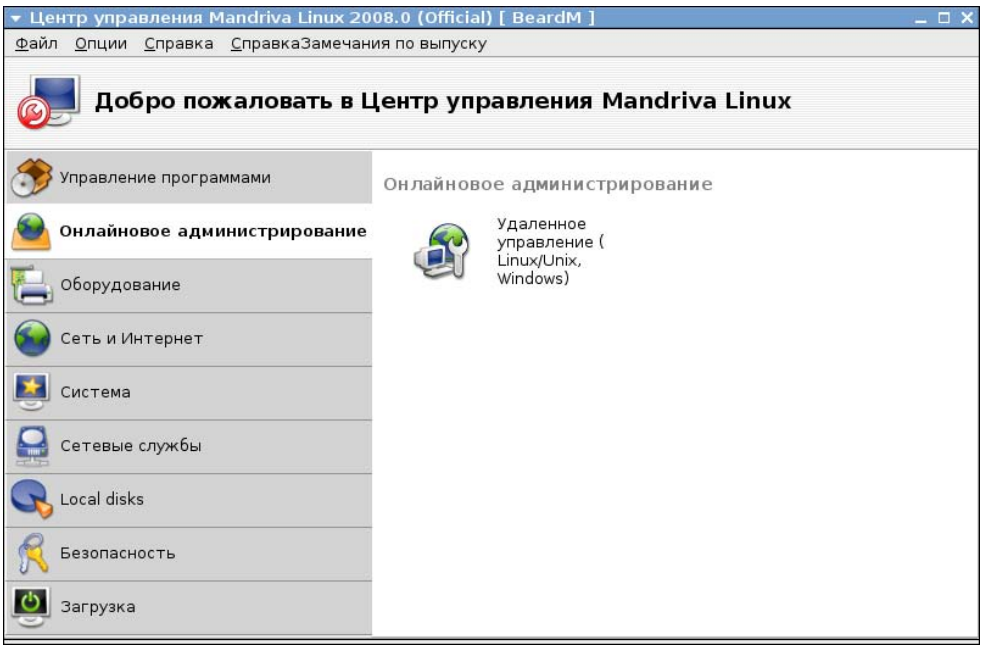


Рис. 5.28. Окно **Центр управления Mandriva Linux 2008.0**, раздел **Онлайновое администрирование**

Чтобы запустить VNC-сервер в Mandriva Linux, следует открыть **Центр управления Mandriva Linux** и войти в **Онлайновое администрирование** (рис. 5.28).

Щелкнув по значку **Удаленное управление (Linux/Unix, Windows)**, откройте соответствующее окно (рис. 5.29).

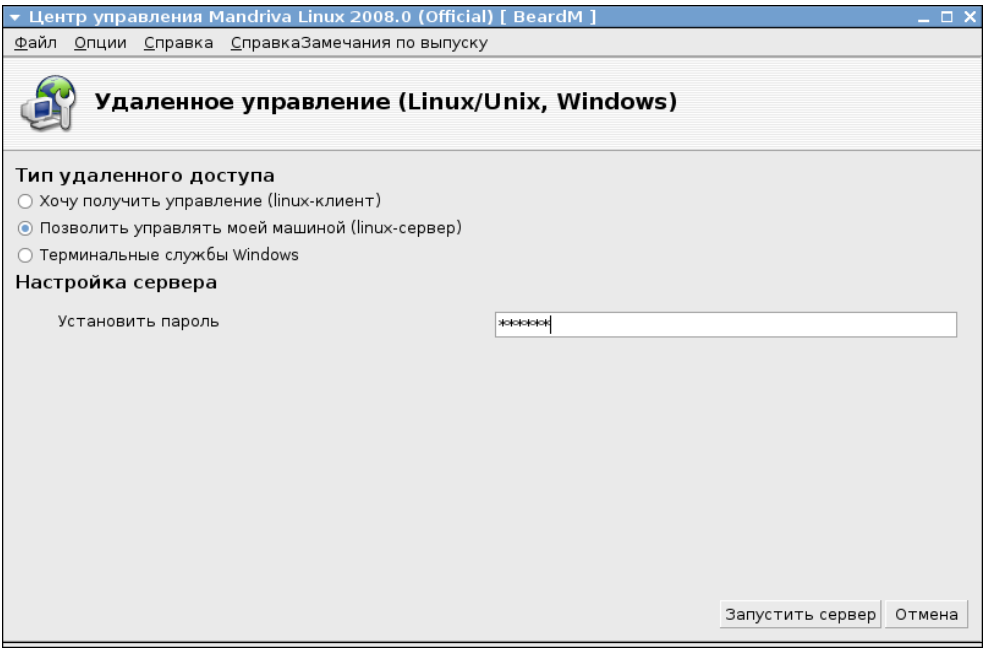


Рис. 5.29. Окно **Центр управления Mandriva Linux 2008.0**, страница **Удаленное управление (Linux/Unix, Windows)**

В этом окне выберите переключатель **Позволить управлять моей машиной (linux-сервер)** и установите пароль для доступа.

Сервер запустится после нажатия кнопки **Запустить сервер**, и вы увидите миниатюрное окно сервера RFB (рис. 5.30). RFB — это протокол Remote FrameBuffer, который применяется в системах VNC.

Можно подключаться. Правда, в Mandriva Linux по умолчанию настройки файервола могут не разрешить подключение. Тогда в **Центре управления Mandriva Linux** на странице **Безопасность** (рис. 5.31) щелкните по значку **Настройка файервола** и в окне **Настройка файервола** (рис. 5.32) укажите в

разделе **Дополнительно** номера разрешенных для входящих подключений портов.

Рис. 5.30. Окно **RFB**

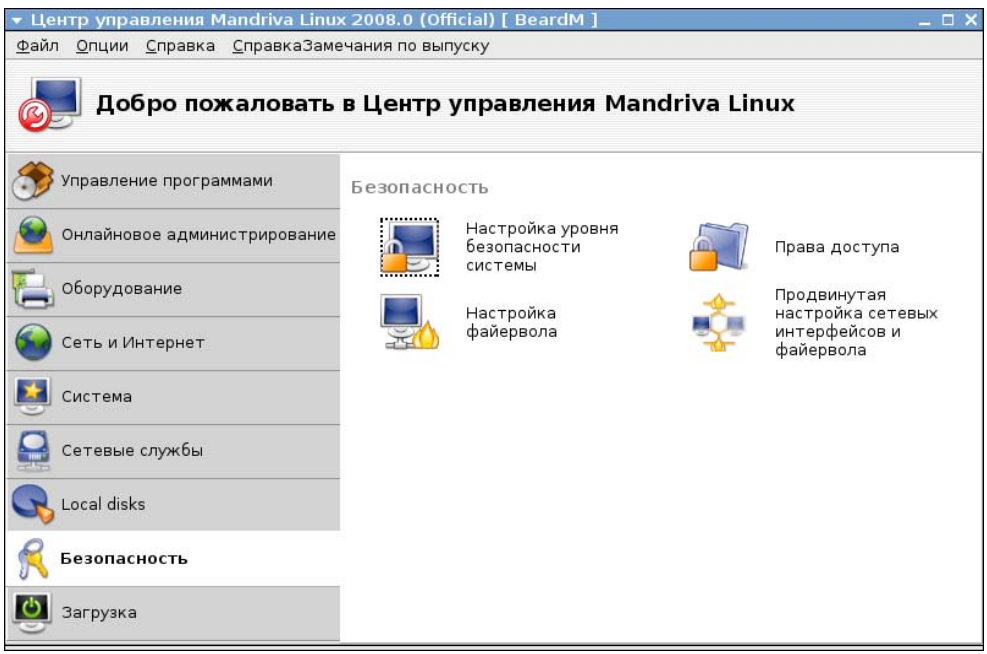


Рис. 5.31. Окно **Центр управления Mandriva Linux 2008.0**, страница **Безопасность**

Лучше указать диапазон возможных номеров портов через двоеточие и вид протокола, по которому будет осуществляться подключение — 5900:5906/tcp. После нажатия кнопки **OK** в этом и следующих двух окнах, в которых ничего менять не надо, сервер будет готов к подключению.

В ASPLinux для запуска сервера выполните **Система | Параметры | Удаленный рабочий стол**. В открывшемся окне **Параметры удаленного рабочего стола** установите все флажки, как на рис. 5.33, установите пароль для подключения и нажмите кнопку **Закрыть**.

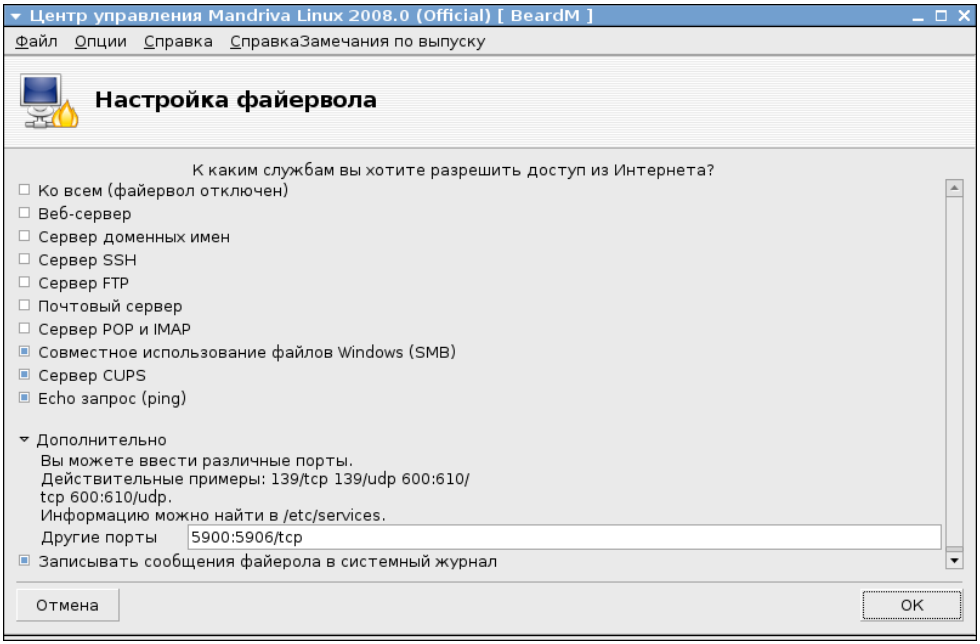


Рис. 5.32. Окно **Центр управления Mandriva Linux 2008.0**, страница **Настройка файервола**

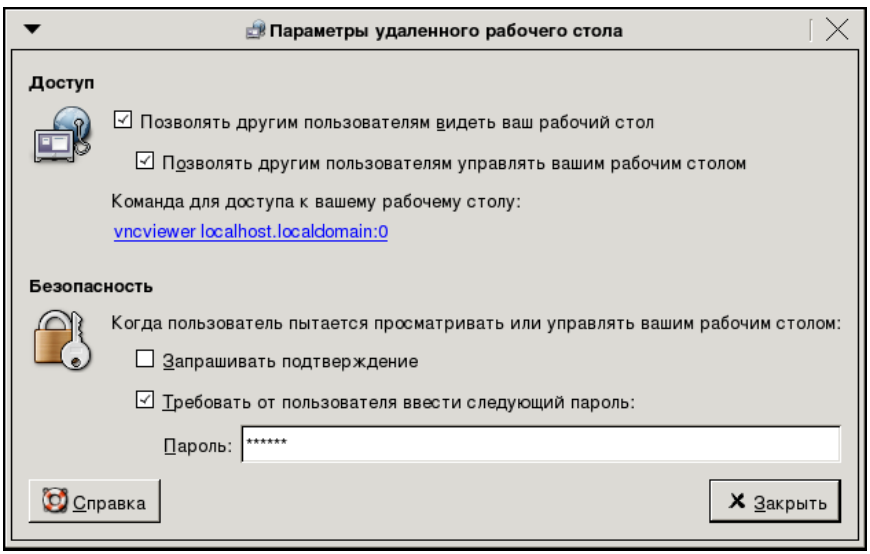


Рис. 5.33. Окно **Параметры удаленного рабочего стола**

Все, можно подключаться. Результат подключения представлен на рис. 5.34. Функция обмена файлами и чат при подключении к Linux не доступны.

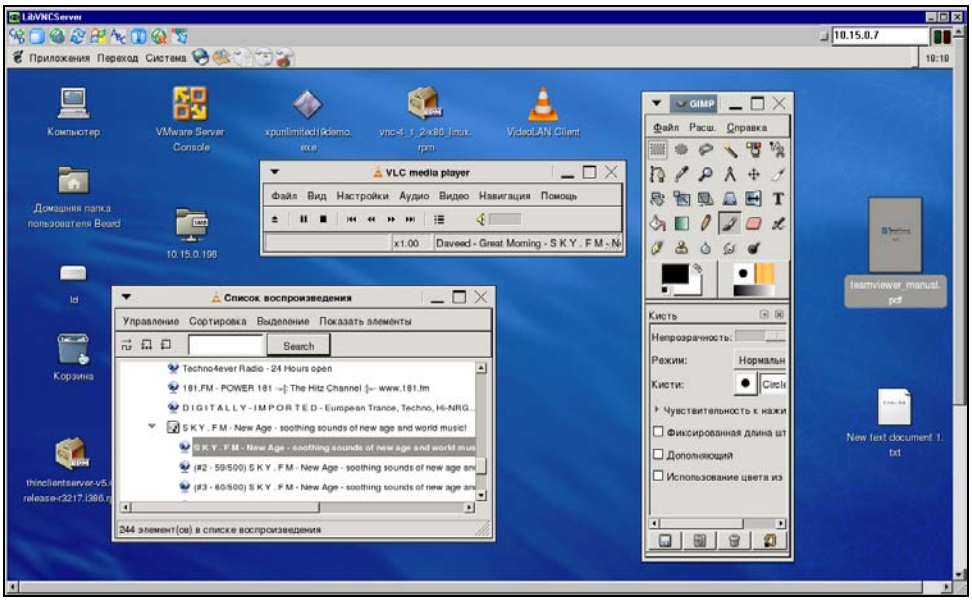


Рис. 5.34. Окно управления удаленным рабочим столом ASPLinux

Подключение "Linux — Windows" и "Linux — Linux"

Ранее мы рассмотрели практически все особенности доступа к Windows и Linux. VNC-клиент в Linux имеет очень простой интерфейс. При его запуске (найдите в меню вашей системы самостоятельно) откроется маленькое окно для ввода IP-адреса или имени компьютера, а после нажатия клавиши <Enter> — окно для ввода пароля. Введя пароль, нажмите клавишу <Enter>. Возможно, что необходимо подобрать, на какую из клавиш <Enter> нажимать, — на цифровой или основной части клавиатуры. Других особенностей подключения из Linux нет.

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, настройки маршрутизаторов, брандмауэров и файерволов, 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:

1. Зайти на сайт **https://logmein.com** и ввести свои учетные данные.

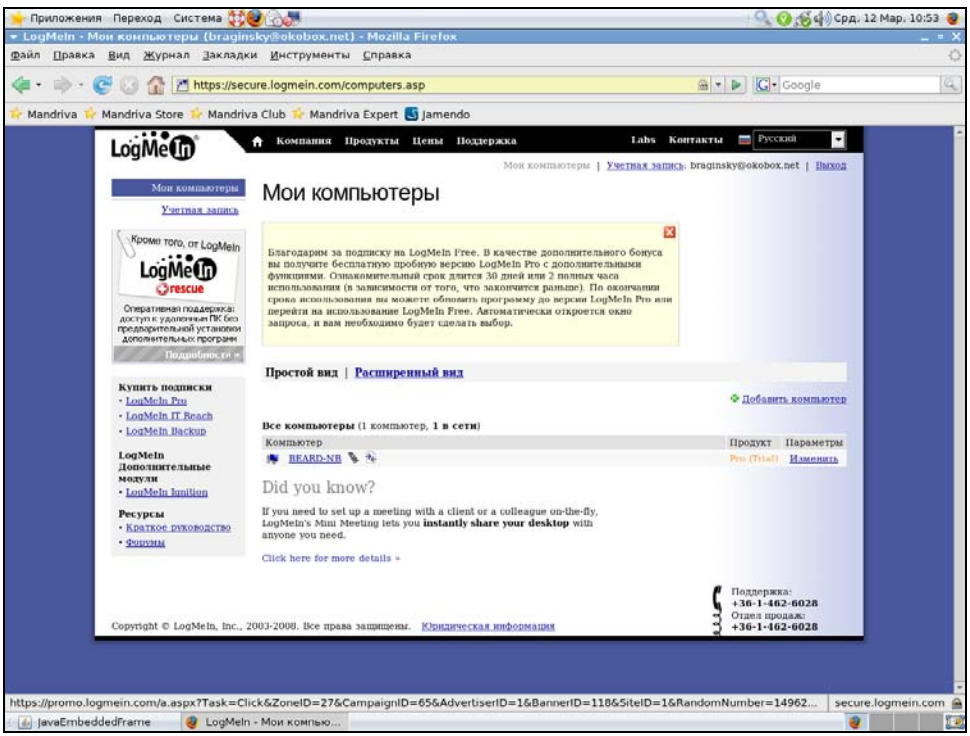


Рис. 5.35. Рабочий стол Mandriva Linux, страница пользователя LogMeIn

2. Попав на страницу пользователя, выбрать управляемый компьютер (рис. 5.35).
3. На открывшейся странице меню пользователя (рис. 5.36) LogMeIn выбрать требуемое действие.

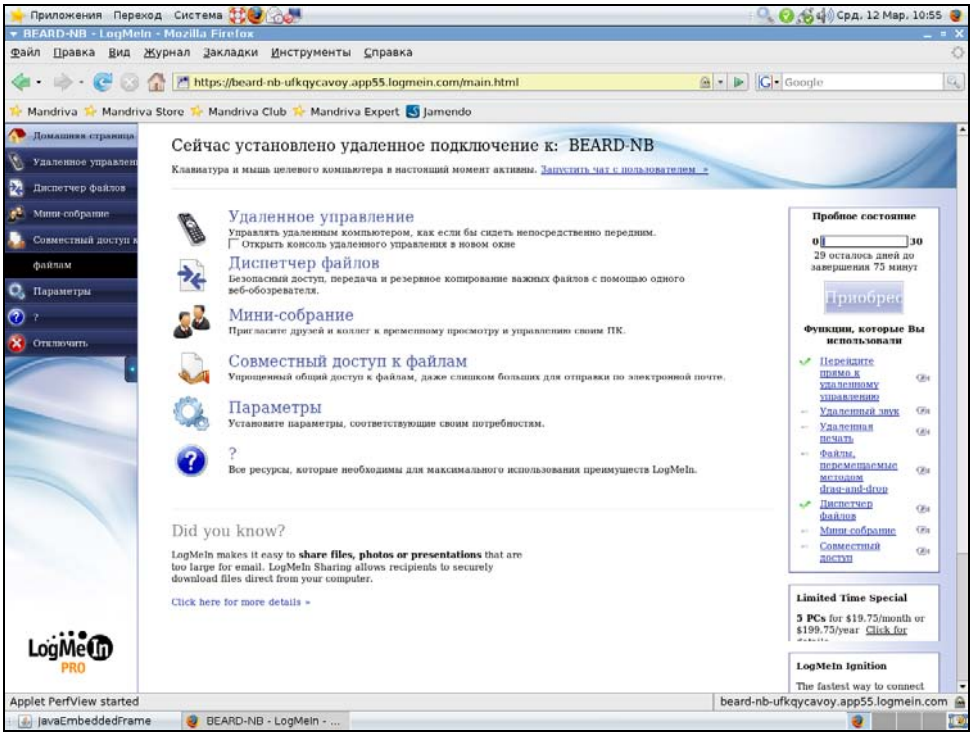


Рис. 5.36. Рабочий стол Mandriva Linux, меню пользователя LogMeIn

При выборе удаленного управления в окне браузера откроется рабочий стол удаленного компьютера (рис. 5.37).

Из этого окна можно инициировать чат с удаленным пользователем (рис. 5.38), а при выборе в меню **Диспетчер файлов** открывается файловый менеджер (рис. 5.39), в двух окнах которого видны файлы локального и удаленного компьютера.

Посредством LogMeIn можно организовать удаленную помощь пользователям компьютеров под управлением Windows.

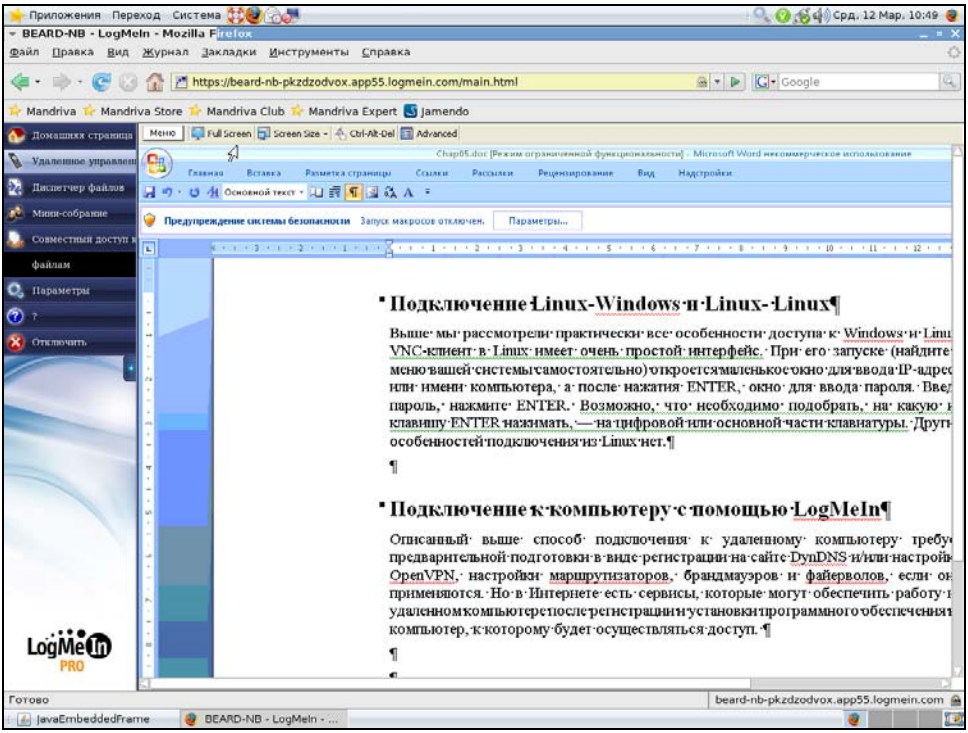


Рис. 5.37. Рабочий стол Mandriva Linux, документ, открытый на удаленном компьютере

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 потребуется 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.

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, Teamviever (**http://www.teamviewer.com/**). Эта программа должна быть установлена на оба компьютера, других настроек она не требует, но бесплатно проработает месяц или 25 часов.

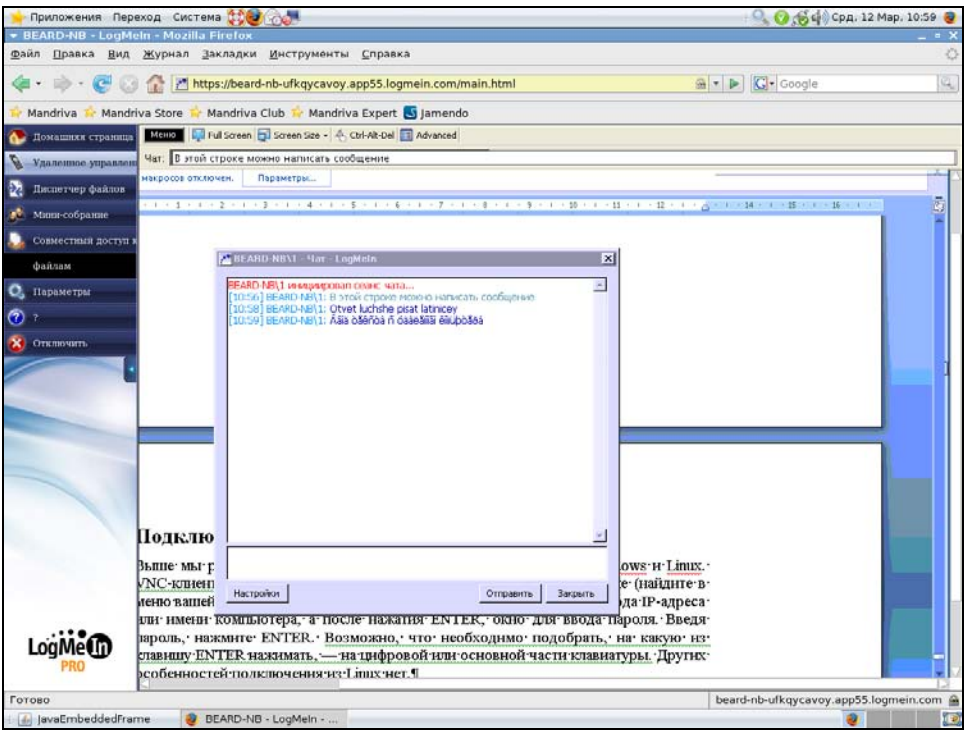


Рис. 5.38. Рабочий стол Mandriva Linux,
чат с удаленным пользователем

Практически все программы для удаленного управления рабочим столом через Интернет используют какие-либо дополнительные сервисы. Именно за их использование надо платить. Только 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.

Впрочем, есть еще одна программа и служба в Интернете, доступная с сайта **logmein.com**, которая во многих случаях поможет организовать доступ к своему компьютеру. Вот что говорится об этой программе на сайте:

"LogMeIn Hamachi — это служба VPN, которая без труда настраивается за 10 минут и обеспечивает безопасный удаленный доступ к сети вашего предприятия отовсюду, где можно подключиться к Интернету.

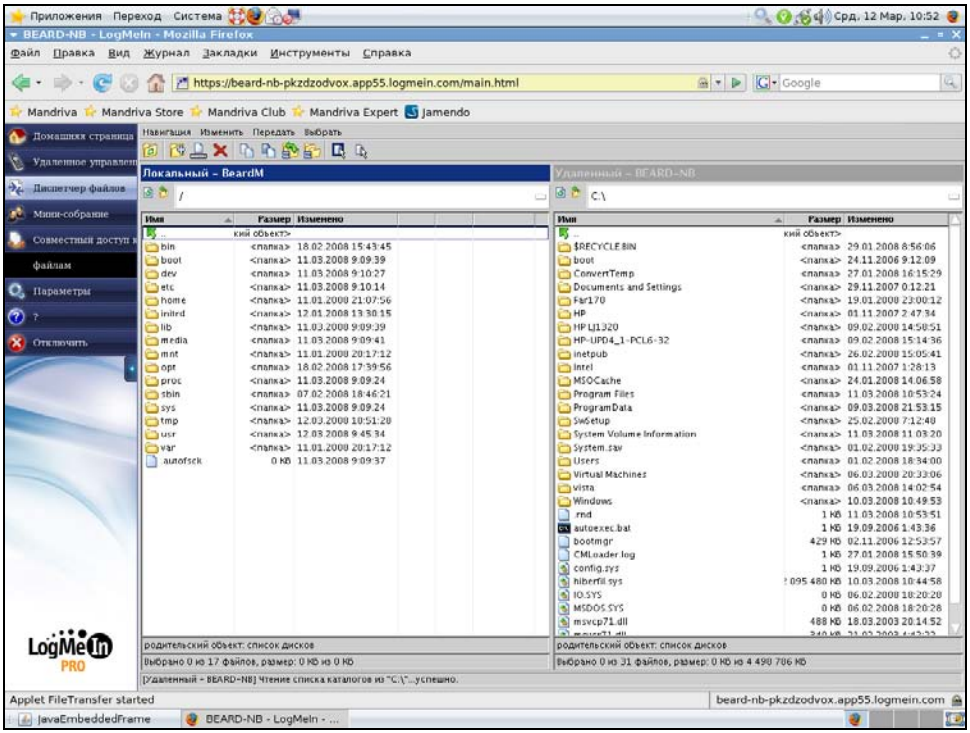


Рис. 5.39. Рабочий стол Mandriva Linux, страница файлового менеджера

Служба взаимодействует с существующим брандмауэром и не требует дополнительной настройки. Hamachi — это первое приложение, успешно объединяющее несвязанные сетевые технологии в один мощный пакет, обеспечивающий непревзойденный уровень прямой связи между одноранговыми узлами".

Программа устанавливается действительно быстро и просто. Язык интерфейса программы может быть выбран во время установки. При первом запуске программы происходит автоматическая регистрация на сервере поставщика услуги, присваивается IP-адрес. Пользователь должен указать имя новой виртуальной сети, в которую будут входить его компьютеры.

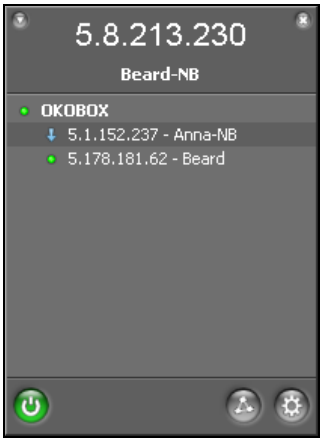


Рис. 5.40. Окно программы LogMeIn Hamachi

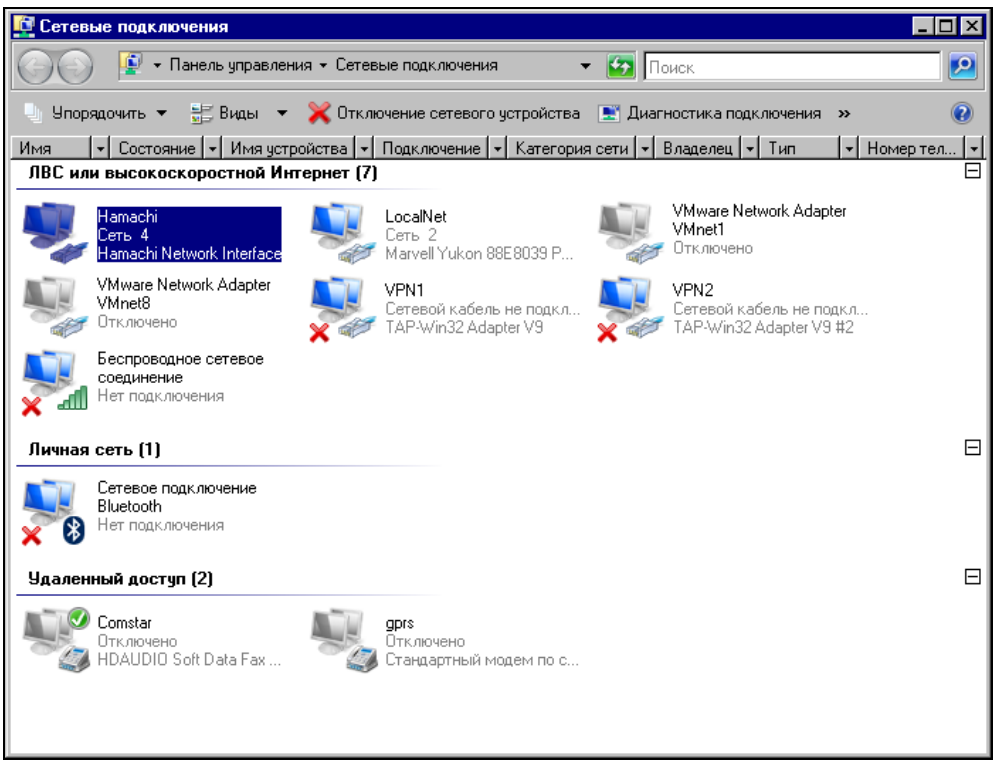


Рис. 5.41. Окно **Сетевые подключения** (подключение Hamachi выделено)

Если нет никаких помех для создания прямого виртуального канала между компьютерами, то он создается. В противном случае канал проходит через сервер поставщика. Такое соединение значительно медленнее, но важно, что оно все равно создается. В окне программы (рис. 5.40) такие медленные соединения помечаются стрелкой. Нормальные соединения отмечены точкой.

Если соединение прямое, то вы можете через него работать с папками и файлами, к которым открыт общий доступ. Можно использовать и программы VNC, терминальный доступ и другие программы удаленного управления и администрирования.

Как и OpenVPN, Hamachi создает виртуальный сетевой адаптер и соответствующее ему сетевое подключение (рис. 5.41).

На странице загрузки программы доступна версия для Linux.

Заключение

Вот мы и подошли к завершению разговора о маленькой домашней сети. Современные технологии и доступность Интернета позволяют создавать такие сети не только в одном помещении, как мы это делали в начале книги, но и объединять в виртуальную локальную сеть компьютеры, подключенные к Интернету. Средства удаленного управления компьютерами позволяют получать доступ к рабочему столу любого компьютера вашей сети. Освоив рассмотренные в книге программы, вы получаете практически неограниченную свободу доступа к вашим компьютерам из любой точки мира. Эту свободу вы ощутите в еще большей степени, если будете использовать несколько способов подключения к Интернету и локальной сети. Вернитесь к рис. 5.41. Обратите внимание, что в окне **Сетевые подключения** показаны десять подключений, выполненных по различным технологиям. Среди них есть два модемных подключения, одно из которых использует модем мобильного телефона (на рисунке подключение gprs).

Подключения через оператора сотовой связи обычно не имеют реальных IP-адресов. Тем не менее, посмотрите на рис. 5.42 и 5.43.

Это сеанс управления удаленным рабочим столом с компьютера, подключенного к Интернету через мобильный телефон. А на втором рисунке страница пользователя LogMeIn, где видно, что два компьютера, находящиеся в разных локальных сетях, доступны. Недоступен третий компьютер, с которого осуществляется доступ к двум другим. Именно он подключен к Интернету через мобильный телефон.

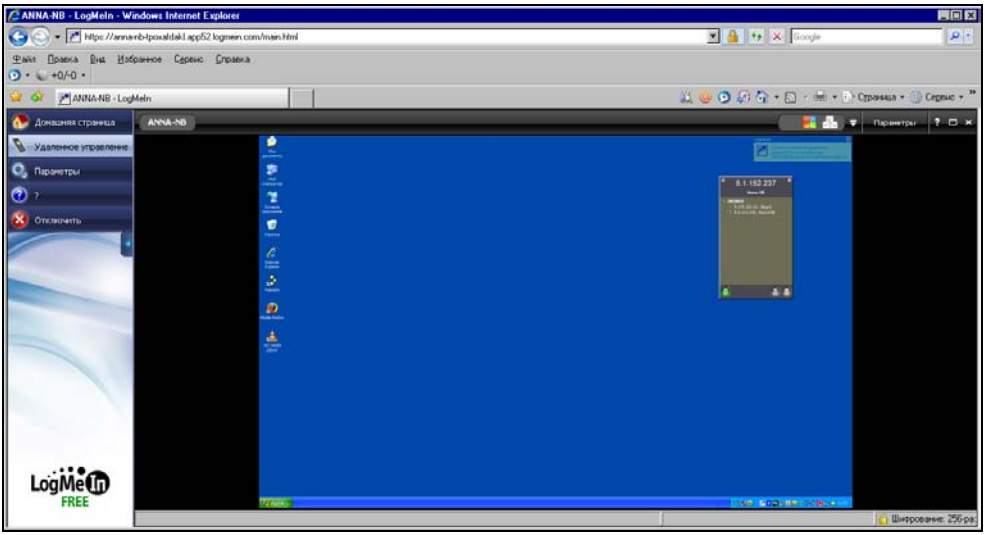


Рис. 5.42. Окно интернет-браузера с выполненным подключением к удаленному рабочему столу через LogMeIn

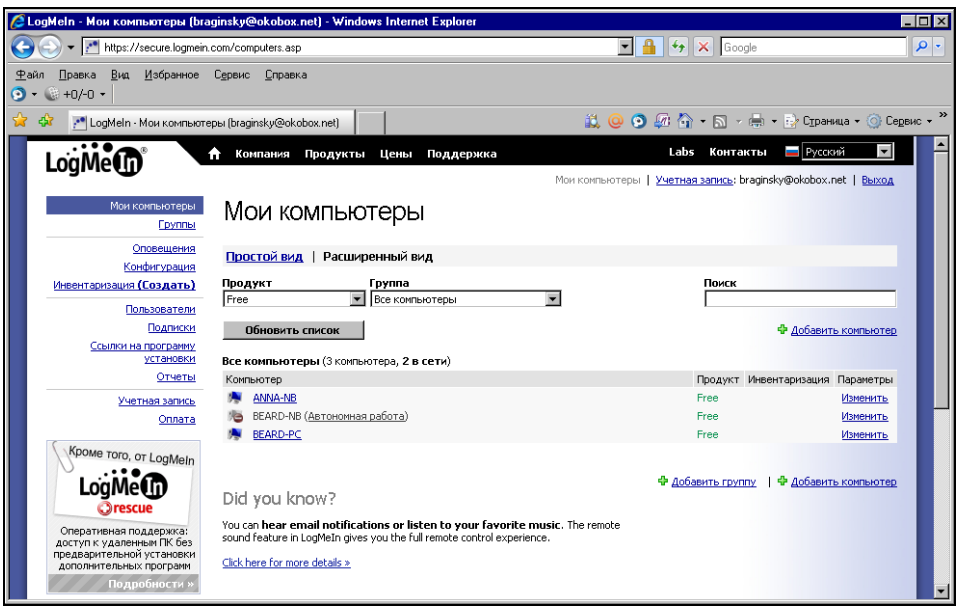


Рис. 5.43. Окно интернет-браузера на странице пользователя LogMeIn

Это говорит о том, что подключения возможны только к тем компьютерам, которые сами сети, в которых они находятся, имеют внешний IP-адрес. Но само подключение возможно с компьютера, имеющего выход в Интернет, выполненный любым доступным способом, включая мобильную связь или районные локальные сети.

Следует сделать еще одно замечание. При создании подключения через мобильный телефон, возможно, придется подкорректировать его настройки. Так, при подключении через оператора "Билайн" (Москва) автор изменил адреса DNS-серверов, использовав адреса, рекомендованные провайдером, коммутируемого подключения, которое он применяет.

* * *

Вот теперь все. Остается пожелать вам успеха в создании своей маленькой, но не имеющей границ сети. Если возникнут вопросы, обращайтесь к автору по адресу электронной почты **braginsky@comail.ru**.

Приложение

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, волоконно-оптическая связь между повторителями (репитерами)).

100BASE-FX (оптоволоконный кабель 100 Мбит/с)

Реализация сети Ethernet на оптоволоконном кабеле, обеспечивающая скорость передачи данных 100 Мбит/с.

10BASE-T (витая пара 10 Мбит/с)

Спецификация IEEE 802.3 сетей Ethernet на неэкранированной витой паре (UTP).

100BASE-T (Fast Ethernet)

Технология 100 Мбит/с, основанная на методе доступа Ethernet/CD и использующая кабель типа "витая пара".

Active Directory

Термин Active Directory используется как для обозначения каталога с информацией о пользователях, компьютерах и других объектах сети, так и для обозначения службы каталога — комплекса программ, обеспечивающих доступ к этой информации. Active Directory поддерживает систему имен DNS, а имена в формате NetBIOS использует только для совместимости со старыми операционными системами. Начиная с 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.

AUI (Access Unit Interface)

Интерфейс устройств доступа; интерфейс подключаемых устройств. *N*-контактный кабельный интерфейс штекерного типа, используемый в магистральных соединениях.

Auto-sensing 10/100 Mbps (автоматическое распознавание скорости передачи данных 10/100 Мбит/с)

Средство, позволяющее коммутаторам и концентраторам автоматически распознавать и настраивать скорость передачи данных по кабелю (называемое также *автосогласованием*). Интеллектуальные средства авторасознавания способны, кроме того, определять качество канала и автоматически выбирать максимальную скорость передачи.

BNS

Кабельный интерфейс для соединения коаксиального кабеля в магистральных сетях.

Bridge (мост)

Комбинация аппаратного и программного обеспечения, соединяющая две локальных сети и позволяющая осуществлять коммуникации между их станциями. Мосты функционируют на канальном (втором) уровне эталонной модели OSI (Open Systems Interconnection, модель взаимодействия открытых систем).

Bridge/Router (мост/маршрутизатор)

Устройство, функционирующее как мост, как маршрутизатор или как оба 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.

CSMA/CD

Метод доступа к среде передачи (кабелю), определенный в спецификации IEEE 802.3 для локальных сетей Ethernet. CSMA/CD требует, чтобы каждый узел, начав передачу, продолжал прослушивать сеть на предмет обнаружения попытки одновременной передачи другим устройством — коллизии. При возникновении конфликта передача должна быть незамедлительно прервана и может быть возобновлена по истечении случайного промежутка времени. В сети Ethernet с загрузкой 35—40% коллизии возникают довольно часто и могут существенно замедлить работу. При небольшом числе станций вероятность коллизий существенно снижается.

DHCP (Dynamic Host Configuration Protocol)

Служба динамического выделения сетевых адресов. Позволяет не загружать администратора сети проблемами распределения адресов, работает автоматически.

DNS (Domain Name System)

1. Символьный идентификатор — имя, например, SERV.FIRMA.RU. Этот адрес назначается администратором и состоит из нескольких частей, на-

пример, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или Telnet.

2. 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.
3. Распределенный механизм имен/адресов, используемых в Интернете. Применяется для разрешения логических имен в IP-адреса. В Интернете позволяет работать с понятными и легко запоминающимися именами вместо неудобных числовых IP-адресов.

DOS ODI и DOS NDIS

Сетевые драйверы, поддерживающие большинство ОС, в том числе Novell NetWare, Microsoft 9*x*, Microsoft Windows for Workgroups, Microsoft LAN Manager, Banyan VINES, Artisoft LANtasic, IBM LAN Server, HP LAN Manager и многие другие.

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 локальных вычислительных сетей, поддерживающий скорости передачи данных 10 и 100 Мбит/с.

FTP (File Transfer Protocol)

Протокол передачи данных в сети. Применяется для передачи файлов.

Hab

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 и для обмена информацией в локальной сети, а также для хранения информации в виде HTML-файлов.

Interface

1. Физическое устройство, соединяющее две системы или два устройства.
2. Стандарт (такой, как RS-232-C), специфицирующий взаимодействие систем.

(Integrated Service Digital Network)

Международный стандарт передачи голоса, видеоинформации и данных по цифровым телефонным линиям.

LAN (Local Area Network)

Локальная компьютерная (вычислительная) сеть. Русское сокращение — ЛВС (локальная вычислительная сеть).

LINKLOCAL

Диапазон сетевых адресов, применяемых в локальных компьютерных сетях и не используемых в глобальных сетях.

MAC-адрес

Аппаратный адрес сетевого устройства. Не может повторяться, обеспечивает идентификацию сетевого устройства независимо от назначаемого адреса или имени.

NetBEUI (NetBIOS Enhanced User Interface)

NetBEUI (расширенный NetBIOS), IPX/SPX, TCP/IP. NetBEUI — устаревающий протокол, пригодный для маленькой сети, которая состоит из одного сегмента. По умолчанию не поддерживается в Windows XP.

Proxy Server (прокси-сервер)

Система, находящаяся между исполняемыми приложениями (такими как Internet Explorer) и соединением с Интернетом. Она перехватывает запросы к серверу, пытаясь выполнить их самостоятельно. Такой способ увеличивает быстродействие за счет отсечения повторных запросов одной и той же информации из Интернета. Proxy Server может кэшировать загружаемые из Интернета страницы (файлы). Если кто-то еще обращается к странице или файлу, ранее уже кем-либо запрошенным, Proxy Server выдает их из своего кэша. Это значительно быстрее, чем снова загружать страницу (файл) из Интернета. Прокси-серверы также могут выступать в качестве сетевого экрана, фильтруя IP-трафик по порту или IP-адресу.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Современный сетевой протокол. Подробно описан в *главе 1*.

Telnet

Один из старейших протоколов Интернета. Он появился в 1969 г. в ARPANET (сеть государственной организации The Advanced Research Projects Agency — бюро проектов передовых исследований. Теперь организация называется DARPA). Имя этого протокола является сокращением от названия telecommunications network protocol (сетевой коммуникационный протокол). Его описание находится в спецификации RFC 854. Этот протокол позволяет подсоединиться к удаленному компьютеру, находящемуся в сети, и работать с ним как будто бы вы работаете непосредственно на этом удаленном компьютере, т. е. в режиме терминала. Ваши возможности ограничены уровнем доступа, который задан для вас администратором удаленной системы.

В поставку Windows входит одноименная программа, которую вы можете запустить из меню **Пуск | Выполнить**.

Throughput (производительность, пропускная способность)

Общий объем корректно переданной (или обработанной) информации в заданный период времени. Выражается в битах в секунду или в пакетах в секунду.

UTP (неэкранированная витая пара)

Это самый популярный тип кабеля, используемый для соединения настольных систем и рабочих групп. *См. витая пара*.

Virtual LAN (VLAN, виртуальная локальная сеть)

Виртуальная локальная сеть (VLAN) состоит из связанной группы пользователей, которые могут осуществлять коммуникации непосредственно друг с другом и получать широковещательную информацию от других пользователей. При этом входящие в группу пользователи необязательно должны находиться в одном месте. В сетевой инфраструктуре, основанной на многопортовых коммутаторах и концентраторах, все рабочие станции могут взаимодействовать непосредственно друг с другом и получать друг от друга широковещательные пакеты. В такой сети виртуальные локальные сети (VLAN) применяются для управления трафиком, обеспечения защиты и для контроля широковещательной рассылки.

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.

Беспроводная сеть

Сеть, построенная на основе беспроводных сетевых адаптеров и концентраторов. Среди множества изделий различных фирм обращают на себя внимание концентраторы фирмы Intel. Intel PRO/Wireless 2011 LAN Access Point (точка доступа для связи удаленного компьютера с локальной сетью) может применяться и как повторитель (repeater) для увеличения максимального расстояния при подключении. Intel PRO/Wireless 2011 LAN PC Card — беспроводный сетевой адаптер для компьютеров.

Строить сеть полностью на основе таких устройств нерационально. В отдельных случаях они позволяют обеспечить доступ пользователям, не имеющим возможности подключиться к сети с помощью кабеля.

Витая пара

Кабели на основе витой пары находят широкое применение в сетях передачи данных. Для кабеля на основе витых пар используются медные проводники диаметром 0,64—0,51 мм. В качестве материала изоляции обычно применяются полиэтилен, полипропилен, тефлон, вспененный полиэтилен. Неэкранированная витая пара представляет собой от 1 до 100 пар медных изолированных проводников, скрученных парами с согласованными шагами для уменьшения взаимного влияния. Наиболее распространены двух- и четырехпарные конструкции. Цветовая комбинация проводников фиксирована: один из проводников в паре имеет белый цвет с метками цвета второго одноцветного проводника этой пары — синего, оранжевого, зеленого или коричневого. Конструктивно все кабели делятся на экранированные и неэкранированные. Экранированные конструкции более защищены от помех и имеют лучшие показатели переходного затухания, но их применение требует специальных разъемов и правильной схемы заземления, поэтому в нашей стране большее распространение получили неэкранированные кабели. Наиболее распространен серый цвет кабеля, однако производятся кабели всех цветов, как правило, пастельных тонов. В случае наружной прокладки используется светостойкий полиэтилен (черного цвета). Все кабели маркируются по оболочке примерно следующим образом: фирма-производитель — марка изделия — тип изделия (4x2x0,52 — четырехпарный кабель с диаметром проводника), далее кодируются дата производства (1002 — октябрь 2002) и отметка метровой длины (иногда футы). Кроме того, на кабеле могут быть указаны материал оболочки, система сертификации и т. д.

Драйвер (Driver)

Небольшая компьютерная программа для работы с конкретным периферийным устройством, таким как, например, сетевая плата или принтер.

Интерфейс

См. Interface.

Коаксиальный кабель

Представляет собой два соосных гибких металлических цилиндра, разделенных диэлектриком. Название произошло от латинских: *co* — совместно и *axis* — ось. Применяется для передачи высокочастотных сигналов. Для организации компьютерных сетей используется ограниченно. Кабель на основе витой пары вытесняет коаксиальный кабель в области сетестроения ввиду

большего удобства применения. В отдельных случаях может быть оправдано использование толстого коаксиального кабеля для связи удаленных на расстояние 180 м и более участков сети.

Коммутатор (switch)

Как и концентратор, позволяет объединить несколько компьютеров, подключив их к одному серверу. В отличие от устаревших теперь концентраторов (hub), коммутатор позволяет пересылать пакеты между несколькими сегментами сети, не загружая остальную сеть. Он является обучающимся устройством. Коммутатор анализирует адрес назначения в заголовке пакета и, сверившись с адресной таблицей, тут же (время задержки около 30—40 мкс) направляет этот пакет в соответствующий порт. Таким образом, его заголовок уже передается через выходной порт, хотя пакет еще целиком не прошел через входной.

Компьютерная сеть

Компьютерная сеть — это компьютеры, соединенные между собой средствами передачи информации. Эти средства достаточно разнообразны и применяются для решения возникающих на практике проблем. Их, тем не менее, можно разделить на программные средства, сетевое оборудование и кабельные системы.

В простейшем случае все компьютеры подсоединяются к одному и тому же коаксиальному кабелю и, тем самым, оказываются соединенными друг с другом. Но чаще используется более совершенная технология, в которой все компьютеры подсоединяются к специальному устройству, называемому концентратором, а для подключения применяется витая пара. В этом случае на каждом рабочем месте оборудуются розетки для подключения компьютера, а в центре, где будет установлен концентратор, — коммутационная 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. Такой кабель позволяет 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 необходимо только задействовать, из-

менив конфигурацию операционной системы. Для более эффективной реализации работы в сети следует использовать специализированный компьютер — сервер, который применяется только для обеспечения работы в сети. Он отличается от обычных компьютеров тем, что при его проектировании предприняты специальные меры для повышения его надежности, расширяемости и безопасности. И это понятно, т. к. на нем чаще всего размещается жизненно важная для компании информация и от его работоспособности может зависеть работоспособность всей компании. На сервер устанавливаются специальные программные средства, которые в состоянии эффективно обслуживать многочисленные запросы, поступающие с остальных компьютеров сети.

Коннектор

Распространенное название электрических разъемов, применяемых для соединения кабельных коммуникаций с оборудованием. Для соединения компьютеров и сетевого оборудования кабелем 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 — от 4 до 32.

Маршрутизатор (router)

Маршрутизатор распознает адрес получателя и перенаправляет по нему пакет. Для этих целей возможно применение отдельного компьютера с несколькими сетевыми адаптерами. Маршрутизатор можно применять для связи различных сетей. Внутри одной сети применяются коммутаторы.

Система, выбирающая один из нескольких путей передачи сетевого трафика. Для выполнения этой задачи используются маршрутизируемые протоколы, содержащие информацию о сети и алгоритмы выбора наилучшего пути на основе нескольких критериев, называемых метрикой маршрутизации (routing metrics). В терминах OSI маршрутизатор является промежуточной системой Сетевого уровня.

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 (HTTP), 21 (FTP) и др. Применение того или иного номера порта обусловлено лишь стандартами и договоренностями, необходимыми для равномерного распределения нагрузки на память компьютера и позволяющими работать максимальному числу процессов в одно время.

Протокол

Правила и язык общения компьютеров сети между собой. Наиболее популярные протоколы: NetBEUI (расширенный NetBIOS), IPX/SPX, TCP/IP. NetBEUI — устаревающий протокол, пригодный для маленькой сети, которая состоит из одного сегмента.

IPX/SPX — протокол для Netware, его поддерживают все версии Netware. У него есть подробности в виде типа кадра Ethernet (тип фрейма). Для того чтобы компьютеры в одной IPX-сети видели друг друга, они все должны работать на одинаковом типе кадра.

TCP/IP — интернет-протокол, ему посвящены целые книги. Сложный протокол, в домашней сети его имеет смысл использовать при наличии систем UNIX, маршрутизатора и/или выхода в Интернет, а также при работе с приложениями, применяющими этот протокол.

"Расшаренный диск"

Очень распространенное жаргонное выражение, ставшее обычным на Web-страницах пользователей и администраторов сетей и означающее диск общего доступа (Shared disk) или область на диске, открытые для доступа другим объектам сети. От английского *share* — разделять. "Шарить диски" — открывать диски для сетевого доступа или подключать чужие диски, предоставленные для доступа.

Сегмент сети

Это часть сети, в которой все компьютеры "видят" друг друга напрямую. Любая сеть состоит, как минимум, из одного сегмента. Сеть, состоящая из нескольких сегментов, имеет в своем составе более сложное сетевое оборудование, как то: маршрутизатор, мост, коммутатор.

Сервер

1. 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.
2. В технологии "клиент-сервер": главная программа, управляющая работой подчиненных программ-клиентов.

Сервер удаленного доступа

Программное средство, обеспечивающее доступ к компьютеру для пользователей, находящихся вне локальной сети.

Сетевая плата

См. сетевой адаптер.

Сетевой адаптер (сетевая карта, сетевая плата)

Устройство внутри компьютера (может быть встроенным в материнскую плату), позволяющее соединить этот компьютер с компьютерной сетью. Обычно применяются адаптеры для кабельных сетей, но могут применяться и беспроводные адаптеры. Выпускаются сетевые адаптеры многими производителями, среди них: 3com, Intel, DEC, AMD, Cabletron и др., но самая 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, например, 1E:34:00:00:FF:12, который называется Ethernet-адрес или MAC-адрес. По этому адресу каждый сетевой адаптер однозначно идентифицируется сервером, что позволяет повысить безопасность сети.

Сетевой кабель

Коаксиальный кабель с волновым сопротивлением 50 Ом или кабель типа "витая пара". В настоящее время коаксиальный кабель применяется реже витой пары. Это связано с тем, что локальная сеть на основе витой пары имеет больше возможностей для расширения и модификации.

Трансивер

Приемник-передатчик. Физическое устройство, которое соединяет интерфейс хоста с локальной сетью, такой как Ethernet. Трансиверы Ethernet содержат электронные устройства, передающие сигнал в кабель и детектирующие коллизии.

Предметный указатель

С

Т

У

Ф

Ш

Э