Александр Поляк-Брагинский

Локальная сеть под Linux

Санкт-Петербург

«БХВ-Петербург»

2010

УДК 681.3.06
ББК 32.973.26-018.2
П54

Поляк-Брагинский А. В.

П54 Локальная сеть под Linux. — СПб.: БХВ-Петербург, 2010. — 240 с.: ил. — (Библиотека ГНУ/Линуксцентра)

ISBN 978-5-9775-0171-2

В практическом руководстве по созданию локальной вычислительной сети под управлением Linux для дома или небольшого офиса рассмотрены вопросы маршрутизации, удаленного администрирования и управления, настройки почтового сервера, совместного использования ресурсов. Описаны программы для удаленного управления и администрирования, веб-интерфейсов для локальной и удаленной настройки компьютеров сети. Даны практические приемы применения виртуальных технологий, позволяющих удешевить сеть, получить максимум функциональности при минимальных затратах, опробовать различные версии операционной системы Linux в сети и использовать выбранный вариант без затрат на оборудование. Для облегчения работы с книгой приведены описания команд, процедур установки и настройки на примерах различных дистрибутивов Linux.

Для опытных пользователей и начинающих системных администраторов

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	*Алексей Семенов*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Виктория Пиотровская*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 26.10.09.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 19,35.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

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

ISBN 978-5-9775-0171-2

Оглавление

Глава 1

Сеть под Linux — с чего начать?

Прежде всего, хорошо бы получить представление о принципах работы компьютерных сетей. Автор надеется, что вы уже имели, пусть и небольшой, но опыт работы в сети под Windows. Сеть под управлением Linux использует те же протоколы и правила. Так же как в сети под Windows, каждый узел сети должен иметь свой IP-адрес, может иметь свое сетевое имя. Здесь мы не будем подробно описывать принципы и правила применения IP-адресов. Эта тема описана во множестве источников, как печатных, так и на веб-страницах. При необходимости вы всегда можете обратиться к этим источникам для пополнения своих знаний. Один из самых универсальных источников теоретических сведений — Википедия. На страницах этого сайта можно найти информацию обо всем. Статьи создаются всеми желающими и знающими материал по теме. Об IP-адресах и протоколах можно прочитать, начав со страницы **http://ru.wikipedia.org/wiki/IP**. Страницы Википедии содержат множество ссылок для получения информации о применяемых терминах и ссылок на смежные по теме статьи. Далее мы не будем останавливаться на подробностях теории применяемых нами технологий. При необходимости будут приводиться ссылки на материалы в Интернете, в том числе и на материалы в Википедии. Если уж вы решили использовать Linux в своей сети, то Интернет у вас должен быть.

Также следует иметь представление о средах передачи данных в сети. Для нас важно знать о сетевых кабелях, представлять, как они подключаются к сетевым адаптерам. Хорошо, если вы сможете самостоятельно готовить кабель, обжимать коннекторы… Информацию о кабельной сети и работе с кабелем можно найти по следующим ссылкам:

- **http://www.orionnsk.net/stat6.html**
- **http://overclockers.ru/articles/lan/**

По второй ссылке можно найти много дополнительной информации, касающейся организации сети.

И последнее, о чем нам желательно иметь представление, — это о режимах работы операционной системы. Два компьютера, соединенные между собой кабелем, — это уже сеть. Если компьютеры оснащены операционными системами, предназначенными для рабочей станции, то сеть обычно получается одноранговой. В этой сети ни один компьютер не имеет видимых преимуществ, и роль каждого компьютера может меняться в зависимости от ситуации. Если один из компьютеров сети предоставляет для других какой-либо сервис, например доступ к файлам, которые находятся на его дисках или доступ к глобальной сети через свое подключение к Интернету, — он становится сервером. Но только до того момента, пока сам не начинает пользоваться сервисами, предоставляемыми другими компьютерами. В этом случае сервер превращается в клиента. Клиент-серверные отношения между машинами существуют в любой сети. Если какой-либо компьютер специально предназначен для предоставления сервисов другим компьютерам сети, его называют выделенным сервером. На выделенных серверах обычно не работают как на рабочих станциях. Выделенных серверов может быть несколько, и каждый из них выполняет определенные для него задачи. В небольшой сети часто все серверные задачи выполняет одна машина. Но в последние годы получили широкое распространение технологии виртуализации компьютеров. Применяя такие технологии, можно даже в совсем небольшой сети иметь несколько специализированных серверов, каждый из которых выполняет свою задачу. При этом физически все они расположены на одной машине. Мы позднее рассмотрим примеры использования таких технологий, а пока каждый компьютер сети, будь то реальный или виртуальный, мы будем рассматривать как самостоятельную машину.

Схема компьютерной сети

Если уж мы решили организовать сеть, следует рассмотреть для начала общую структуру сети и ее варианты, с которыми нам придется столкнуться. Эта галерея схем не претендует на полноту, сеть — дело творческое, и решения могут быть разнообразными. Постепенно вникая в работу своей сети, сравнивая ее с другими известными вариантами, вы начнете чувствовать красоту правильной организации сети. Совсем не обязательно использовать дорогостоящие программные продукты, когда можно найти простое и эффективное решение задачи. В нашей галерее схем представлены несколько основных решений для небольших сетей. Встречающиеся на рисунках IP-адреса приведены только для большей наглядности, и не стоит их воспри-

нимать как рекомендованные. В отдельных случаях, когда IP-адрес должен быть именно таким, как на рисунке, будет соответствующий комментарий. Во всех случаях будем считать, что сеть подключена к Интернету. Современная сеть, даже совсем небольшая, должна иметь выход в глобальную сеть. Если окажется, что в вашем конкретном случае этого не требуется, то можно не рассматривать это подключение, как необходимую часть. Сеть будет работать и без выхода в Интернет. Но в какой-то момент вам придется столкнуться с такой необходимостью, и случится это быстрее, чем вы сейчас думаете.

Сеть из двух компьютеров

Это самый простой вариант сети (рис. 1.1). Всего два компьютера объединены в сеть. Выход в Интернет обеспечивается одним из компьютеров, который подключен к модему или выделенной линии. Вариантов подключения может быть несколько, и мы их рассмотрим применительно к разным вариантам сети. Для соединения компьютеров можно применить перекрестный кабель, но мы сразу предполагаем расширение сети в будущем. Это условие требует стандартного включения компьютеров в сеть через концентратор или коммутатор. Начиная с этой простейшей схемы, мы будем применять коммутаторы.

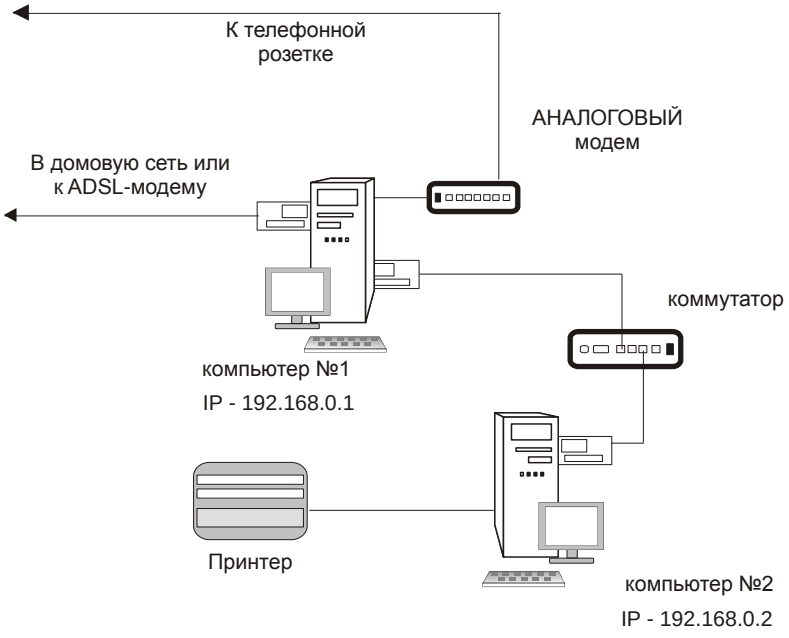


Рис. 1.1. Простейшая сеть из двух компьютеров

Несмотря на простоту, даже эта сеть требует некоторого внимания и первичной настройки. Как и в больших сетях, компьютеры этой сети должны иметь свои IP-адреса. Выбор адреса для компьютера, с которого вы начнете настройку сети, может быть в большой степени произвольным. Но существующих ограничений на применение IP-адресов в локальных сетях лучше придерживаться сразу. Это избавит нас от необходимости делать глобальные изменения в адресной политике, когда сеть вырастет. В очень больших локальных сетях часто используются адреса из зарезервированного диапазона для сетей класса A, начинающиеся на 10. Так называемые адреса самонастройки, которые компьютеры себе назначают сами, когда недоступны другие средства назначения адресов, находятся среди зарезервированных адресов в классе B. Эти адреса начинаются на 169.254. В том же классе есть еще один диапазон зарезервированных адресов, который может применяться в локальных сетях (172.16.0.0—172.31.255.255). В классе C также зарезервирован диапазон адресов для малых локальных сетей (192.168.0.0—192.168.255.255). Все перечисленные диапазоны адресов можно описать как 192.168.0.0/16, 172.16.0.0/12 и 10.0.0.0/8. И, наконец, диапазон зарезервированных адресов из класса A, начинающийся на 127, вообще не применяется в сетях, а используется для внутреннего локального адреса компьютера. По этим адресам можно установить связь компьютера с самим собой.

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

Одинаковые компьютеры под управлением выбранной вами ОС, объединенные в сеть, образуют *одноранговую* сеть. У нас нет сервера, и все компьютеры в такой сети равны. Но тот факт, что один из компьютеров должен обеспечить выход в Интернет, уже нарушает равноправие. Компьютер становится *шлюзом* в Интернет для всей сети. Часто, но не обязательно, шлюзу присваивают адрес 192.168.0.1. Кроме компьютеров в нашей сети есть и другие устройства: принтер, модем. Они используются всеми клиентами сети. Значительно удобнее послать на печать подготовленный документ или вебстраницу по сети, чем переписывать ее на дискету и нести на другой компьютер. На рисунке показаны сразу два подключения к Интернету. Одно посредством обычного аналогового модема, а другое через выделенную линию, или ADSL-модем. Так может быть и на самом деле. Во всяком случае, у меня дома именно так и сделано. Всякое может случиться: то профилактические работы у поставщика услуги подключения к Интернету, то забыли оплатить вовремя эти услуги. Если есть такая возможность, лучше подстраховаться, особенно когда подключение требуется постоянно.

Добавляем маршрутизатор

Возможны различные варианты построения сети из двух компьютеров. Посмотрите на рис. 1.2. На первый взгляд почти ничего не изменилось, но у компьютера №1 поменялся IP-адрес, исключен один сетевой адаптер, вместо коммутатора установлен маршрутизатор. Сейчас в продаже появилось достаточно много недорогого сетевого оборудования для домашних и офисных сетей. И этим можно воспользоваться, выбирая наиболее оптимальный вариант своей сети.

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

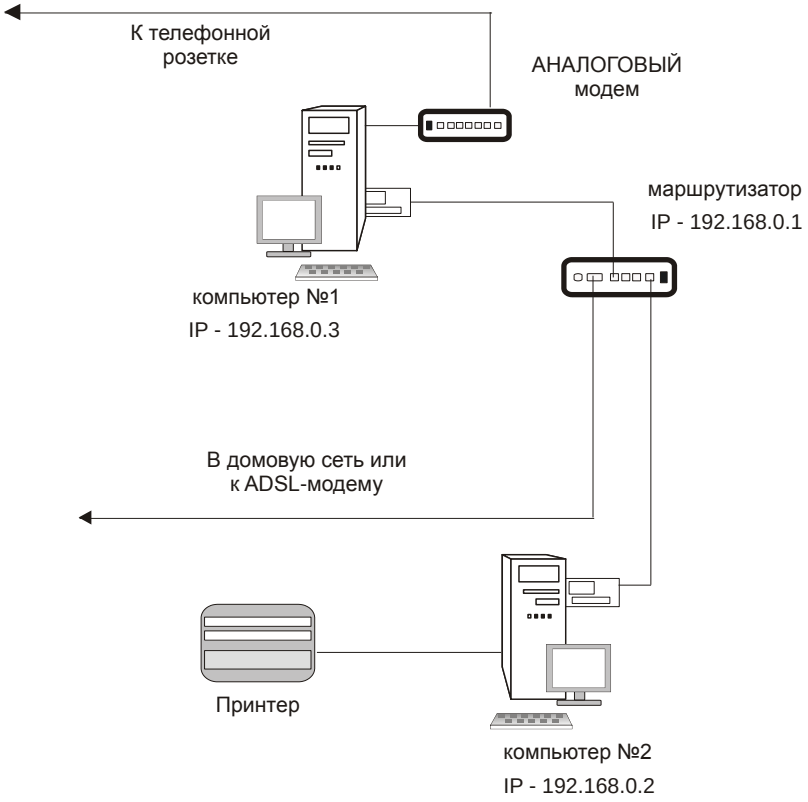


Рис. 1.2. Модифицированная сеть из двух компьютеров

Добавляем коммутатор

Можно пойти еще дальше. На рис. 1.3 показана схема сети, в которой есть и маршрутизатор и коммутатор. Зачем? Дело в том, что среди маршрутизаторов есть такие, у которых только один Ethernet-порт. Для того чтобы подключить к ним несколько компьютеров, необходим и коммутатор.

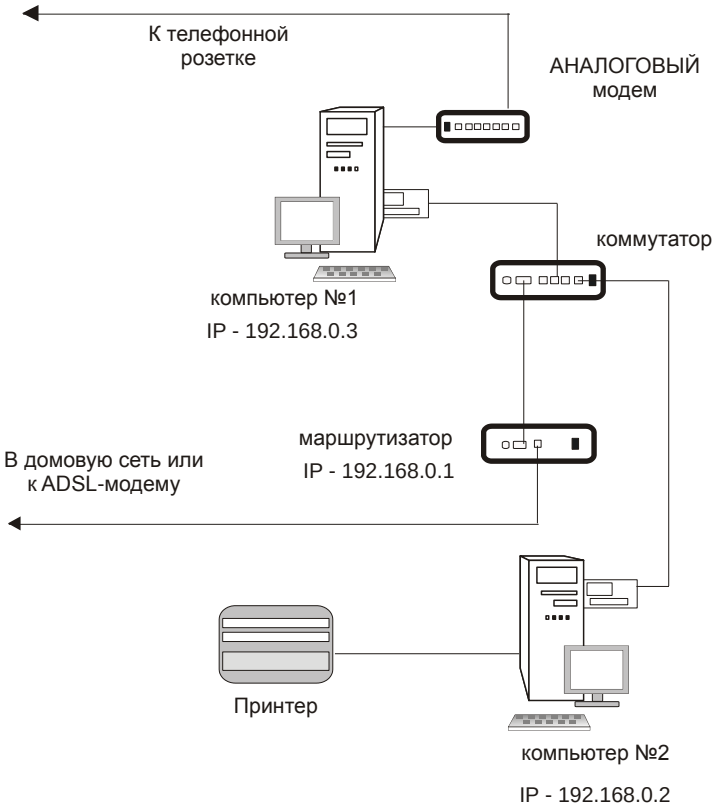


Рис. 1.3. Сеть из двух компьютеров с маршрутизатором и коммутатором

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

Сеть с сервером

Компьютерные сети не ограничиваются одноранговыми. Большинство локальных сетей имеют не только рабочие станции, но и серверы. Серверов может быть один, два и более, в зависимости от задач, решаемых в сети. Давайте посмотрим на варианты построения простой сети с сервером (рис. 1.4).

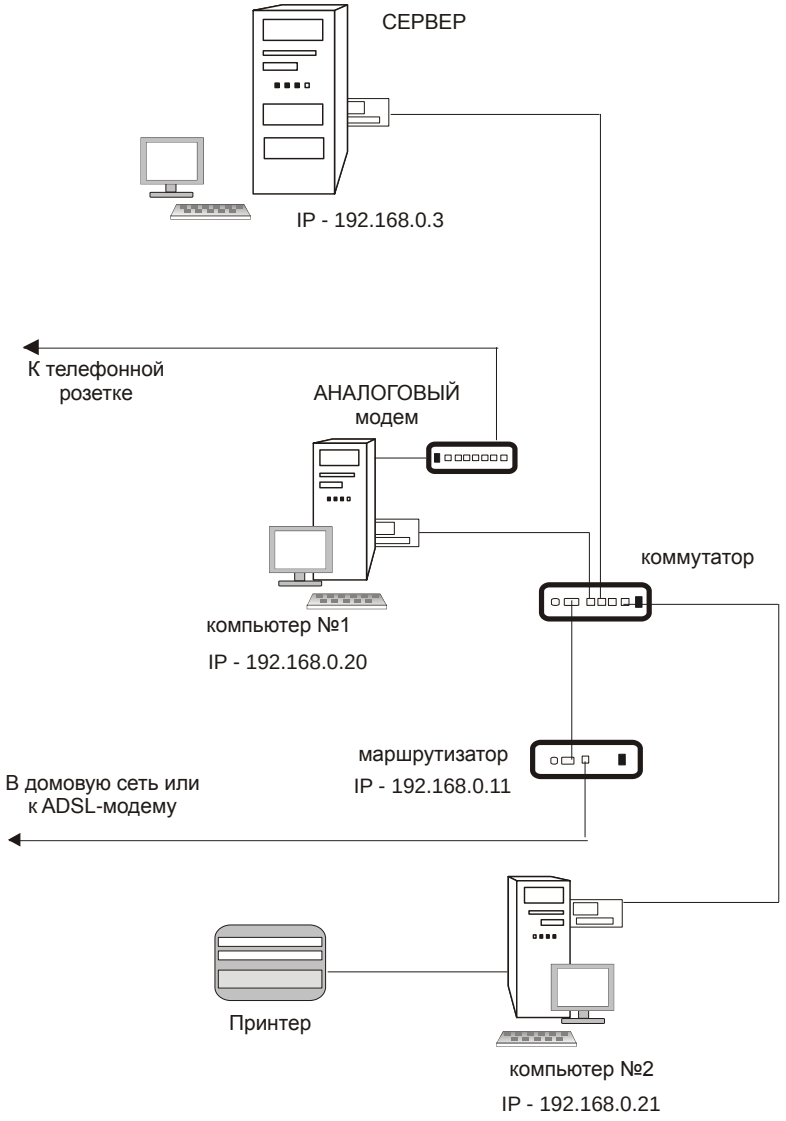


Рис. 1.4. Сеть с сервером

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

Интернет для сети через сервер

Возможен и вариант подключения сети к Интернету без применения маршрутизатора. Такой вариант показан на рис. 1.5.

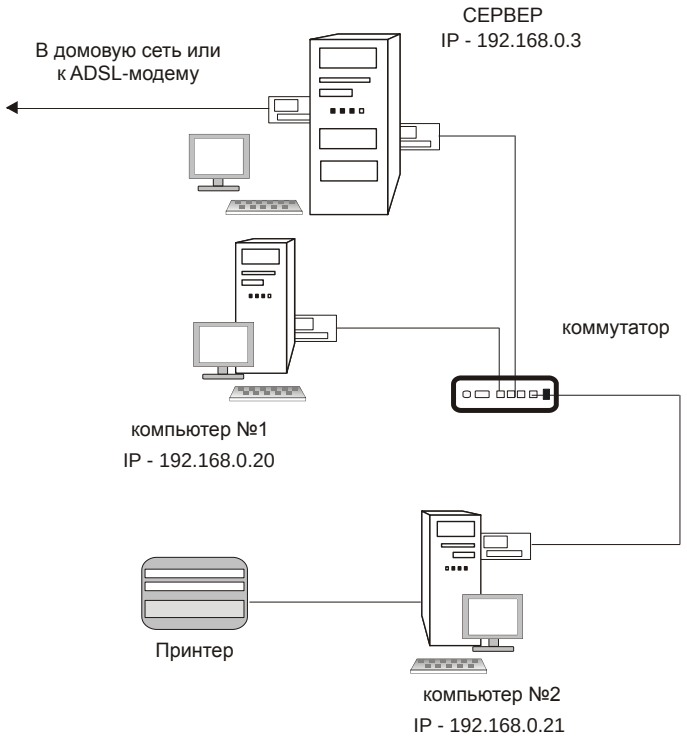


Рис. 1.5. Сеть с сервером, подключенным к Интернету

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

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

Объединение сетей

Иногда наступает необходимость установить связь между двумя локальными сетями. Причины, которыми вызвана такая необходимость, могут быть разными. Это и доступ к данным удаленных сотрудников, и сетевые игры с соседями по дому, и необходимость передачи информации от автоматизированных систем, и удаленное администрирование нескольких сетей… Да, не удивляйтесь. Начали мы рассмотрение вариантов построения сетей с двух компьютеров, но вполне возможно, что вам придется заняться организацией, пусть даже простых, но нескольких сетей. При этом администрирование этих сетей будет осложнено необходимостью вашего присутствия сразу в двух или более местах. Но это, как вы понимаете, невозможно. Поэтому рассмотрим последний в этой главе пример, иллюстрирующий связь двух удаленных сетей. Таких вариантов, как и вариантов самих сетей, может быть множество. Один из них показан на рис. 1.6. Две локальных сети, имеющих выход в Интернет, соединены защищенным каналом VPN (Virtual Private Network — виртуальная частная сеть). Установлена связь между компьютером администратора, находящимся в сети №1, и сервером сети №2. Реально канал связи, конечно, проходит в Интернете, но для пользователей и компьютеров этот канал выглядит так, как будто проложен отдельный кабель. Никакой связи между данным каналом и Интернетом нет. Это значит, что канал защищен со стороны Интернета, а связь через него абсолютно безопасна. Пока нам не важно, как это достигается. Мы рассмотрели лишь основные примерные схемы локальных сетей, опираясь на которые, комбинируя, расширяя, можно строить свою сеть.

Сама по себе сеть не связана с какой-либо определенной операционной системой. Когда-то были распространены сети с серверами Novell NetWare, в которых могли работать рабочие станции под управлением DOS различных

версий, а затем и Windows, теперь в этих сетях там, где они сохранились, могут работать и рабочие станции под управлением Linux. Там где это было возможно, администраторы переводили свои сети на работу с другими серверами.

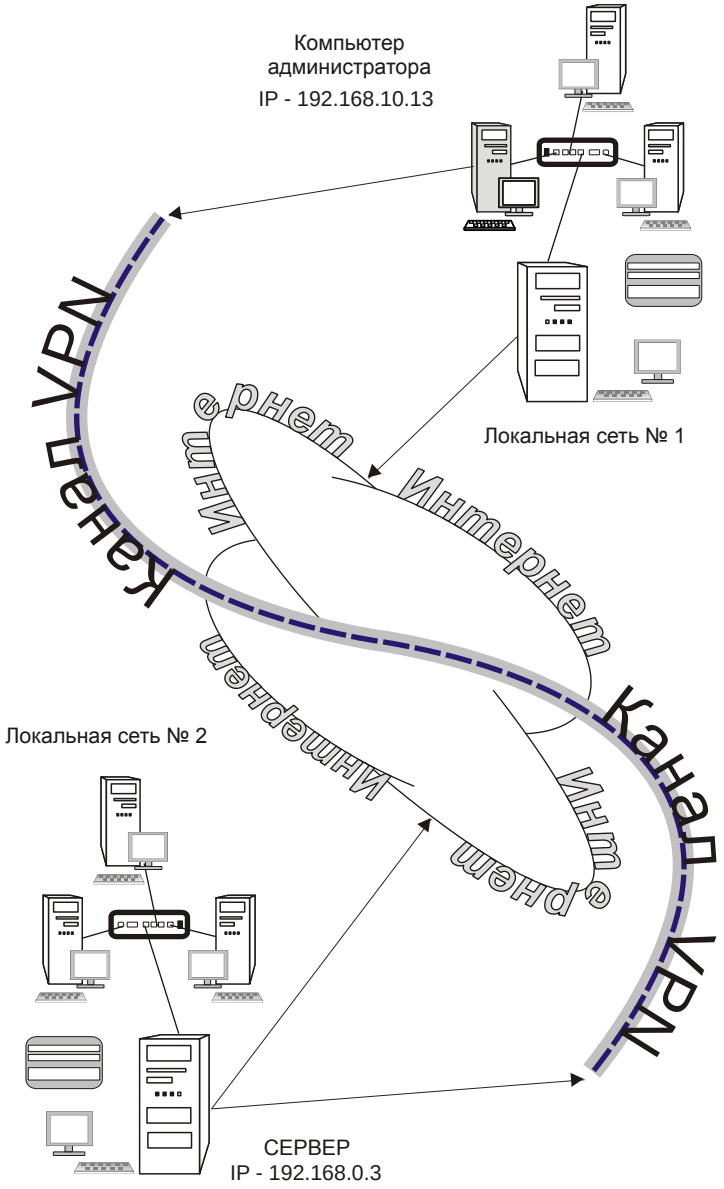


Рис. 1.6. Связь двух сетей через Интернет

Время идет, многие разработчики сетевых программ перестали поддерживать работу с сервером Novell NetWare. Все большее распространение получали серверные версии Windows. В локальных сетях серверы Windows 2000 Server, Windows Server 2003, Windows Server 2008 сейчас имеют очень широкое распространение. А мы с вами задались целью строить сеть на основе Linux и будем рассматривать возможности именно этих операционных систем. Интересно, что и фирма Novell обратила свое внимание на Linux. Именно в дистрибутивах Linux, разработанных этой фирмой, есть встроенная поддержка технологий сетей NetWare. Разработаны фирмой и специализированные серверные версии Linux, и версии для рабочих станций. Это коммерческие проекты. Получить такие дистрибутивы может каждый желающий, но получить поддержку и неограниченное время обновлений можно, заплатив некоторую сумму. Выпускаются и совершенно свободные версии дистрибутивов, такие как OpenSUSE. В этих дистрибутивах содержатся как компоненты для рабочей станции, так и для сервера. Обновления для них бесплатны. Если не ставить перед собой задачу поддержки технологий Novell в своей сети, то можно использовать и дистрибутивы других разработчиков.

Идеология Linux

Мы не будем обсуждать политическую или этическую сторону этого вопроса. Нам необходимо всего лишь решить конкретную задачу построения сети на основе Linux. Но для понимания работы сети следует понять суть работы операционной системы, которая будет работать в сети. Именно об этом сейчас и поговорим.

Операционная система Linux в состоянии работать с любым оборудованием для персональных компьютеров и с любыми файловыми системами. Например, вы всегда имеете возможность прочитать информацию с дисков, которые были созданы операционной системой Windows, а в ряде случаев и записать на них информацию. Linux поддерживает все известные сетевые протоколы. Отдельные проблемы при установке Linux могут возникнуть только на совершенно новом оборудовании, поддержку которого не могли включить в дистрибутив, имеющийся у вас. Достаточно взять новый дистрибутив, и все проблемы будут решены.

Изначально идея Linux состояла в том, чтобы каждый мог применить ее в своих конкретных условиях и настроить под эти условия оптимальным образом, получив удобный и надежный инструмент для выполнения своих задач. Универсальность системы настолько высока, что применяется она и для управления устройствами, выполняющими специальные задачи, например маршрутизаторами, и для обеспечения взаимодействия пользователя с компактными мобильными устройствами, такими как сотовые телефоны, и для

управления рабочими станциями и серверами, работающими в сетях любого масштаба. Обеспечила такую универсальность и гибкость системы изначально заложенная в нее идеология. Система должна быть многозадачной, многопользовательской, масштабируемой, платформонезависимой и свободной. Последнее позволило внести свой вклад в реализацию идеи тысячам талантливых программистов. В результате получилась ОС, состоящая из шести базовых элементов. Независимо от того, какой конкретный дистрибутив системы вы держите в руках, эти элементы в нем присутствуют.

Ядро и модули

Ядро системы представляет собой программу, которая может быть запущена под управлением BIOS компьютера, и выполняет следующие функции:

- распределение процессорного времени между различными одновременно работающими задачами;
- работа с памятью, как физической, то есть установленной в машине, так и ее образом на жестком диске — так называемым пространством своппинга (swapping), которые в сумме составляют единую виртуальную память;
- обращение к носителям информации, таким как жесткие диски, CD/DVD, USB-накопители и др.;
- управление видеоподсистемой компьютера, звуковыми картами, принтерами и сканерами, другим оборудованием;
- доступ к данным, организованным в виде различных файловых систем на дисках и дисковых разделах;
- поддержка сетевых устройств и сетевых протоколов;
- управление вводом и выводом данных — обменом информацией между всеми устройствами машины.

Часть функций обеспечивается самим ядром, а часть доверяется подгружаемым дополнительно модулям. Если на вашей машине никогда не появится диск с файловой системой NTFS, то зачем ядру поддерживать возможность работы с ним и при этом бесполезно занимать оперативную память компьютера? Ядро всегда полностью загружено в оперативную память, а модули при необходимости могут быть загружены и выгружены из памяти.

Загрузчик

Загрузка ядра Linux возможна и без него. Но в целях рационального использования дискового пространства, возможности загрузки других операционных систем, установленных на компьютере, разработаны специализирован-

ные программы — загрузчики. Для персональных компьютеров сейчас применяют загрузчики Grub и Lilo. Первый, наверное, чаще, но оба обычно входят во все дистрибутивы Linux, и вы вправе использовать тот, который больше понравится.

Утилиты инициализации

После загрузки ядра начинается процесс инициализации. Происходит монтирование файловых систем, включение разделов своппинга, активизация виртуальных терминалов и другие действия, участие пользователя в которых не требуется. Завершается инициализация приглашением пользователя к авторизации. Для осуществления этого процесса используются специальные программные инструменты, запускаемые еще на стадии входа в систему.

Программы управления устройствами

Файловые системы, сетевые протоколы, виртуальные терминалы, принтеры, сканеры, клавиатура, мышь, другие устройства, кроме поддержки ядром, требуют внешнего инструментария для управления. Иначе пользователь так и не узнает, что ядро поддерживает работу с множеством устройств, и система будет для него бесполезной. Для взаимодействия пользователя с устройствами системы созданы специальные программы, к которым пользователь обращается посредством других прикладных программ или сценариев.

Оболочка

Это командный интерпретатор (когда-то с подобной программы для первого персонального компьютера начал Билл Гейтс). Синонимы этой программы в Linux — командная оболочка или просто шелл (shell — оболочка). Она выступает в качестве интегратора вышеуказанных пользовательских утилит и прикладных программ пользователя. Без оболочки пользователю было бы непросто получить доступ к устройствам и программам. В Linux применяется несколько оболочек. Даже разные пользователи одной системы могут использовать оболочки, необходимые именно им.

Общесистемная библиотека

Можно встретить название главная общесистемная библиотека (libc). Ряд функций, которые используются прикладными и системными программами, требуется выполнять очень часто. Эти функции содержатся в виде участков программного кода в этой библиотеке. Нет смысла в код каждой программы

включать одну и ту же функцию. Все программы используют стандартные функции из системной библиотеки. Такой подход к программированию сокращает как затраты труда программиста, так и объем кода программ. Программы, использующие графический интерфейс в Linux, — нередко только надстройки над программами оболочки, которые, в свою очередь, используют функции из системных библиотек.

Все элементы системы доступны в исходных кодах. Это значит, что при желании и достаточных знаниях вы можете на основе существующей системы создать собственную версию ядра, загрузчика, утилит и библиотек. Что и делают иногда продвинутые пользователи. Они включают в ядро только им необходимые функции, используют только им необходимые программы и утилиты, получая компактную и в высшей мере персонализированную систему. Но это, конечно, для настоящих энтузиастов — настоящих хакеров. А мы приступим к знакомству с конкретными версиями дистрибутивов Linux. Вариантов множество, но какой из них выбрать?

Какую версию Linux применить?

На сегодняшний день существуют более 150 дистрибутивов Linux! Не полный их перечень можно увидеть на сайте **http://www.distromania.com**. Конечно, выбрать дистрибутив из такого списка не просто. Мы ограничимся рассмотрением лишь небольшой части из всего разнообразия дистрибутивов, с которыми пришлось иметь дело автору. Критерии выбора в нашем случае могут быть основаны на следующих требованиях:

- простота установки;
- поддержка нашего оборудования;
- наличие необходимых на рабочей станции программ;
- возможность работы в качестве сервера с необходимыми функциями;
- простота установки дополнительных программ и возможность найти эти программы в Интернете;
- удобство графического интерфейса;
- возможность запуска хотя бы некоторых Windows-программ;
- распространенность дистрибутива и возможность найти ответы на возникающие в процессе работы с ним вопросы в Интернете;
- возможность получить дистрибутив с минимальными финансовыми затратами.

Создание сети предполагает, что в ней будут рабочие станции и серверы (по крайней мере, по одной машине). Поэтому рассмотрение дистрибутивов мы поведем в два этапа. На первом этапе рассмотрим дистрибутивы для рабочей станции, а на втором — для сервера. Деление, правда, довольно условно. Обычно в каждом дистрибутиве содержатся программы для сервера и для рабочей станции. Но иногда сделан уклон в ту или иную сторону. При желании вы можете остановиться на каком-либо одном дистрибутиве и использовать его на всех ваших компьютерах. Обычно серверная установка отличается от установки для рабочей станции некоторой аскетичностью. Зачем, например, серверу звуковая карта или особые эффекты рабочего стола? Кроме того, если сервер предназначен для выполнения важных внутрисетевых задач, ему не дают доступ в Интернет. Береженого Бог бережет. Чем тратить нервы и силы на защиту от проникновения внешних врагов системы, лучше просто закрыть границу, на которой отдельное устройство или компьютер стоит на страже безопасности сети. Причем применение виртуальных технологий позволяет выполнять это правило даже при отсутствии дополнительного физического компьютера, чтобы организовать защищенный сервер. Но о виртуальных технологиях мы поговорим позднее, а сейчас рассмотрим несколько дистрибутивов Linux.

Linux для рабочей станции

Рабочая станция должна быть укомплектована пакетом программ, которые требуются для повседневной работы. Конечно, будь то работа или развлечение, стандарта здесь нет. Тем не менее, по опыту работы с Windows, можно сделать вывод, что на большинстве рабочих мест используется офисный пакет, средства для работы с электронной почтой, средства для обмена мгновенными сообщениями, веб-браузер, проигрыватель видео- и аудиофайлов, графический редактор. Далее может быть перечень специальных программ, связанных с конкретной деятельностью офиса или отдельного человека. Не все программы, к которым привыкли пользователи Windows, могут работать в ОС Linux. Часть таких программ может быть запущена под управлением эмуляторов Windows, а когда в среде Linux нет возможности использовать крайне необходимую Windows программу, на помощь может прийти виртуальная машина или работа в терминальном режиме. Практически все дистрибутивы Linux имеют в своем составе набор повседневно необходимых стандартных программ. Многие современные версии Linux имеют встроенные средства виртуализации, что позволяет устанавливать другие операционные системы, используя их как дополнительные, причем без перезагрузки и выхода из основной ОС. Возможность работы со специализированными программами и запуска игр следует рассматривать индивидуально в каждом случае.

Большинство существующих дистрибутивов распространяются свободно. Если в составе дистрибутива применяются коммерческие драйверы, которые расширяют возможности аппаратуры, или коммерческие программы, то распространение осуществляется на платной основе. Тем не менее, обычно не устанавливается ограничений на число установленных копий и на число компьютеров, где эти копии могут быть установлены. Некоторые версии ОС Linux распространяются только на платной основе. Например, Linux XP можно бесплатно использовать в течение испытательного периода, а затем необходимо приобрести ключ активации и активировать систему через Интернет. Прочитать о Linux XP можно на сайте разработчиков **http://www.linux-xp.ru/**. Есть версии Linux, разработчики которых пытаются привести файловую систему в Windows-подобный вид. Такая попытка сделана и в Linux XP, и в свободно распространяемом дистрибутиве GoboLinux **http://www.gobolinux.org**. Файловая система GoboLinux устроена таким образом, что для просмотра установленных программ не требуется менеджер пакетов, поскольку для каждой программы и даже ее версии определяется отдельная папка. Эта версия Linux распространяется в виде образа Live CD, с которого можно загрузить систему, не устанавливая на жесткий диск, а впоследствии при желании или необходимости установить. GoboLinux не имеет русификации интерфейса и не содержит средств автоматизации подготовки жесткого дика. Рассматриваемые далее версии Linux по мнению автора в наибольшей степени подходят для применения в малых сетях. При установке и настройке они требуют внимания, но даже начинающий пользователь Linux в состоянии справиться с этими процедурами. Несмотря на очень серьезный подход разработчиков к упрощению процедуры установки и настройки системы, не отчаивайтесь, если для достижения оптимального результата установки придется переустановить систему один-два раза. То, что для опытного пользователя Linux является само собой разумеющимся, может вызвать трудности у начинающего, но опыт и терпение сделают свое дело.

В Linux при установке можно выбрать вариант рабочего стола, который будет использоваться по умолчанию. В отличие от Windows здесь есть довольно широкий выбор. С каждым вариантом рабочего стола может устанавливаться соответствующий набор программ и утилит. Иногда трудно сделать окончательный выбор, с каким рабочим столом эксплуатировать систему. Но есть возможность установить не один, а два и более варианта рабочего стола. Это позволит при необходимости использовать тот или иной вариант. Утилиты, поставляемые с каким-либо рабочим столом, могут быть использованы и с другими рабочими столами, установленными в системе. Более подробно об установке системы мы поговорим в следующей главе, а сейчас посмотрим на примеры уже установленных версий Linux.

Mandriva

Одна из быстро развивающихся версий Linux — Mandriva (**http://www.mandriva.com**). Интерфейс системы в варианте по умолчанию рассчитан на обычного пользователя, не имеющего глубоких познаний в Linux. Уже с момента установки системы вы можете просто соглашаться с предложениями мастера установки. Пожалуй, единственное, что потребуется выбрать осознано — это язык системы. Если вы устанавливаете Linux впервые и хотите познакомиться с новой для вас системой, этот дистрибутив может быть хорошим выбором. Существуют свободные и коммерческие версии дистрибутива. Для ознакомления с Mandriva свободный дистрибутив можно загрузить с сайта разработчиков. Для приобретения доступен вариант системы, уже установленной на флэш-накопитель. Если компьютер может быть загружен с USB-диска, то этот вариант может быть интересен для отдельных пользователей.

Дистрибутивы системы могут быть загружены с сайта **http://fr.rpmfind.net/linux/Mandrake-iso**, а дополнительные пакеты можно найти на FTP-сервере **ftp://ftp.free.fr/mirrors/ftp.mandriva.com**.

Здесь приведен пример установленной версии дистрибутива Mandriva 2009 Free.

Интерфейсы новых версий операционных систем могут отличаться довольно существенно, поскольку могут отличаться настройки по умолчанию, применяемые разработчиками дистрибутива. Тем не менее, интерфейс пользователя любой версии Linux может быть настроен под себя. В любом случае будут отличия экранов приветствия, если используется графический способ входа.

На экране приветствия (рис. 1.7) вы можете выбрать вариант рабочего стола, наиболее подходящий вам по вашему вкусу и выполняемым задачам. В данном примере доступ к меню выбора рабочего стола выполняется с помощью значка редактора меню в окне приветствия. Меню выбора рабочего стола может иметь другой вид, доступ к этому меню может быть в другом месте экрана, но оно всегда есть. Рабочий стол по умолчанию может быть выбран как во время установки системы, так и после установки.

На рис. 1.8 приведен вид рабочего стола Xfce. Несмотря на то, что наиболее популярны рабочие столы KDE и GNOME, Xfce может быть очень хорошим выбором для ноутбуков, когда следует экономить ресурсы системы и сохранить большую часть удобств графического интерфейса. Да и на рабочей станции этот рабочий стол может показаться удобнее тем пользователям, которые не любят излишеств в оформлении.

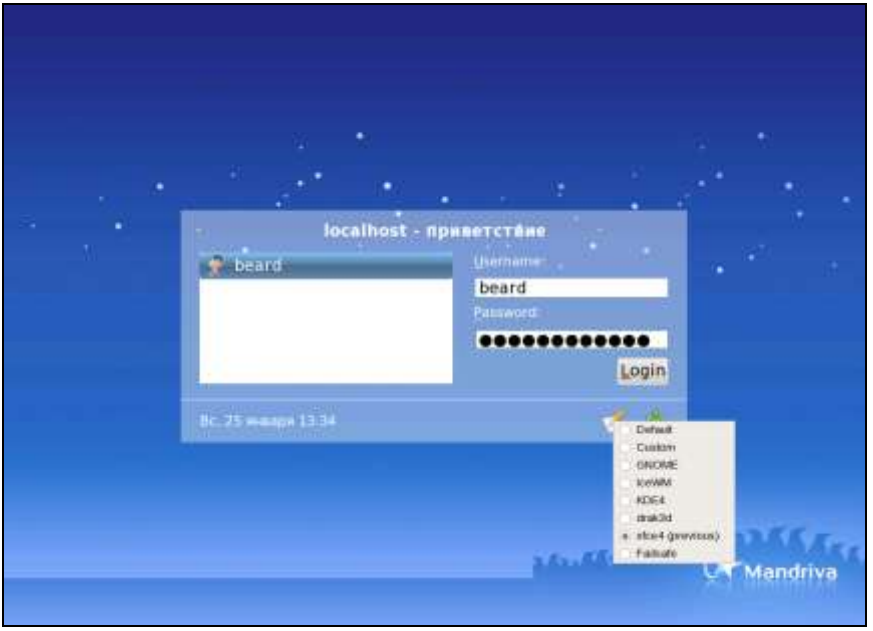


Рис. 1.7. Экран приветствия в Mandriva 2009

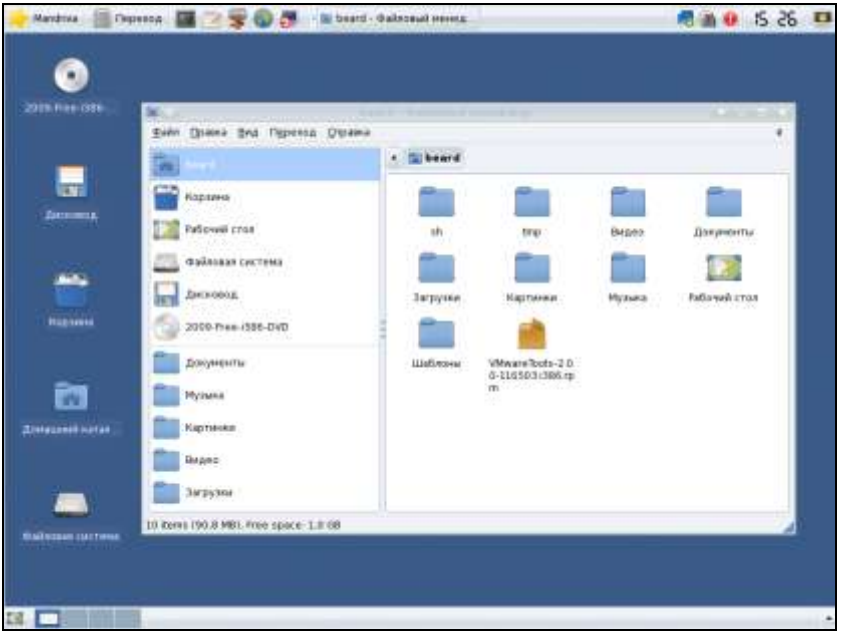


Рис. 1.8. Рабочий стол Xfce с открытым окном файлового менеджера

В верхней части рабочего стола находится панель задач с кнопками доступа к различным меню и программам. В данном случае на панели расположены следующие кнопки:

- **Mandriva** — аналог кнопки **Пуск** в Windows;
- **Переход** — кнопка выбора каталога для перехода;
- кнопка вызова окна терминала — важнейшего средства для выполнения процедур администрирования рабочей станции, а часто и очень удобного средства для работы с программами, выполнения часто встречающихся задач;
- кнопка вызова текстового редактора;
- кнопка вызова файлового менеджера;
- кнопка запуска браузера Firefox;
- кнопка вызова Центра управления (Mandriva Control Center) — аналог панели управления Windows;
- в центральной части панели появляются кнопки открытых окон.

Далее в правой части панели находится системный лоток (Tray), в котором размещены значки для доступа к Сетевому центру, системе поиска, обновлению системы, часы и кнопка блокировки экрана.

В нижней части экрана еще одна панель. На ней кнопка "Свернуть все окна" и переключатель рабочих столов… Нет, это не средство для переключения вида рабочего стола. В Linux без применения дополнительных программ можно использовать несколько рабочих мест. Окна, открытые на одном рабочем месте, не будут видны на других. Использование отдельных рабочих мест для выполнения различных задач позволяет более рационально располагать открытые окна и оперативно переходить с одного удобно организованного рабочего стола на другой. Сама эта возможность была перенесена в графический интерфейс Linux из терминального режима, когда основная работа происходит в командной строке. Даже в этом случае Linux позволяет открыть несколько консолей для выполнения отдельных задач и переключаться между ними. Число рабочих мест можно изменять.

Конечно, Xfce не позволяет применить различные эффекты, такие как объемный рабочий стол, прозрачные окна и другие. Этих эффектов для KDE и GNOME больше, чем для Windows, и вы сами можете поэкспериментировать с ними, если позволяют возможности видеокарты.

Есть еще более аскетичные варианты рабочего стола. IceWM, например, имеет лишь несколько кнопок на панели задач и возможность вызова главного меню щелчком мыши на самом рабочем столе. На рабочем столе нет воз-

можности создавать файлы или помещать значки запуска программ. Интересно, что в последних версиях популярных интерфейсов разработчики снова обращаются к идее чистого поля рабочего стола, давая возможность отобразить на нем какую-либо папку, где могут находиться файлы и значки.

Самый аскетичный интерфейс рабочего стола — Twm (может быть не включен для установки по умолчанию). На этом рабочем столе можно нажатием кнопки мыши вызвать меню, а затем показать место размещения окна выбранной программы. Кнопок нет никаких.

Debian

Эта операционная система не имеет коммерческих версий. Она абсолютно свободно распространяется, и техническая поддержка возможна только на форумах. Дистрибутив системы можно получить на сайте **http://www.debian.org**.

Экран приветствия (рис. 1.9) содержит дополнительные меню в нижней части экрана.

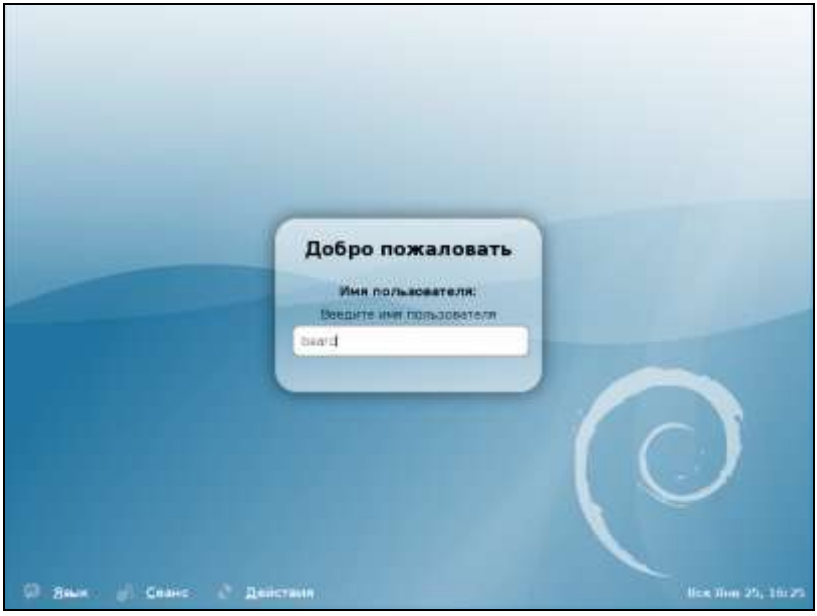


Рис. 1.9. Экран приветствия Debian Linux

Рабочий стол GNOME, показанный на рис. 1.10, по функциональности напоминает рассмотренный ранее Xfce. Но возможностей у него больше, больше дополнительных приложений и утилит.

Рис. 1.10. Рабочий стол GNOME и открытое окно веб-браузера Epiphany

Примечание

Обратите внимание, что дополнительные возможности связаны с применением рабочего стола GNOME, а не дистрибутива Debian. В большинстве случаев возможности дистрибутивов одинаковы, и в любом из них можно установить любой рабочий стол.

Система Debian, как и другие, основанные на ней, имеет свой способ управления программным обеспечением, отличающийся от используемого в Mandriva, например. Эта особенность не позволит применить в других версиях Linux дистрибутивы, предназначенные для Debian, и наоборот. Для Debian существует множество официальных и неофициальных разработок. Применение только свободно распространяющихся программ с открытым кодом полностью исключает возможность лицензионных недоразумений при использовании этой версии Linux. Тем не менее, для Debian создаются и программы с закрытым кодом, даже коммерческие. Их можно получить у разработчиков этих программ. Например VMware Server, предназначенный для создания виртуальных машин, можно получить на сайте VMware, но он никогда не будет входить в состав дистрибутива Debian.

OpenSUSE

Это свободная разработка фирмы Novell. На бесплатно распространяемых версиях разработчики обкатывают новые идеи, совершенствуя таким образом коммерческие продукты. По адресу в Интернете **http://ru.opensuse.org** можно загрузить образ дистрибутивного диска с OpenSUSE.

В состав системы входит большое число пакетов, предназначенных для реализации весьма специальных задач. Например, есть возможность установить систему с ядром Xen. Это открытая система виртуализации, которая позволяет устанавливать в качестве виртуальных машин другие операционные системы. Для обычного домашнего пользователя эта возможность тоже может пригодиться.

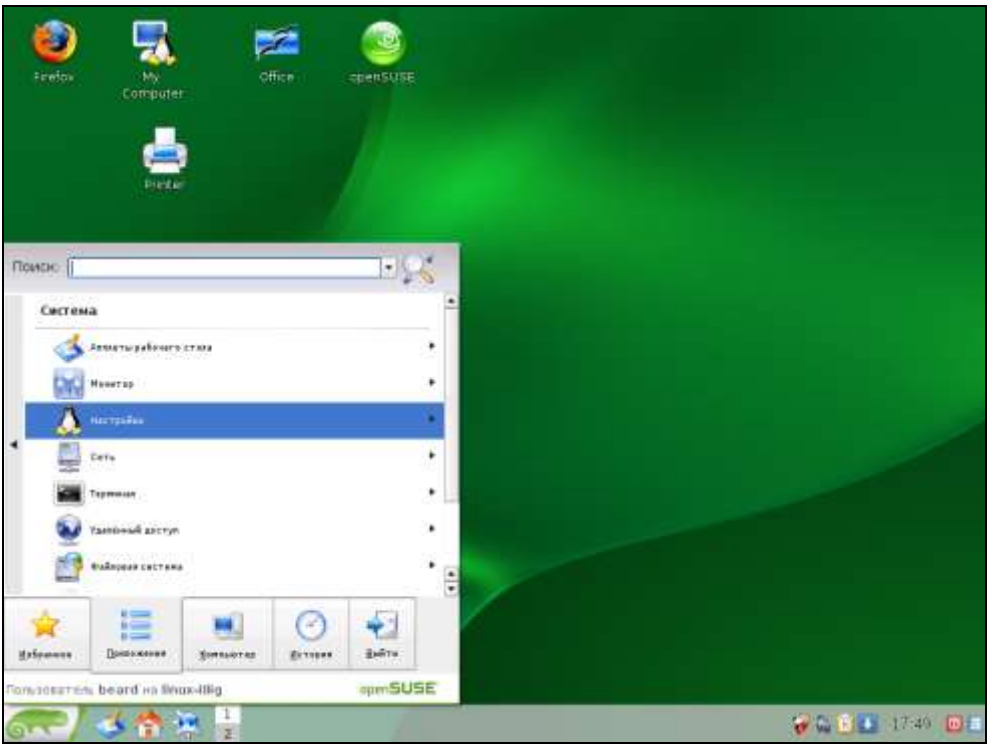


Рис. 1.11. Рабочий стол KDE в OpenSUSE

На рис. 1.11 рабочий стол KDE в OpenSUSE 11.1. Вид главного меню можно переключить на привычный вид, но можно использовать и новый вариант, показанный на рисунке. Вкладки и перелистываемые списки в них делают

меню компактным, и вид его нравится многим пользователям. Рабочий стол KDE имеет те же элементы, что и рассмотренные ранее рабочие столы с развитой графикой. Но в отдельных случаях программное обеспечение разрабатывается с учетом особенностей определенного рабочего стола. Например, в OpenSUSE есть возможность установки официальной версии клиента для сетей Novell NetWare. Корректная установка этой программы оказывается возможна только для рабочего стола KDE. В практике обычного пользователя такие ситуации могут встречаться, но очень редко. Поэтому выбор рабочего стола может быть обусловлен вкусом пользователя и возможностями компьютера. Рабочий стол KDE наиболее требователен к ресурсам компьютера, но вместе с ним устанавливается больше полезных и удобных программ.

Linux для сервера

В условиях малой сети деление версий Linux на серверные и для рабочих станций довольно условно. Любая версия Linux содержит северные компоненты. Дистрибутивы, рекомендуемые для организации серверов, в свою очередь, содержат компоненты, необходимые для рабочей станции. Все же даже в малой сети можно рекомендовать для сервера специализированные дистрибутивы. В эти дистрибутивы по умолчанию не включают такого разнообразия программ, их рабочие столы имеют достаточно скромные возможности оформления. Чем меньше в системе компонентов, тем легче обеспечить высокую стабильность системы.

Одна из таких систем — CentOS.

CentOS

Это свободно распространяемая версия Linux, основанная на исходных кодах Red Hat Linux. Это значит, что не используя специфические программы, созданные для CentOS, можно использовать пакеты для Red Hat и Fedora. CentOS вполне можно применить и на рабочей станции. Но программы для этой ОС придется искать по репозитариям других дистрибутивов (Red Hat, Fedora). Разработчики программ для Linux обычно принимают во внимание существование CentOS и публикуют версии программ для этой системы. Дистрибутив CentOS можно получить на сайте разработчиков **http://www.centos.org**.

На рис. 1.12 изображен рабочий стол KDE в CentOS 5.2. На компьютере, с экрана которого снят этот скриншот, установлены приложения, отсутствующие в стандартной поставке. Это VLC media player, транслирующий видео из Интернета, выше на рабочем столе можно увидеть значок Skype.

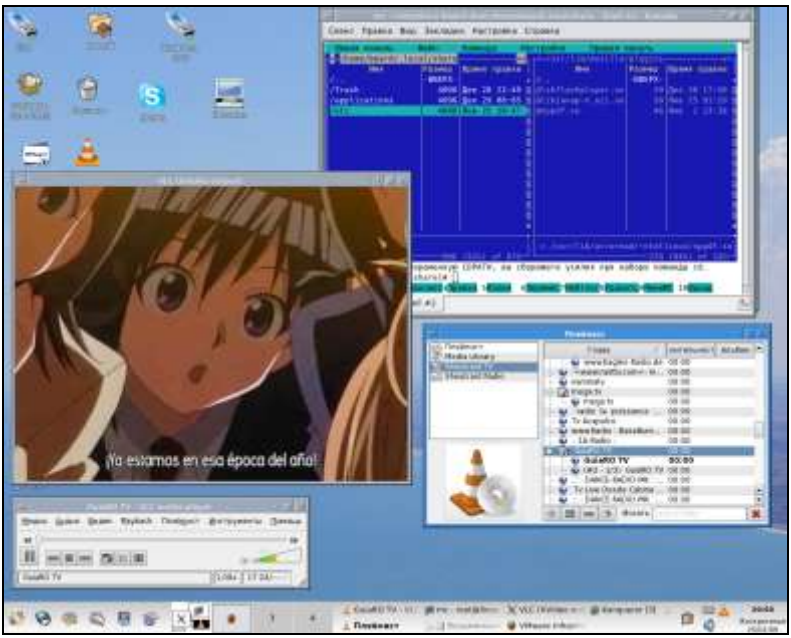


Рис. 1.12. Рабочий стол KDE в CentOS 5.2 (рабочее место 1)

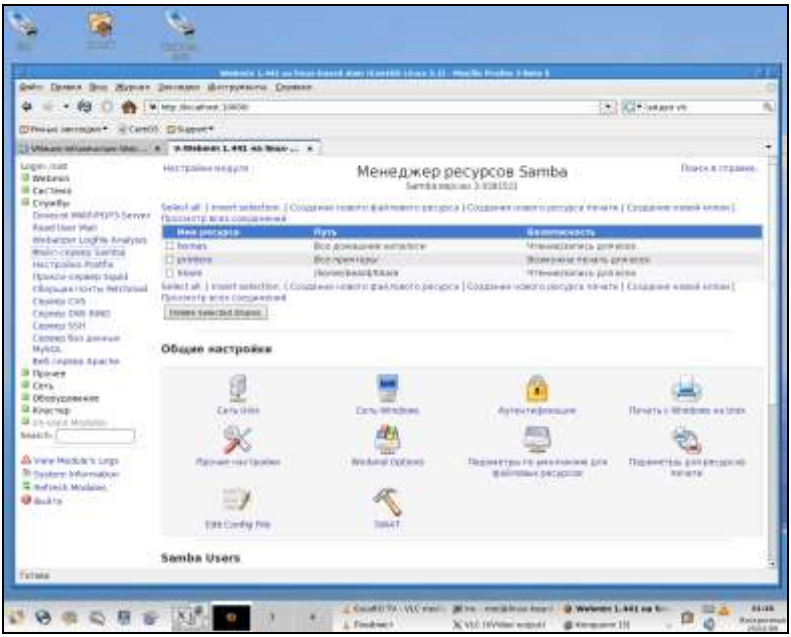


Рис. 1.13. Рабочий стол KDE в CentOS 5.2 (рабочее место 2)

Система, предназначенная для сервера, вполне может работать в качестве рабочей станции. Но все же для сервера важны другие приложения. Практически все важные серверные приложения включены в дистрибутив, а некоторые приложения, облегчающие настройку сервера, можно получить у их разработчиков. На рис. 1.13 приведен экран того же компьютера, но на втором рабочем месте.

Здесь ожидают действий администратора веб-интерфейсы для управления сервером. В больших сетях не принято выполнять на сервере какие-либо действия, не связанные с работой самого сервера. Но если в вашей сети всего два-три компьютера, можно отступить от этого правила — компьютер дома требует отдельного места, стоит не очень дешево, да и потерь при решении проблем с сервером будет не много. Зато эффективность использования такого компьютера в маленькой сети может оказаться очень высокой.

SLES

Эту серверную операционную систему рассмотрим потому, что это коммерческая разработка, которая доступна для бесплатного использования при отсутствии возможности обновлений и поддержки. Точнее, зарегистрировавшись на сайте разработчика, можно получить возможность обновлений на один месяц бесплатно. Если поддержка или обновления потребуются в дальнейшем, то придется заплатить. Во всяком случае, у вас есть возможность попробовать в действии коммерческую серверную версию Linux — SLES (SUSE Linux Enterprise Server). Этот дистрибутив разработан фирмой Novell, и дистрибутив можно получить по адресу **http://www.novell.com**.

В состав дистрибутива входят пакеты, обеспечивающие возможность установки на сервере средств для работы с промышленными приложениями и базами данных (SAP и Oracle), средства для кластеризации серверов. В домашних условиях, конечно, такое вряд ли понадобится. Как и в OpenSUSE, в систему включены средства виртуализации. Для управления всеми функциями системы применяется Центр управления YaST2.

На рис. 1.14 представлен рабочий стол GNOME в SLES 10.0. Как и в новых версиях KDE, главное меню выглядит нестандартно. Для каждой группы задач вызываются окна меню, подобные меню центру управления. Работа с таким интерфейсом удобна, все средства управления работают корректно. Если вы внимательно рассмотрели рисунок, то обратили внимание на отсутствие переключателя рабочих мест. Он в системе есть, как и во всех Linux, но по умолчанию в специализированной серверной системе его решили отключить. На сервере должно быть только одно рабочее место администратора.

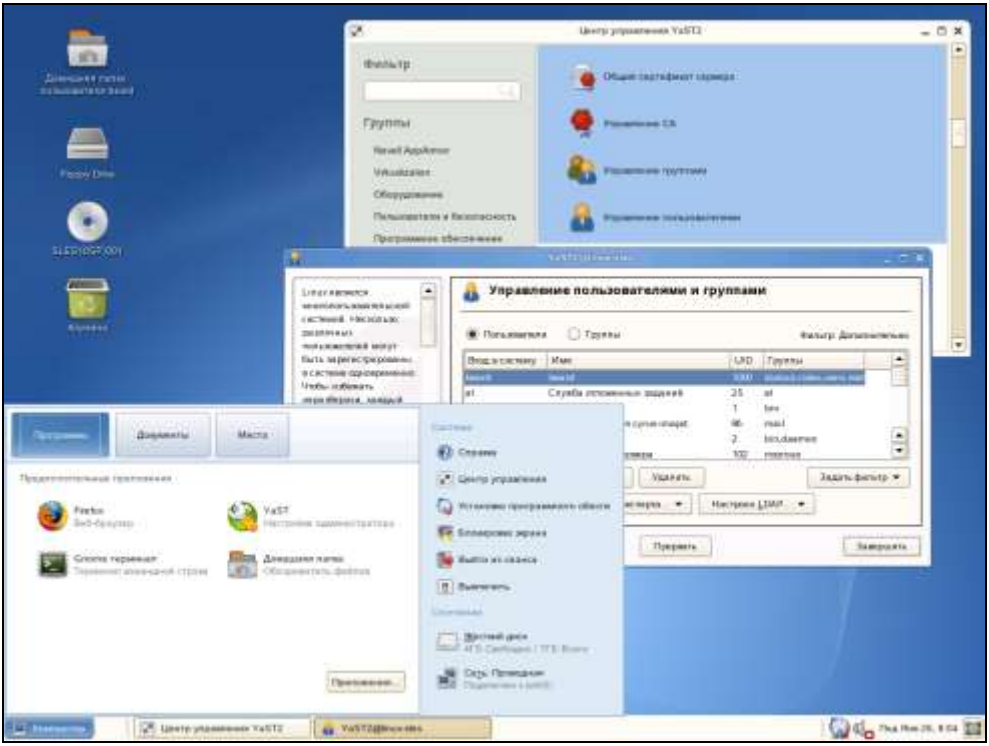


Рис. 1.14. Рабочий стол GNOME в SLES 10.0

На этом обзор вариантов Linux для рабочих станций и серверов можно остановить. Несмотря на различия в интерфейсах и средствах управления, в целом все системы Linux похожи. Главное средство работы с Linux — терминал, который в графическом режиме тоже может выглядеть по-разному, позволяет использовать команды, которые совершенно одинаково работают во всех версиях системы. Конечно, и здесь наблюдается прогресс. Некоторые команды со временем изменяются, добавляются новые, но изучив основной набор команд, вы в любой версии Linux будете чувствовать себя уверенно. Настройка системы сводится к правильному заполнению конфигурационных файлов и выполнению необходимых команд. Знать, какие конфигурационные файлы для какой подсистемы применяются — тоже неплохо. Иногда графический интерфейс системы позволяет выполнить только основные настройки программы, а тонкая настройка возможна через исправление конфигурационных файлов, выполнение команд с различными параметрами в командной строке. Поначалу это кажется сложным. Но надо отметить, что новейшая серверная ОС Windows Server 2008 может быть установлена… совсем без графического интерфейса.

Человек так устроен, что все непривычное воспринимает в штыки, если это ему не интересно. Первое знакомство с Linux как с заменой Windows может и не вызвать восторга. Это не замена. Это одна из существующих в мире операционных систем, со своей идеологией, своими поклонниками, своими возможностями. Графический интерфейс сделал управление системой более наглядным и доступным, но и Linux, и Windows имеют как преимущества, так и недостатки. Можно сравнить операционную систему с транспортным средством. Для различных дорожных условий и требований пользователя должно быть свое средство. Квадроцикл, снегоход, мотоцикл, легковой автомобиль спортивного типа — все выполняют одну задачу, перевозят пару человек. И бывает, что один и тот же человек имеет в своем распоряжении все перечисленные средства. Linux в локальной сети, — одно из средств управления этой сетью и ее эксплуатации. И если это средство применяется, то надо его осваивать, находить его лучшие стороны.

В следующей главе рассмотрим процедуры, связанные с установкой Linux с учетом предполагаемого назначения системы.

Глава 2

Установка и обновление Linux

Сама по себе установка Linux не сложна. Важно только не пропустить некоторые моменты, чтобы потом не заниматься этой процедурой повторно. Но до установки необходимо правильно выбрать дистрибутив системы. Несмотря на то, что все рассматриваемые нами системы — Linux, и все базовые функции отличаются мало, удобство работы из графического интерфейса может отличаться сильно. Да и не только из графического. Разработчики дистрибутивов ставят перед собой различные цели. Одни делают ставку на высокую стабильность системы, другие на наличие в системе средств украшения графического интерфейса, которые будут "круче", чем в Vista, третьи обращают внимание на логическую завершенность интерфейса, удобство выполнения настроек, четвертые стараются включить в состав дистрибутива как можно больше программ различного назначения, чтобы пользователю дать возможность выбора. Кто-то ориентируется на пользователей, которые чувствуют себя в Linux как рыба в воде, и прекрасно может обойтись совсем (или почти совсем) без графического интерфейса, а кто-то из разработчиков понимает, что если уж есть графический интерфейс, то он должен работать корректно, быть понятным и удобным. Ведь и в Windows можно править реестр в текстовом редакторе, создавать подключения к сетевым ресурсам из командной строки… Но большинство обычных пользователей приходят к этому, освоив систему через графический интерфейс. Наверное, и в Linux можно пойти таким путем. Более того, если есть конкретная задача, которую требуется решить в кратчайшее время, хороший графический интерфейс может оказать неоценимую помощь. Более того, если графический интерфейс тщательно отработан, то он станет поводырем на пути освоения и настройки системы. Другое дело, когда первоначальная настройка выполнена, вы убедились, что все в общих чертах работает правильно, но хотите выполнить тонкие настройки, которые приблизят работу системы к некоторому идеалу, который вы себе представили. В этом случае правка конфигурационных файлов в текстовом редакторе, выполнение особенных команд в терминале неизбежны.

К сожалению, не все версии Linux имеют графический интерфейс, который может выполнить функции поводыря. Нередко можно встретить графические средства, которые просто повторяют строки конфигурационного файла в некоторой форме с полями, которые требуется заполнить. В таком случае придется читать руководства, обращаться к форумам в Интернете, экспериментировать, как и при отсутствии графики. Созданный таким путем конфигурационный файл пользователи обычно сохраняют, делают в нем подробные комментарии, чтобы в следующий раз не тратить уйму времени на подобные настройки, а подкорректировать уже имеющийся файл для новой задачи. Тексты таких файлов можно встретить в Интернете, когда пользователи делятся своими достижениями с теми, кто только начал решать подобную задачу. Но иногда можно пойти другим путем. Даже когда необходимо выполнить настройки в системе, где графический интерфейс далек от совершенства, можно воспользоваться другой системой с развитым графическим интерфейсом. Настроить эту систему, а получившиеся конфигурационные файлы скопировать. Возможно, что придется внести затем некоторые изменения и корректировки, но большая часть настроек будет выполнена верно. Во всяком случае, ускорение работы будет налицо. Мастер установки Linux тоже может работать по-разному для разных дистрибутивов системы. Возможен вариант почти автоматической установки с минимальным участием пользователя. Но мы рассмотрим процедуру установки достаточно подробно, чтобы обойти не очень правильные при решении конкретных задач автоматизированные варианты. Несмотря на некоторые отличия в работе мастера установки в различных дистрибутивах, вы сможете самостоятельно определить момент для вмешательства в его работу, представляя себе все этапы установки Linux. Установка должна выполняться с учетом назначения будущей системы. Это позволит сэкономить место на диске, если в этом есть необходимость, и снизить вероятность появления конфликтов между установленными программами.

Особенности установки Linux в зависимости от назначения системы

Назначение устанавливаемой системы в малой сети может быть следующим:

- рабочая станция, с офисным пакетом и другими прикладными программами;
- универсальный компьютер с функциями рабочей станции и некоторыми серверными функциями;
- сервер для малой сети.

Для каждого из этих случаев можно выбрать один хорошо освоенный вами дистрибутив. Но иногда есть смысл применить разные дистрибутивы Linux, разработчики которых уделили больше внимания выполнению тех или иных задач. Приведем примеры установки Linux из трех дистрибутивов. Для случая рабочей станции применим Mandriva 2008 PowerPack, для универсальной установки CentOS 5.2, а для сервера SLES 10 SP1.

Выбор дистрибутивов в большой степени условен, — грамотный пользователь Linux может любую систему настроить по своим требованиям. Но, во-первых, мы познакомимся сразу с тремя вариантами Linux, а во-вторых, эти системы действительно подходят для решения поставленной задачи. Кто-то может обратить внимание на "свежесть" рассматриваемых продуктов. Есть более новые версии Mandriva, в которые включены приложения для малого и среднего бизнеса. Подобные средства есть в дистрибутивах для сервера, которые мы еще будем рассматривать в книге. Есть более новые версии SLES (дистрибутив SLES 10 SP2 занимает два DVD). Процедура установки рассматриваемых дистрибутивов не изменилась с выходом новых версий.

Установка Mandriva 2008 PowerPack

Как и любой другой дистрибутив Linux, Mandriva 2008 PowerPack необходимо получить на DVD или CD-диске. Получить диски можно, купив дистрибутив в магазине или заказав его по почте. Дистрибутивы Linux можно загрузить через Интернет в виде образов дисков. Образы имеют расширение iso, и их можно записывать на обычные CD-R DVD-R-диски. В Linux это делается очень просто. Файлы образов дисков можно записывать на физические носители, копируя образ как физический диск штатными средствами Linux. Если вы устанавливаете Linux впервые, то создать диск с дистрибутивом можно и из Windows с помощью программ Nero или Roxio, которые могут прилагаться к новым компьютерам и даже входить в дистрибутивы, если Windows была предустановлена на ваш компьютер изготовителем. На рис. 2.1 показано окно программы Roxio, в котором выбрана команда **Copy | Burn Image** и выбран источник записи — загруженный из Интернета образ диска.

Вы можете также обратиться к знакомым, у которых уже установлена Linux, и попросить их записать образ на болванку. Думаю, что они с удовольствием выполнят вашу просьбу, порадовавшись, что еще один пользователь ПК решил войти в мир open source.

Теперь, когда у вас есть установочный диск с дистрибутивом Linux, загрузите с него компьютер, на который хотите установить новую систему. Если на этом компьютере уже установлена Windows, но есть свободное место на дисках, Linux установится, сохранив возможность загрузки Windows. Но автор

рекомендовал бы первую установку выполнять на отдельный винчестер, отключив винчестер с установленной Windows. Это необязательное требование, но на отдельном винчестере вы можете чувствовать себя свободнее, проводя эксперименты с новой системой. А когда все будет установлено, и вы решите использовать Linux и Windows, можно подключить винчестер с Windows, а вариант загрузки выбирать с помощью клавиши <F12> на начальном этапе загрузки компьютера, выбирая винчестер с требуемой системой. Вариантов установки системы может быть много, но мы рассмотрим обычную установку на отдельный винчестер. Для пояснения некоторых особенностей установки системы к тестовому компьютеру подключен второй винчестер. Итак, загрузите компьютер с диска с дистрибутивом Linux.

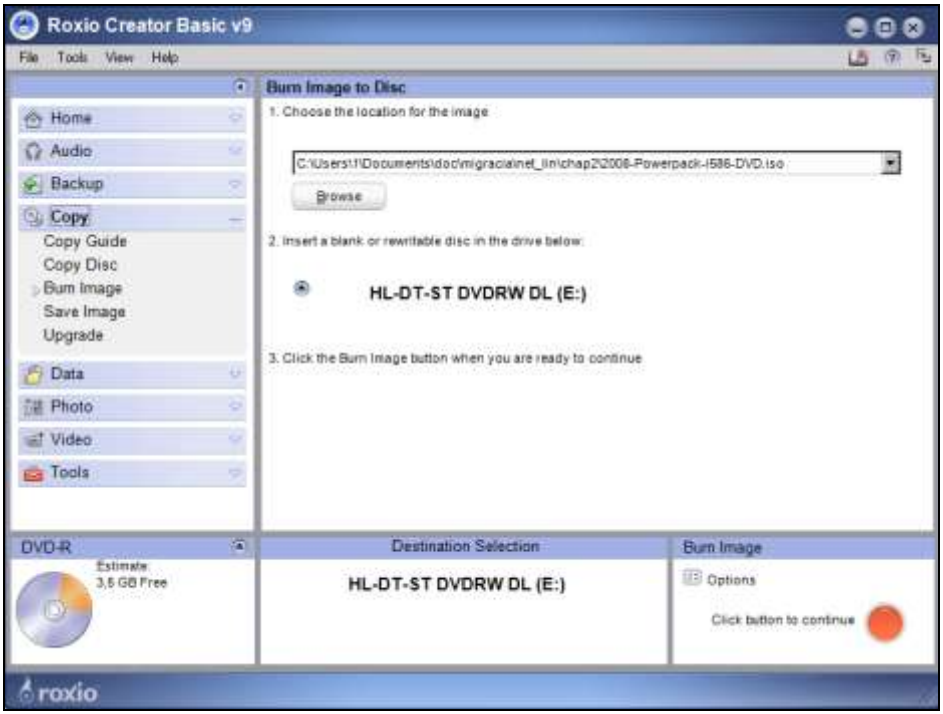


Рис. 2.1. Окно Roxio Creator Basic V9

После загрузки программы установки в память компьютера вы увидите экран установки системы на этапе выбора языка системы (рис. 2.2).

На этом экране можно выбрать язык вашей системы, но при желании можно выбрать не один, а несколько языков, развернув меню **Multi languages** (над кнопкой **Help**), что позволит выбирать желаемый вариант при загрузке.

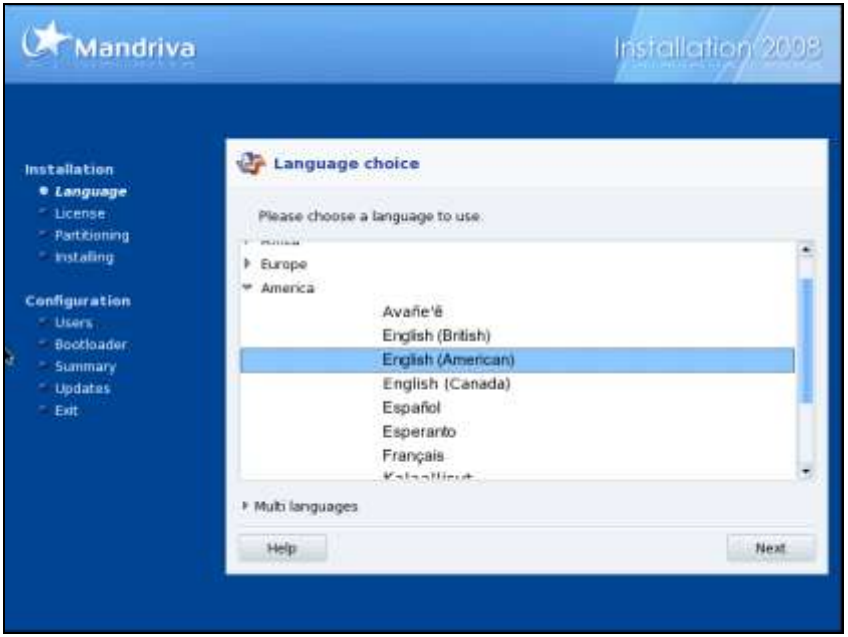


Рис. 2.2. Экран установки Linux Mandriva 2008 PowerPack. Выбор языка

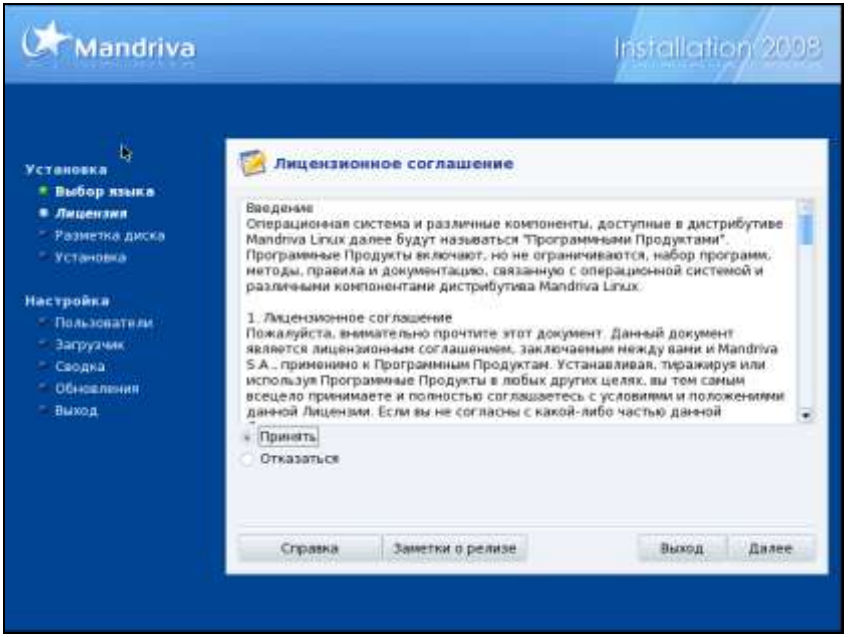


Рис. 2.3. Экран установки Linux Mandriva 2008 PowerPack. Лицензия

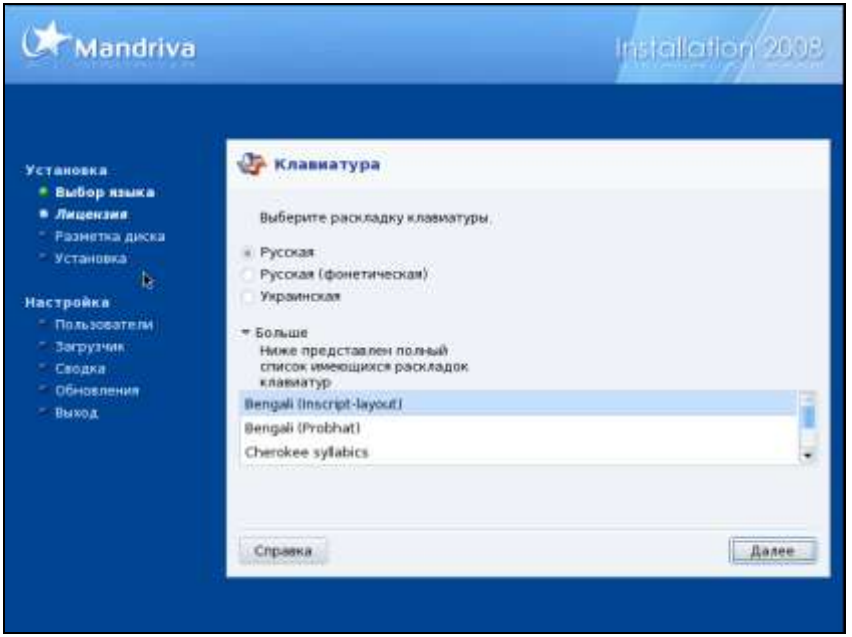


Рис. 2.4. Экран установки Linux Mandriva 2008 PowerPack. Выбор раскладки клавиатуры

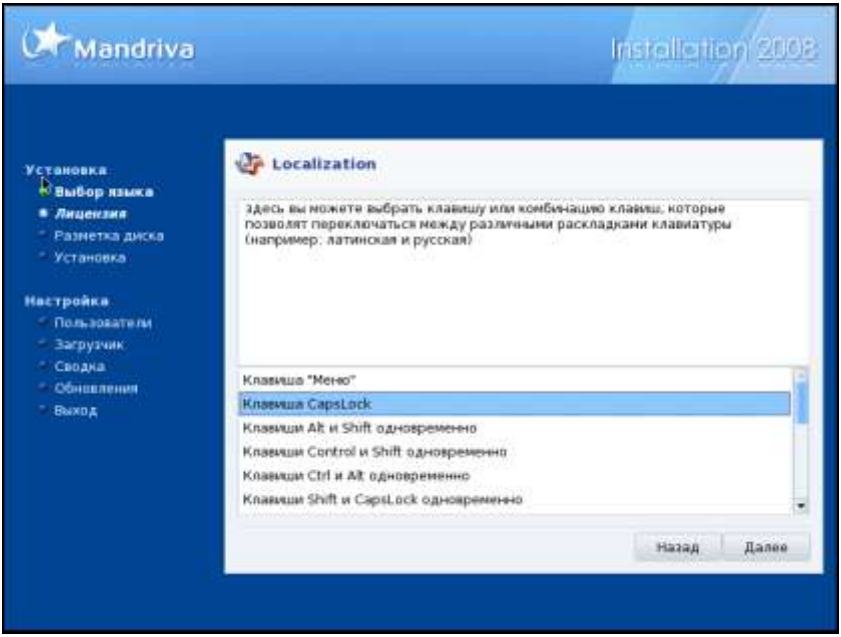


Рис. 2.5. Экран установки Linux Mandriva 2008 PowerPack. Переключение раскладок

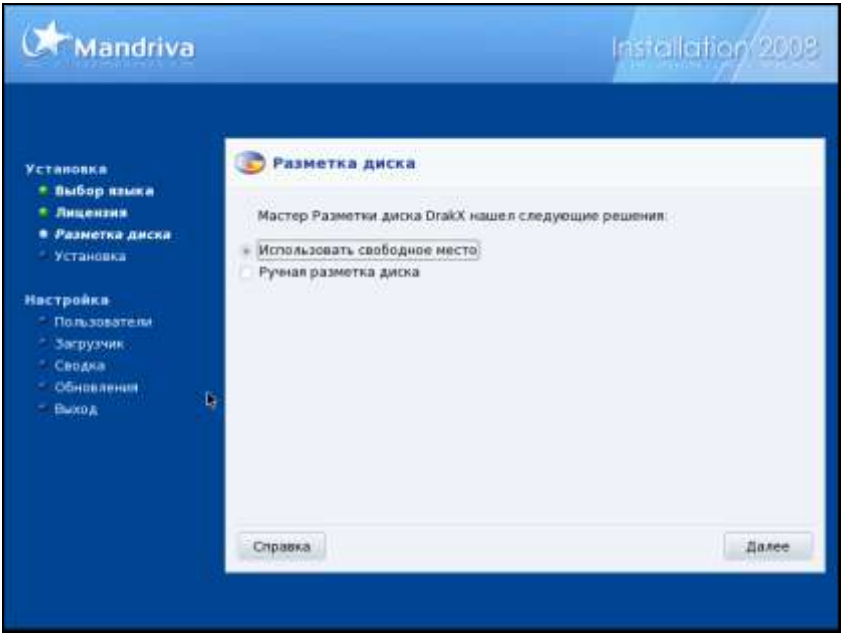


Рис. 2.6. Экран установки Linux Mandriva 2008 PowerPack. Выбор способа разметки диска

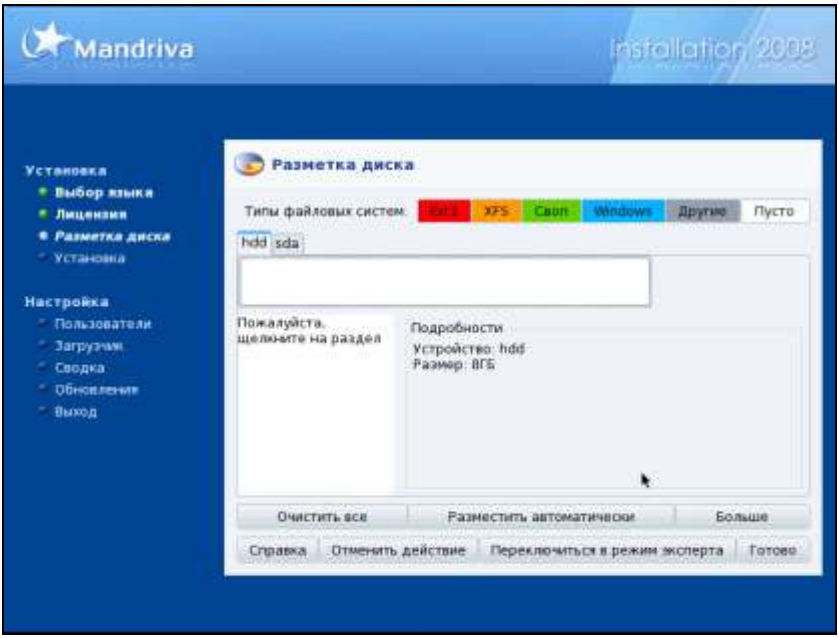


Рис. 2.7. Экран установки Linux Mandriva 2008 PowerPack. Разметка диска

С момента выбора языка программа установки системы будет использовать выбранный язык и предложит принять Лицензионное соглашение (рис. 2.3). Этот этап есть при установке как коммерческих, так и совершенно бесплатных версий системы. Прочитайте текст лицензии и отметьте переключатель **Принять**, если вы согласны с лицензией.

Следующий этап — выбор раскладки клавиатуры (рис. 2.4). На этом экране можно выбрать раскладку из короткого списка, предложенного системой, или, раскрыв список **Больше** в нижней части экрана, выбрать какую-нибудь особенную раскладку. Но даже если вам и потребуется другая раскладка кроме русской, ее можно выбрать и после установки системы в качестве дополнительной. Независимо от вашего выбора всегда будет использоваться латинская раскладка, как дополнительная. На следующем экране (рис. 2.5) вы можете выбрать способ переключения между раскладками клавиатуры. Среди возможных сочетаний следует обратить внимание на те, что не используются в Linux, например клавиша Windows. Назначение этой клавиши для переключения раскладок оставит больше свободы для назначения горячих клавиш, которые в Linux широко применяются опытными пользователями.

Выбранные параметры переключения раскладок начнут действовать только после перезагрузки по завершении инсталляции. А пока будет работать правая клавиша <Ctrl>. Об этом система предупредит вас соответствующим сообщением.

После выбора параметров переключения раскладок система предложит выбрать вариант разметки диска (рис. 2.6). Начинающие пользователи Linux на этом этапе не решаются выбрать ручную разметку и полагаются на мастера разметки диска, который может предложить вариант, пригодный для большинства способов установки. Вы можете посмотреть вариант, предложенный мастером, а потом сделать по-своему, вернувшись к экрану выбора способа разметки. Выберем **Ручная разметка диска** и перейдем к следующему экрану (рис. 2.7).

На этом экране показаны имеющиеся в системе жесткие диски и разделы на них. Поскольку мы выполняем установку на новый винчестер, разделов пока нет, и мы создадим их самостоятельно. В примере установка выполняется на виртуальные диски малого размера, поэтому размер создаваемых разделов тоже будет небольшим. В данном случае нам важно понять принцип выбора разделов, выбора их размеров и точек монтирования. Файловая система в Linux устроена иначе, чем в Windows. Дискам, как физическим, так и логическим, не присваиваются буквы. Системе не важно, сколько на дисках первичных или расширенных разделов, — загрузчик Linux прекрасно разбирается, где установлено ядро системы. А если на дисках есть другая операционная система,

то он в состоянии предложить для загрузки и ее, выводя такую возможность в загрузочное меню. Устанавливая Linux на отдельный винчестер, мы пока не воспользуемся такими выдающимися способностями загрузчика.

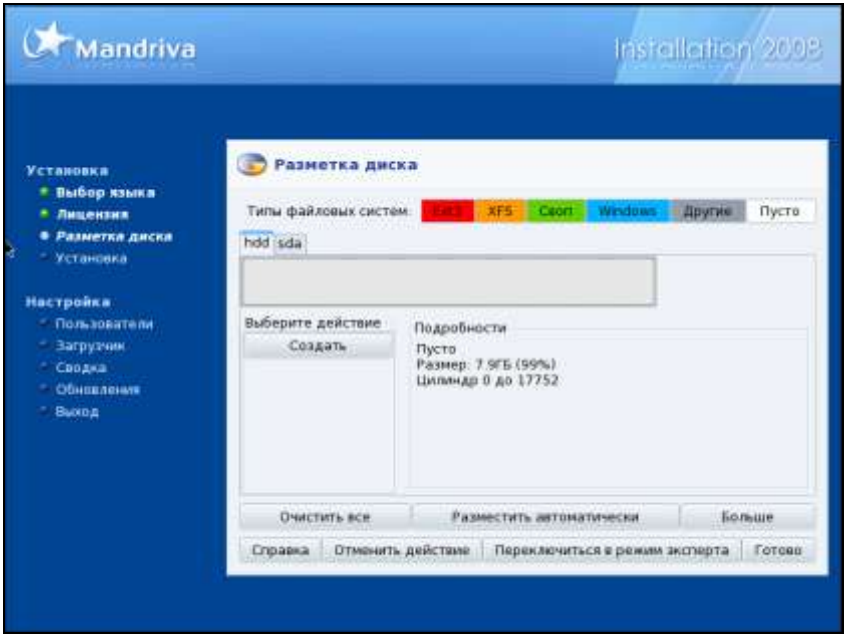


Рис. 2.8. Экран установки Linux Mandriva 2008 PowerPack. Переключение раскладок

Воспользуемся подсказкой, которую видим на экране, и щелкнем мышью на поле диска hdd. При этом вместо подсказки появится кнопка **Создать** (рис. 2.8). Нажав эту кнопку, мы увидим экран (рис. 2.9) с полями, где можно выбрать из ниспадающих списков файловую систему и точку монтирования для нового раздела. Самой распространенной в Linux файловой системой на сегодняшний день является журналируемая файловая система ext3. Она позволяет надежно хранить данные, а за счет отслеживания транзакций восстанавливать файлы до состояния, предшествующего сбою. Вы можете увидеть в списке и другие файловые системы. Каждая из них может применяться для достижения тех или иных качеств системы, но нас практически во всех случаях устроит ext3. Ее и будем выбирать при создании каждого раздела.

Примечание

Следует сразу пояснить, почему диски обозначены на экране по-разному. Диски с интерфейсами SCSI и SATA в начале своего обозначения имеют букву "s", обозначение IDE дисков начинается на "h".

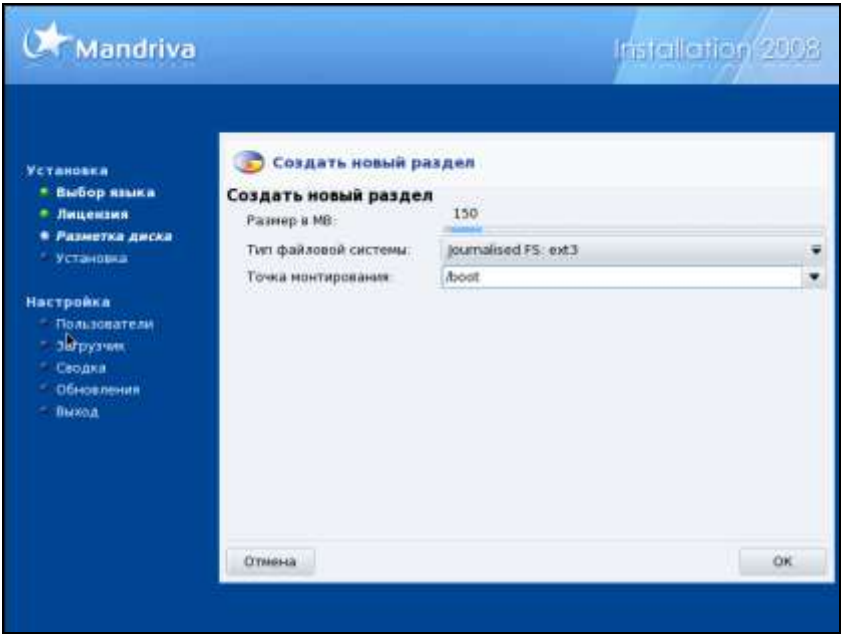


Рис. 2.9. Экран установки Linux Mandriva 2008 PowerPack. Создание раздела

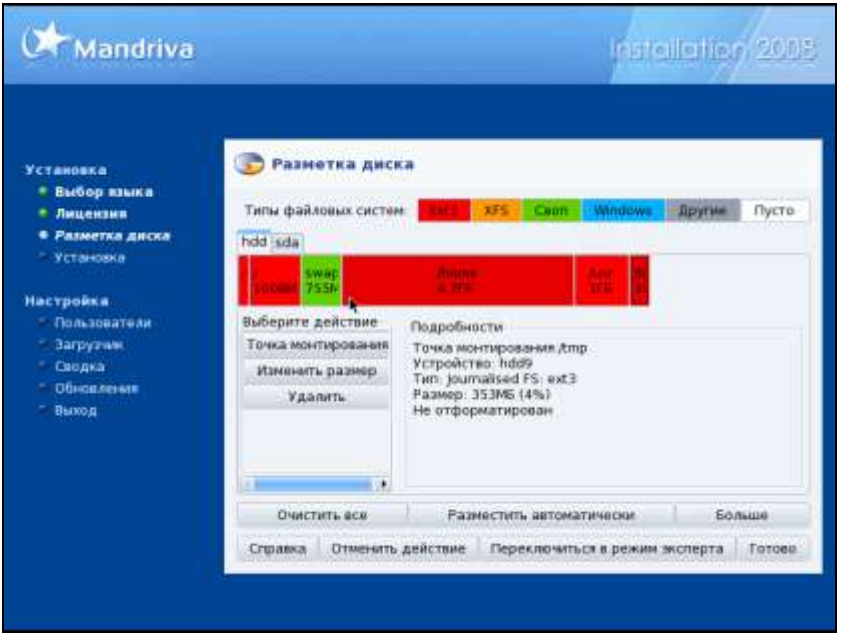


Рис. 2.10. Экран установки Linux Mandriva 2008 PowerPack. Созданные разделы

Программа установки Mandriva Linux не показывает нам, какой раздел создается — первичный или расширенный. Это для нас не имеет значения, и программа установки создает тот или иной вариант раздела по мере их создания автоматически.

Точка монтирования первого создаваемого нами раздела — /boot. Это раздел, который в процессе работы системы практически не изменяется, если только мы не будем добавлять дополнительные варианты загрузки системы. Одним из таких вариантов может быть загрузка с ядром Xen. Это ядро виртуальной машины, в которую можно устанавливать другие операционные системы. В этой книге средства виртуализации будут рассматриваться, но другие. С Xen вы можете ознакомиться самостоятельно в Интернете или в справке для систем, с которыми это ядро поставляется (SUSE, CentOS и др.). Практически для всех вариантов установки Linux достаточно 150 Мб для загрузочного раздела. Современные винчестеры имеют такой значительный объем, что изображение загрузочного раздела может быть почти незаметным, когда будут добавлены остальные разделы системы (рис. 2.10). Все последующие действия похожи на описанное как две капли воды. Меняем только размер раздела и точку монтирования.

Точка монтирования в уже установленной системе выглядит, как папка с файлами, но ее размер не может превысить заранее выбранный нами при создании раздела. Поэтому следует позаботиться о достаточном размере для разделов, в которые может добавляться значительное число файлов при установке самой системы и программ при дальнейшей ее работе. Один из необязательных, но влияющих на производительность системы раздел — /swap. Этот раздел имеет одноименную файловую систему и должен иметь размер не менее половины размера оперативной памяти. Его назначение подобно файлу подкачки Windows. Как и файл подкачки, этот раздел может быть заменен файлами, создаваемыми после установки системы, но это в случае, когда не рассчитали при установке. Корневой раздел (/) может иметь размер 50—70 Мбайт, разделы /usr, /var могут интенсивно пополняться при установке дополнительных программ. Им можно выделить также по несколько десятков мегабайт. Раздел /tmp можно не выделять отдельно. Этот каталог может просто находиться внутри корневого раздела. Но при недостатке дискового пространства временные файлы могут занять все свободное место. При этом работа системы может быть нарушена. Если для временных файлов выделен отдельный раздел, то они не смогут занять места больше, чем им отведено. Значительное место может потребоваться разделу /home, где находятся папки и файлы пользователей. Если вы предполагаете сохранять документы пользователей таким образом, чтобы они не были потеряны при уста-

новке другой версии Linux, можно создать раздел, которого нет в списке. В примере (рис. 2.11) раздел /home/doc создан на втором винчестере. В системе он будет виден как папка, вложенная в /home, но физически он находится на отдельном диске. Это позволит в будущем при переустановке системы не форматировать этот раздел, а просто подключить его к какой-либо точке монтирования. Причем совершенно не обязательно помещать его внутрь раздела /home, но в этом разделе файлы могут быть по умолчанию доступны пользователям — не администраторам. Впрочем, установить любые необходимые вам права можно для файлов, находящихся в любом разделе.

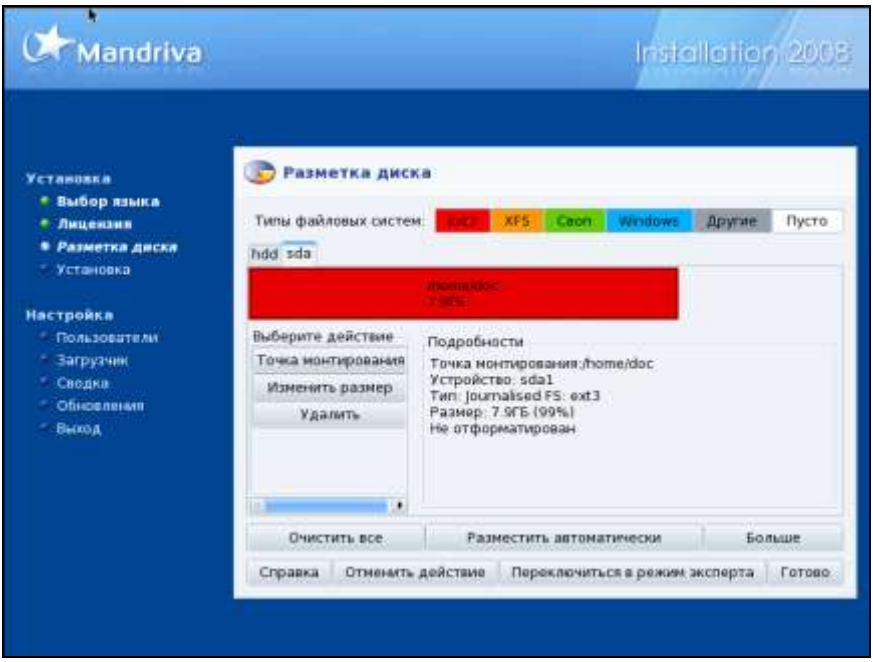


Рис. 2.11. Экран установки Linux Mandriva 2008 PowerPack. Раздел на втором винчестере

После создания разделов программой установки по нашим указаниям можно выбирать программное обеспечение, которое будет установлено в системе (рис. 2.12). Можно выбрать стандартный комплект программ, которые будут установлены с выбранным по умолчанию рабочим столом KDE или GNOME, но можно выбрать все самостоятельно, отметив **Custom install** на экране выбора группы пакетов (рис. 2.12). При этом откроется экран с более подробным перечнем групп пакетов (рис. 2.13).

Рис. 2.12. Экран установки Linux Mandriva 2008 PowerPack. Выбор группы пакетов

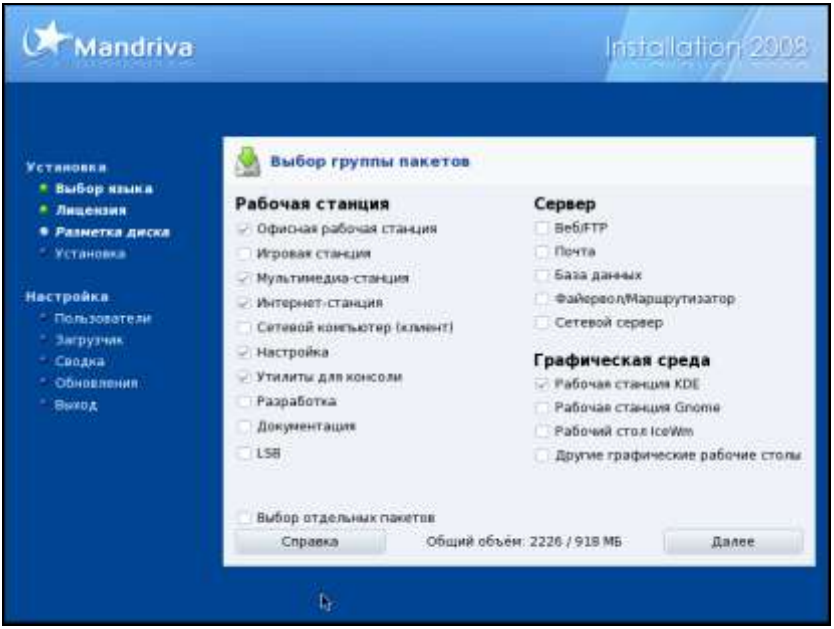


Рис. 2.13. Экран установки Linux Mandriva 2008 PowerPack.
Выбор группы пакетов (подробно)

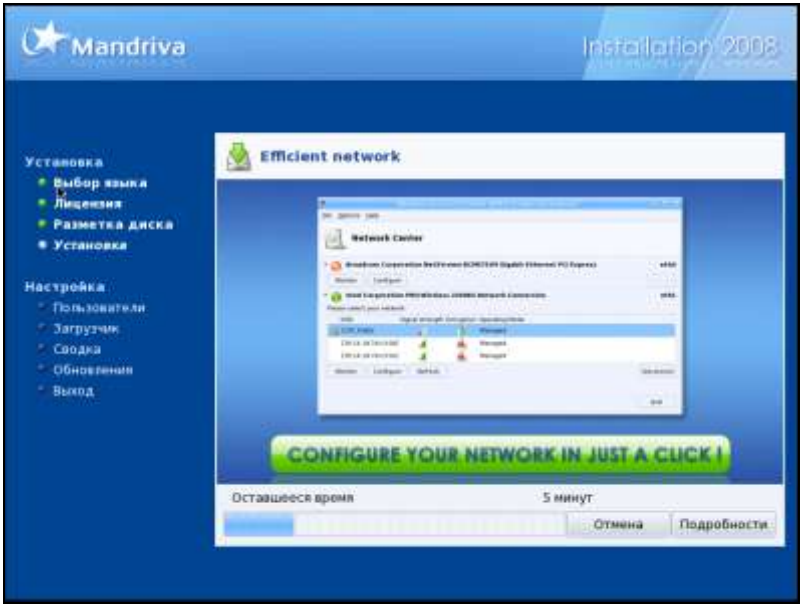


Рис. 2.14. Экран установки Linux Mandriva 2008 PowerPack. Выполняются автоматические операции

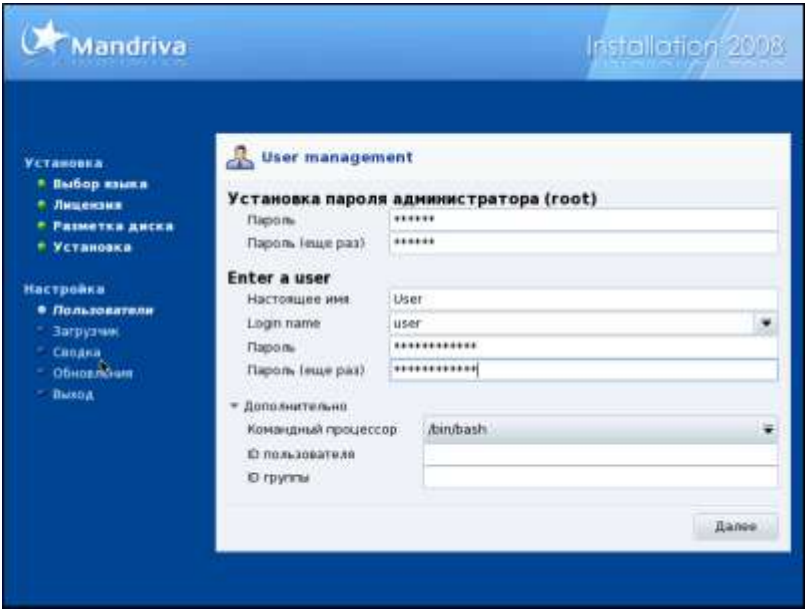


Рис. 2.15. Экран установки Linux Mandriva 2008 PowerPack. Управление пользователями

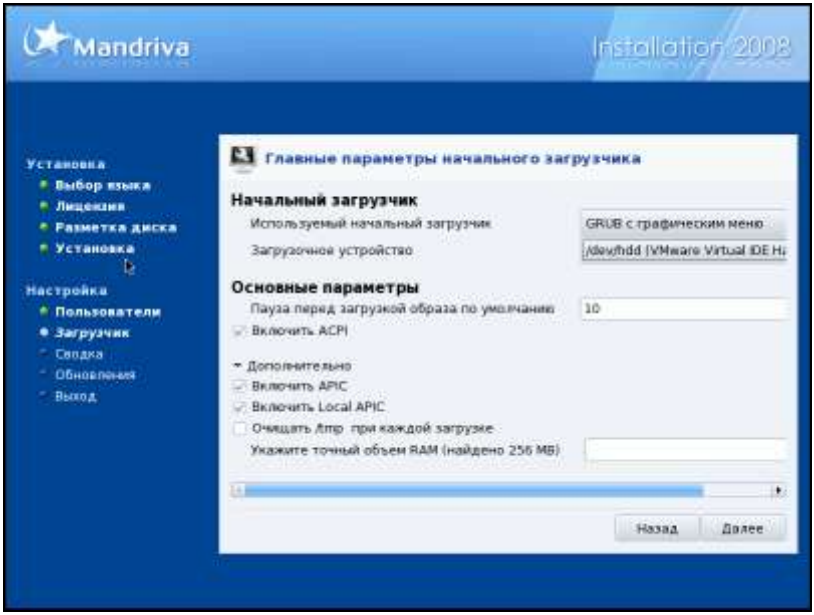


Рис. 2.16. Экран установки Linux Mandriva 2008 PowerPack. Параметры загрузчика

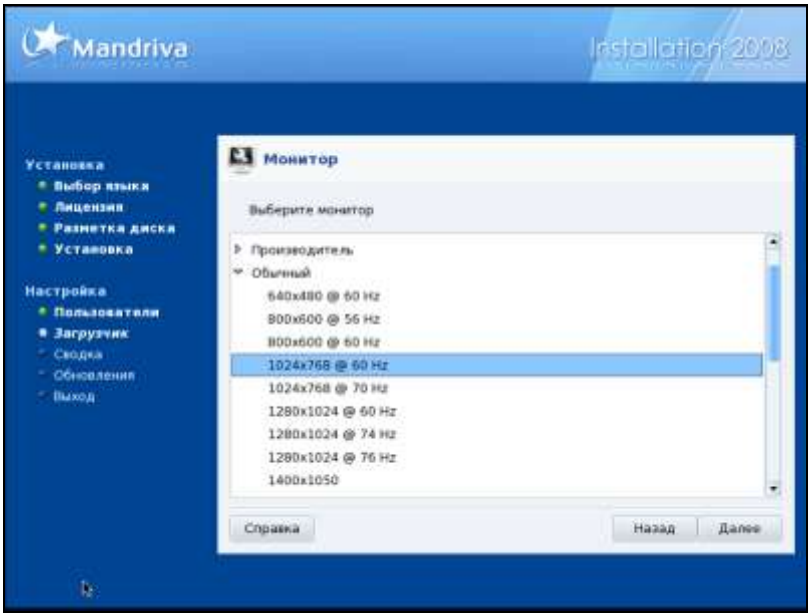


Рис. 2.17. Экран установки Linux Mandriva 2008 PowerPack. Параметры монитора

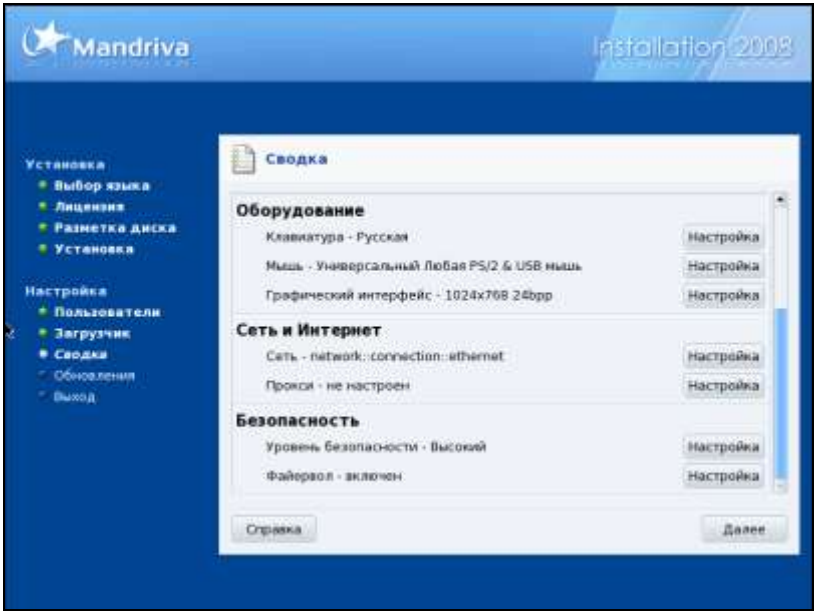


Рис. 2.18. Экран установки Linux Mandriva 2008 PowerPack. Сводка

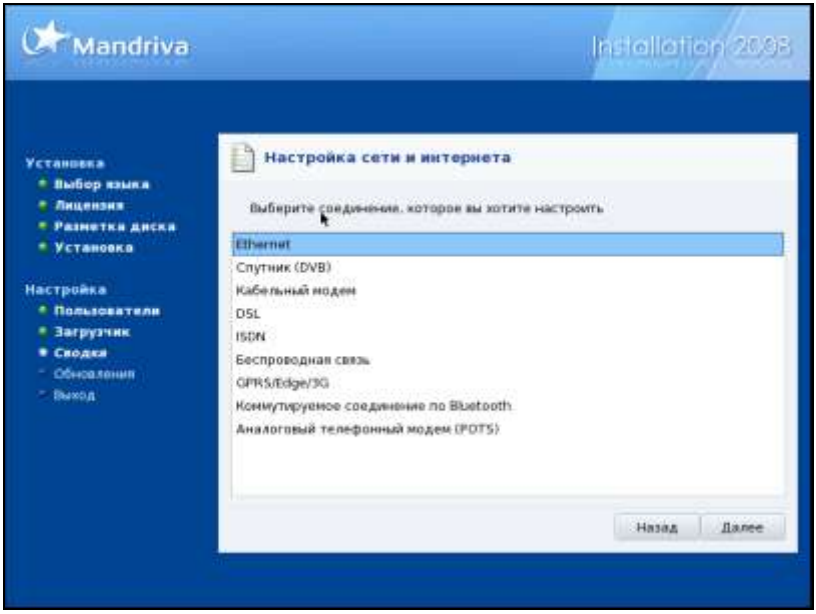


Рис. 2.19. Экран установки Linux Mandriva 2008 PowerPack. Настройка сети, выбор соединения

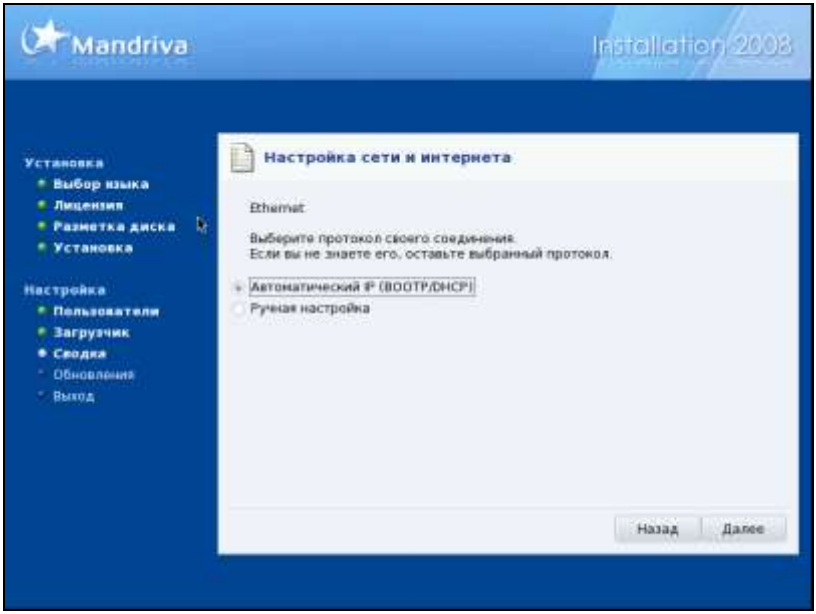


Рис. 2.20. Экран установки Linux Mandriva 2008 PowerPack.
Настройка сети, выбор способа настройки

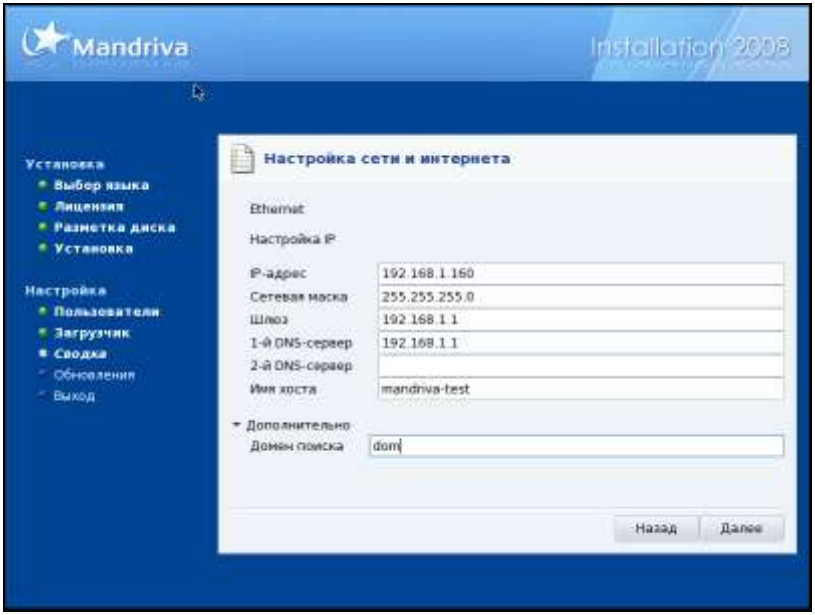


Рис. 2.21. Экран установки Linux Mandriva 2008 PowerPack.
Настройка сети, параметры соединения

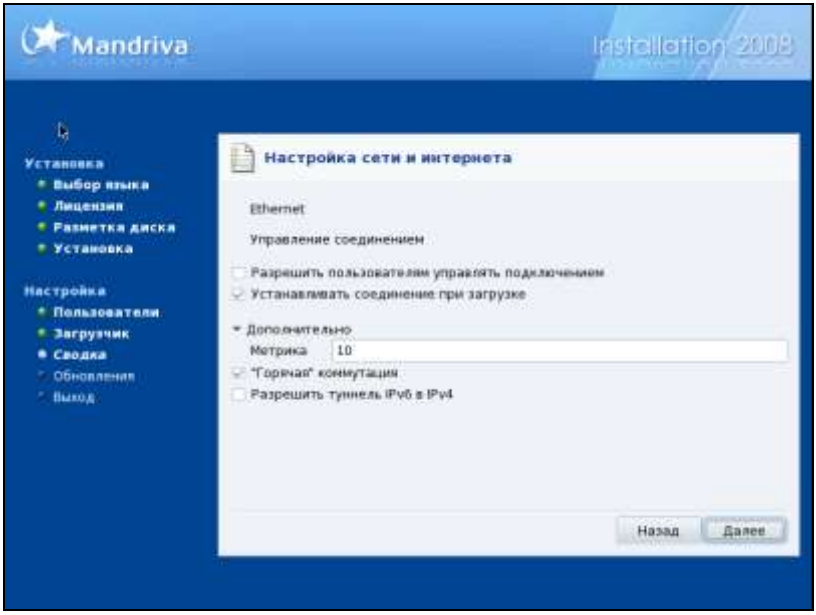


Рис. 2.22. Экран установки Linux Mandriva 2008 PowerPack. Настройка сети, параметры управления

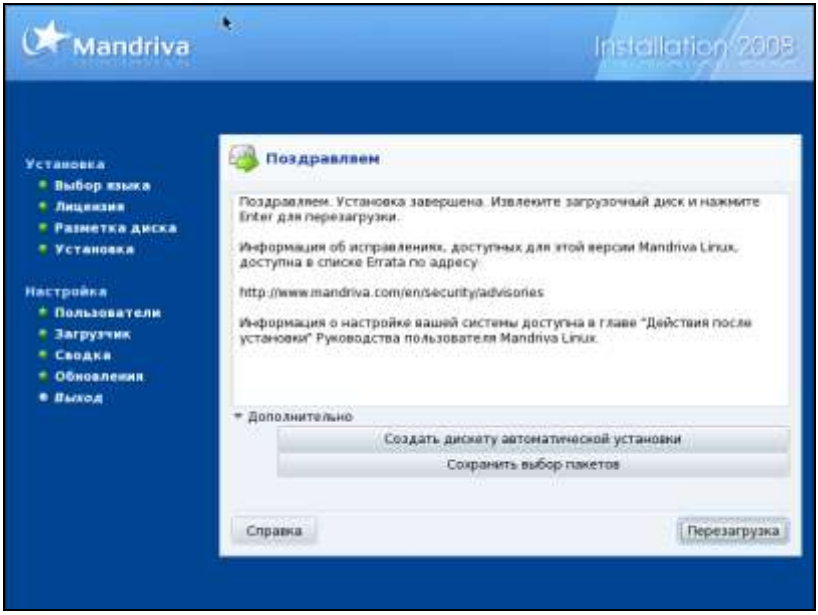


Рис. 2.23. Экран установки Linux Mandriva 2008 PowerPack. Финал

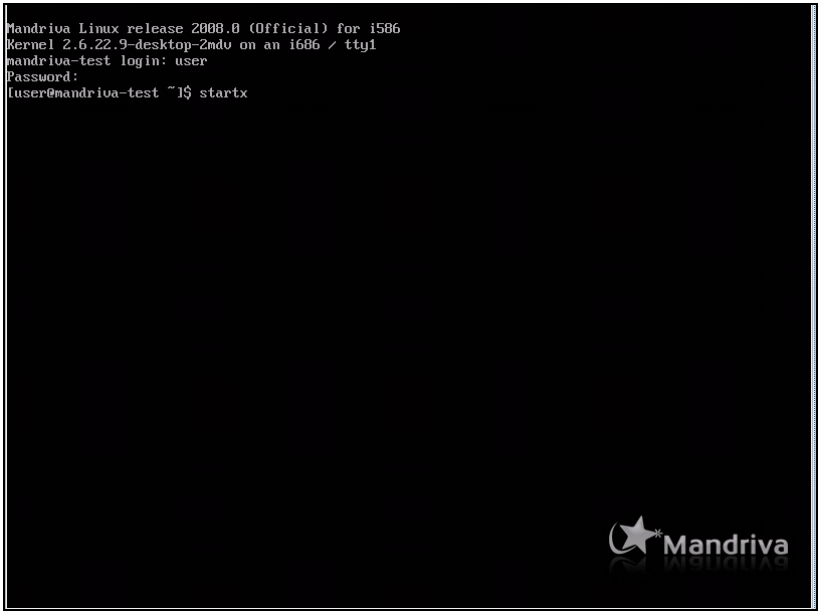


Рис. 2.24. Первый запуск Linux Mandriva 2008 PowerPack. Текстовый режим

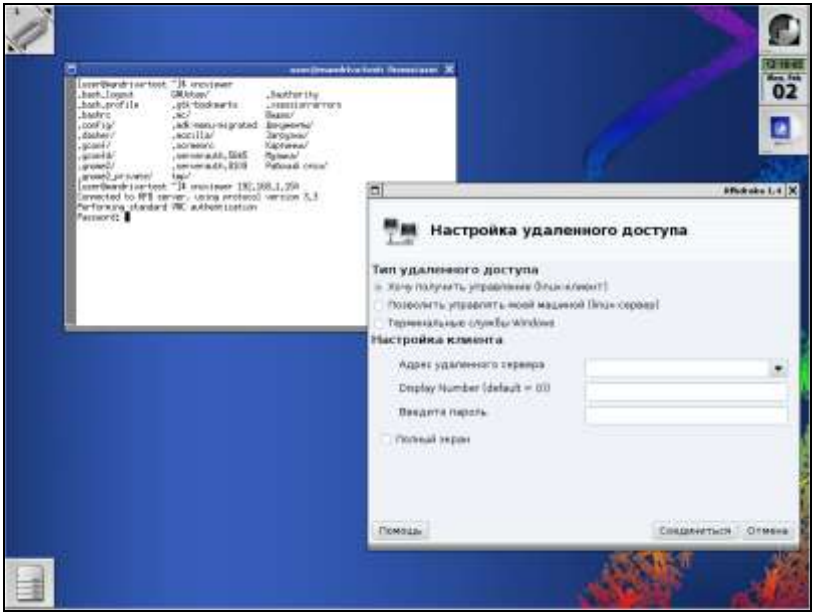


Рис. 2.25. Первый запуск Linux Mandriva 2008 PowerPack. Графический режим

Здесь можно указать необходимые группы программ. Мы устанавливаем систему для рабочей станции, и нас могут интересовать программы для рабочей стации. При необходимости можно отметить опцию **Выбор отдельных пакетов**, и из отмеченных групп выбрать только необходимые пакты. Выбор **Графической среды** (рабочего стола) — дело вкуса. По умолчанию предлагается рабочий стол KDE. Если ваш компьютер не имеет достаточного объема оперативной памяти и ограничено место на жестких дисках, можно ограничиться рабочим столом IceWM. В этой тестовой установке будет выбран именно этот рабочий стол. Закончив с выбором программного обеспечения, дадим системе поработать самостоятельно. По нашему предварительному выбору она выполнит все необходимые действия (рис. 2.14), сообщая об оставшемся до завершения операций времени.

Установка системы близка к завершению. Следующий экран (рис. 2.15) предлагает установить пароль для администратора системы и ввести имя пользователя и пароль для первого обычного пользователя системы. Дополнительные параметры можно не указывать, и система их установит автоматически.

На рис. 2.16 показан экран установки параметров загрузчика. Можно оставить все параметры по умолчанию. Стоит обратить внимание на опцию **Очищать /tmp при каждой загрузке**. Она может помочь ограничить захват дискового пространства временными файлами, но при условии регулярной перезагрузки системы. А Linux, как известно, может работать продолжительное время совсем без перезагрузок.

Установив параметры загрузчика, переходим к параметрам монитора (рис. 2.17). Здесь можно выбрать драйвер монитора по производителю или указать разрешение экрана, при котором будет работать ваш монитор.

Наконец, выполнены все основные действия по выбору параметров установки. Программа установки выводит на экран сводку с указанием параметров системы (рис. 2.18). Но часть этих параметров либо настроена автоматически, либо не настроена совсем. Если есть такая необходимость, мы можем уточнить настройки системы, выбрав кнопку **Настройка** напротив требуемого параметра. Обычно требует уточнения настройка сети.

Для начала следует выбрать вариант нашего сетевого соединения (рис. 2.19). Выбрав Ethernet, перейдем к экрану выбора способа настройки соединения (рис. 2.20). Система предлагает два варианта — автоматический и ручную настройку. Так же как в Windows, есть возможность оставить заботы по настройке сети самой системе.

Выбрав ручную настройку (рис. 2.21), достаточно указать обычные параметры для ваших сетевых адаптеров, которые вы указывали при настройке сети в Windows.

В качестве последнего штриха перед завершением установки система предлагает указать параметры управления сетевым соединением (рис. 2.22). При желании можете поменять их по своему усмотрению. Но можно оставить как есть.

Вот мы и подошли к финишу. Система, завершив все операции по настройке сети, вывела экран с поздравлением (рис. 2.23). Остается перезагрузить компьютер и увидеть приглашение системы. Выбирая графическую среду для нашей рабочей станции, мы указали IceWM. Если при установке KDE или GNOME загрузка системы завершается запуском графического режима работы, то в данном случае она остановилась на текстовом режиме (рис. 2.24).

Что ж, нас это не пугает. Вводим имя и пароль пользователя, учетную запись которого мы уже создали. После удачной авторизации вводим команду `startx`.

Загрузится рабочий стол, выбранный при установке системы (рис. 2.25). Несмотря на очень скромный вид, IceWM позволяет запускать необходимые программы и работать с ними.

Установка SLES 10

Установка любой современной версии Linux выполняется практически однотипно. Программы — установщики Linux проведут вас по всем этапам установки системы и с помощью наводящих вопросов помогут установить именно тот вариант системы, который вам необходим. На рис. 2.26 показан один из завершающих моментов установки SLES 10 SP1 — настройка оборудования. Сравните его с рис. 2.18. Не правда ли, очень похоже? Некоторые отличия в процедурах установки не существенны, поэтому подробно описывать процесс установки не имеет смысла.

На рис. 2.27 показан экран входа в систему SLES 10. Подобный экран входа будет появляться при загрузке любой версии Linux, если при установке будет выбран рабочий стол KDE или GNOME. При желании вы можете отключить автоматическую загрузку графического режима для экономии ресурсов, например. Это может иметь смысл для сервера, на котором никто не будет выполнять обычную работу, как на рабочей станции.

Особенности установки системы в качестве сервера заключаются в выборе несколько иной разбивки дискового пространства и выборе программного обеспечения. На диске могут быть созданы специализированные разделы для выполнения определенных функций. Например, если предполагается использовать сервер в качестве сервера виртуальных машин, то есть смысл под эти виртуальные машины (файлы виртуальных машин) выделить отдельный раздел. Еще лучше поместить этот радел на отдельном диске, что улучшит быстродействие виртуальных машин.

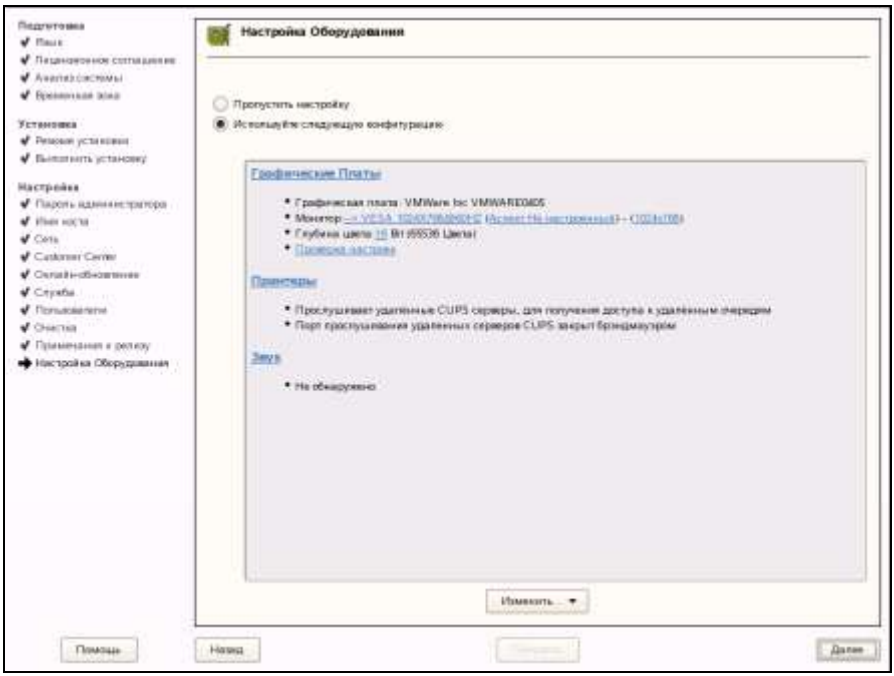


Рис. 2.26. Экран установки SLES 10. Настройка оборудования

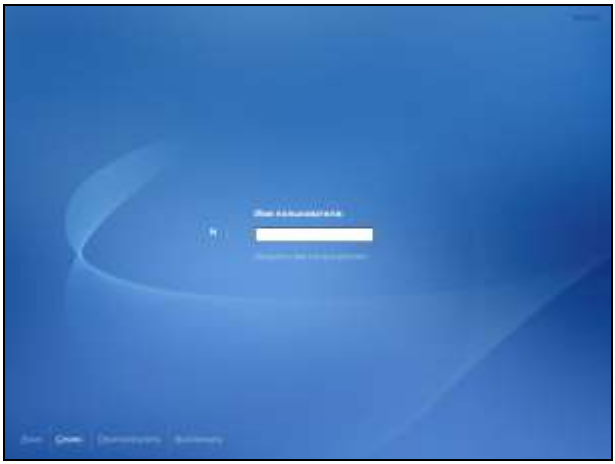


Рис. 2.27. Первый запуск SLES 10. Графический режим

При выборе программного обеспечения следует ориентироваться на задачи сервера. Он может выполнять функции файлового сервера (Samba), веб-сервера (Apache), сервера авторизации (LDAP), маршрутизатора, сервера

печати (CUPS) и др. Для работы в качестве маршрутизатора дополнительных пакетов потребуется дополнительная настройка сетевых служб. Все эти варианты будут рассмотрены в книге подробно.

Обновления — всегда ли они необходимы?

Работая с Windows вы, наверное, привыкли к тому, что необходимо систему поддерживать в актуальном состоянии. Значительная часть обновлений связана с безопасностью, исключением возможности отрицательного воздействия на систему вирусов и вредоносных программ. Ситуация усугублялась тем, что вы практически всегда работали от имени администратора системы, чтобы не ограничивать себя в возможностях установки и удаления программ, и в других действиях, требующих административных привилегий.

В Linux такой стиль работы не только не приветствуется, но даже сама система вас очень красноречиво предупреждает, когда вы начинаете работать от имени суперпользователя. Это не принято. У вас всегда есть простые средства для выполнения каких-либо действий с повышенными полномочиями. А вирусов для Linux слишком мало, чтобы их всерьез опасаться. Никто и никакая неизвестная вам программа не может получить доступ к системе с достаточными для выполнения деструктивных действий правами. Поэтому к обновлениям в Linux отношение может быт другим.

Есть такое мнение, что обновления в Linux нужны только в случаях, когда они устраняют ошибку, с которой вы столкнулись, или добавляют необходимую вам функциональность. И в самом деле, если у вас уже настроена система и прекрасно работает, зачем выполнять ее обновление? Особенно верно это для закрытых внутри сети серверов.

С другой стороны, если вы знаете, что обновление не принесет с собой проблем по перенастройке компьютера, канал в Интернет у вас хороший, то можно получать все обновления, чтобы осознавать, что вы обладаете самой последней стабильной версией всех компонентов системы.

Осторожно следует относиться к обновлениям ядра системы. Существуют программы, которые настраиваются при установке на работу с тем ядром, которое установлено в этот момент в системе. Сама процедура такой настройки не сложна, но если ваш сервер получает обновления автоматически, а вы в этот момент находитесь не рядом с ним, работа каких-то компонентов системы может быть нарушена. В качестве примера можно привести VMware Server для Linux. Если обновить ядро, виртуальные машины перестанут запускаться до повторного запуска скрипта конфигурации виртуальной машины. При этом на все вопросы, которые задаст скрипт конфигурации, достаточно дать утвердительные ответы, подтвердив ранее выбранные параметры.

Глава 3

Рабочая станция

В этой главе мы рассмотрим рядовую рабочую станцию под управлением Linux.

Рабочая станция — это обычный компьютер, входящий в локальную сеть. На ней выполняются пользовательские приложения, через нее осуществляется выход в Интернет, выполняется печать на локальный или сетевой принтер, подключение к ресурсам локальной сети. Работая с рабочей станцией под управлением Windows, тоже можно использовать ресурсы сети под Linux. Для обеспечения возможности взаимодействия рабочих станций Windows и Linux есть все необходимые средства. Для файлового обмена в сети Linux реализуется работа по протоколу Samba, любой сетевой принтер может быть подключен как к Windows, так и к Linux рабочей станции. Работа с программами и программными пакетами, имеющими графический интерфейс, в Linux мало отличается от аналогичной работы в Windows, но сами программы могут отличаться как по функциональности, так и по своему интерфейсу. Но это дело привычки. Даже в Windows переход от офисного пакета Microsoft Office 2003 к Microsoft Office 2007 сопряжен с достаточно продолжительным процессом привыкания. Освоив программные средства рабочей станции под управлением Linux, вы, вполне вероятно, посчитаете возможным полностью отказаться от Windows, если только нет требований полной совместимости форматов ваших данных с какими-нибудь другими системами. Например, многие издательства работают исключительно с форматами документов Windows. Но и в этом случае можно не отказываться от самой операционной системы. Есть средства, которые обеспечат полную совместимость форматов ваших файлов с требованиями внешних организаций.

В отличие от Windows, Linux обычно содержит в своем составе несколько программных средств для выполнения определенной задачи. Это позволяет выбрать наиболее удобные в данный момент или наиболее доступные пользователю. Обзор рабочей станции под управлением Linux начнем со средств управления и администрирования.

Средства управления и администрирования

Рабочая станция Linux обязательно должна иметь своего администратора. Им может быть и единственный пользователь компьютера, если это ваша личная машина. Но учетная запись администратора используется только в случае крайней необходимости. Текущая работа под учетной записью root запрещена. Имя учетной записи суперпользователя всегда одинаково, а возможности обычной работы под этой учетной записью разработчики дистрибутивов стараются ограничить. Root имеет неограниченные права в системе, поэтому и сам пользователь, и злоумышленник может нарушить ее работу. При работе от имени обычного пользователя система надежно защищена и не подвержена деструктивным действиям злоумышленников. При необходимости выполнения процедур администрирования обычный пользователь имеет возможность временно получить права администратора, введя пароль суперпользователя по запросу системы. Есть также возможность запуска приложений от имени администратора.

Вход под учетной записью суперпользователя при загрузке системы имеет смысл только в одном случае. Если вы во время инсталляции системы не указали ни одной учетной записи обычного пользователя, то войдя в систему под именем root, вы сможете создать дополнительные учетные записи. Далее следует завершить сеанс администратора и войти от имени рядового пользователя.

> ***Примечание***
>
> Ограничения на работу от имени root распространяются не только на графические сеансы работы, но и на сеансы консольные. Графика в Linux только дополняет систему наглядными и удобными средствами. Средства администрирования системы всегда в своей основе имеют консольные приложения, которые не требуют наличия графики.

Первое средство администрирования — это возможность открыть консольный сеанс от имени root. Для этого нет необходимости выходить из текущего сеанса работы. Можно нажатием сочетания клавиш <Ctrl>+<F*n*> перейти в консольный сеанс номер *n*. Всего таких сеансов может быть шесть. На экране вы увидите приглашение ввести логин, а затем пароль. Если вы намерены только выполнить какие-либо действия от имени root, а затем выйти из сеанса, то можно зарегистрироваться суперпользователем, а по завершении административных действий выйти из сеанса с помощью команды Exit. Вернуться в окно графического сеанса можно с помощью сочетания клавиш <Ctrl>+<F7>. Если вам удобно использовать текстовую консоль, часто переключаясь в нее, то регистрироваться лучше обычным пользователем, а привилегии получать командой `su` или `su -`. После ввода этих команд требуется ввод пароля суперпользователя. Вторая команда кроме повышенных прав

включает переменные окружения пользователя root, подключая и его домашний каталог по умолчанию. Обычно для вызова многих программ в таком случае не требуется указывать полный путь к ним.

Возможность открыть консольный сеанс есть и прямо в графическом режиме работы. Для этого служит программа `terminal` или `x-terminal`, меню вызова которых в различных дистрибутивах Linux может иметь некоторые отличия. В CentOS с установленным менеджером окон KDE путь вызова консоли — **Главное меню | Система | Терминал**. Еще один способ вызвать окно консоли — **Главное меню | Выполнить программу** и в единственное поле открывшегося окна ввести имя файла программы (иногда требуется полный путь). Имя файла программы может отличаться от названия программы, и для вызова окна терминала необходимо ввести команду `console` (рис. 3.1) и нажать кнопку **Выполнить.**

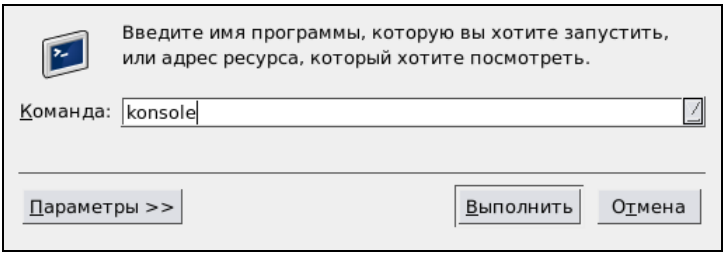


Рис. 3.1. Окно Выполнить команду

Окно **Выполнить программу** может быть развернуто с помощью кнопки **Параметры**. При этом появится возможность указать дополнительные параметры запуска, например пользователя и пароль, от имени которого будет запущена программа. На рис. 3.2 показано вызванное окно консоли, в котором выполнены команды перехода от рядового пользователя к пользователю root в двух описанных выше вариантах.

Окно терминала в графическом режиме может иметь несколько вкладок, в каждой из которых может быть открыт отдельный консольный сеанс.

Таким образом, в вашем распоряжении несколько способов открыть сеанс суперпользователя, и не один. Это позволяет одновременно выполнять несколько программ и наблюдать за результатом их выполнения. Некоторые команды приводят к выводу на экран динамической информации, и пока идет выполнение такой команды, вы не можете выполнить другую в том же сеансе. Например, если выполнить команду `top`, будет выводиться перечень процессов, которые отсортированы по используемым ими ресурсам (рис. 3.3).

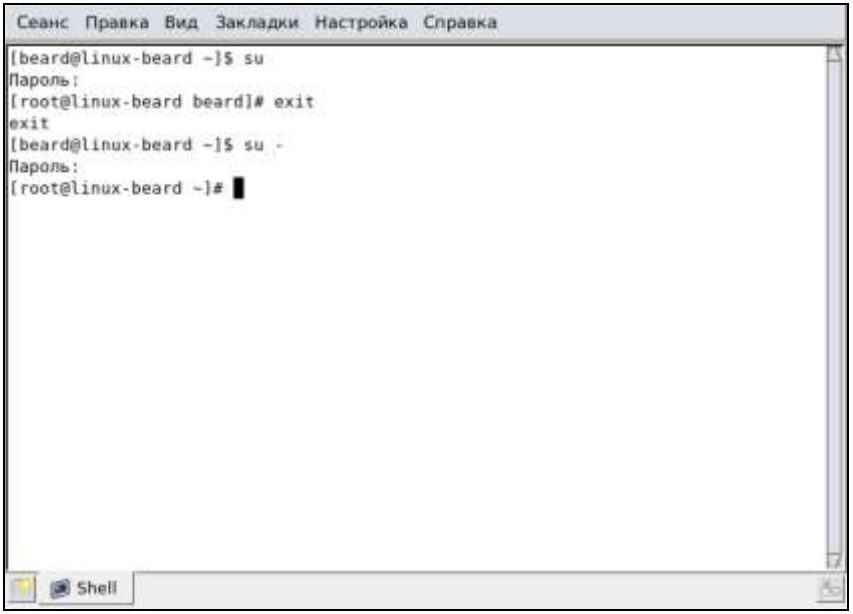


Рис. 3.2. Окно **Konsole**

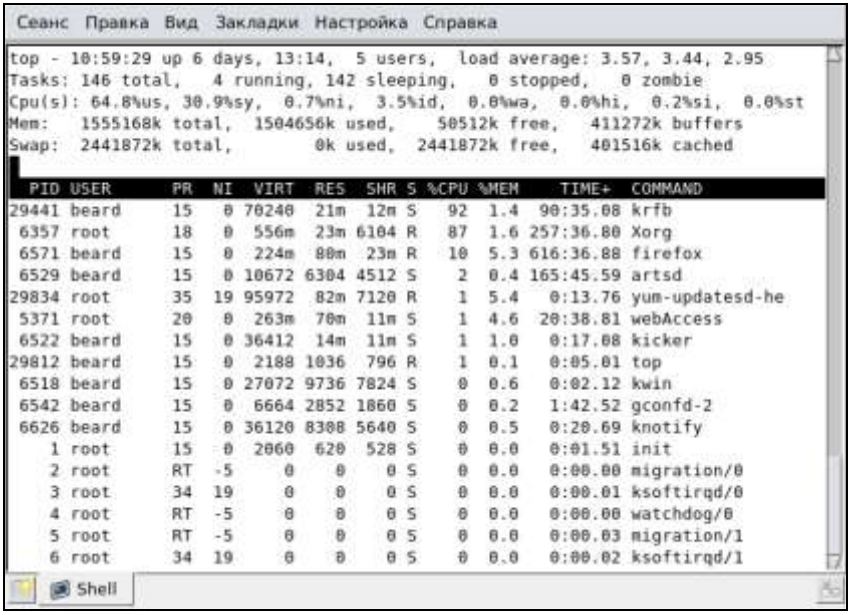


Рис. 3.3. Окно **Konsole** с выполняемой командой `top`

Также до остановки пользователем может выполняться команда `ping` и многие другие. Остановить выполнение таких команд можно сочетанием клавиш <Ctrl>+<C>.

Пользуясь окном терминала, вы можете выполнять практически все действия, необходимые администратору компьютера. Создавать и удалять учетные записи пользователей, назначая им права в системе, создавать и удалять группы пользователей, создавать и удалять каталоги и файлы, назначая права доступа к ним, управлять сетевыми подключениями, организовать защиту рабочей станции по сети… Невозможно перечислить все задачи администратора рабочей станции, которые можно выполнить в окне терминала. Окно терминала позволяет выполнять все задачи администратора. Тем не менее, часто хотелось бы более наглядных средств администрирования рабочей станции. И такие средства в Linux есть. От версии к версии они могут довольно существенно отличаться, но логика их работы всегда одна и та же. Рассмотрим некоторые возможности администрирования и управления рабочей станцией Linux с использованием графических средств. Наиболее распространенные операции по управлению и администрированию рабочих станций заключаются в следующем.

- ❒ Настройка параметров экрана
- ❒ Управление учетными записями пользователей
- ❒ Настройка параметров сети, включая брандмауэр или firewall, доступ в Интернет и настройка общего доступа к подключению Интернета
- ❒ Настройка доступа к ресурсам рабочей станции из сети
- ❒ Настройка доступа к ресурсам сети
- ❒ Настройка печати

Конечно, это не все возможные процедуры управления и администрирования рабочей станции. С другими процедурами вы сможете ознакомиться и справиться самостоятельно по аналогии с описанными ниже.

Настройка параметров экрана

Рассмотрим эту процедуру в Mandriva Linux с установленным менеджером экрана KDE. Для доступа к настройкам параметров экрана перейдите по следующему пути **Меню** | **Утилиты** | **Системные** | **Центр управления**.

Здесь можно выбрать темы оформления и собственно параметры экрана. Для изменения темы оформления (вид окон и меню) выберите в левой части открывшегося окна **Центр управления** (рис. 3.4) раздел **Внешний вид и темы**. Развернув меню этого раздела, вы увидите несколько полезных пунктов меню, первый из которых — **Декорации окон**.

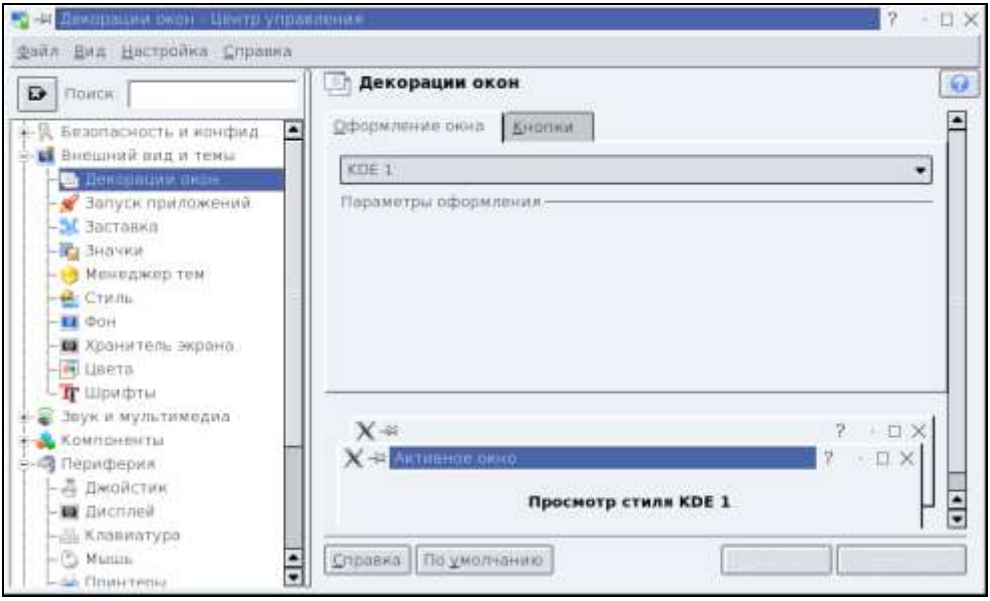


Рис. 3.4. Окно **Декорации окон — Центр управления**

Здесь можно абсолютно безопасно экспериментировать и выбирать наиболее подходящий вам вариант настроек внешнего вида окон и самого рабочего стола.

Перейдя к разделу **Периферия** и выбрав пункт **Дисплей** (рис. 3.5), можно настроить параметры дисплея, переходя по вкладкам и выбирая необходимые значения параметров. На рисунке показана вкладка **Питание**, где можно настроить режим энергосбережения или выключить его. На вкладке **Размер и ориентация** есть возможность подкорректировать параметры дисплея.

Выполненные вами изменения сохраняются только для текущего пользователя. Но, как и в других версиях Linux, более глубокие настройки дисплея, включая выбор и изменение драйвера, возможны в другом окне. Перейдите к Центру управления Mandriva Linux по пути **Меню | Утилиты | Системные | Настройка компьютера**. Скорее всего, система попросит вас авторизоваться в качестве администратора компьютера (ввести пароль пользователя root). В открывшемся после авторизации окне **Центр управления Mandriva Linux** (рис. 3.6) выберите раздел **Оборудование**.

Для настройки параметров дисплея в правой части окна найдите значок **Настройка графического сервера** и щелчком мыши по нему откройте соответствующее окно (рис. 3.7).

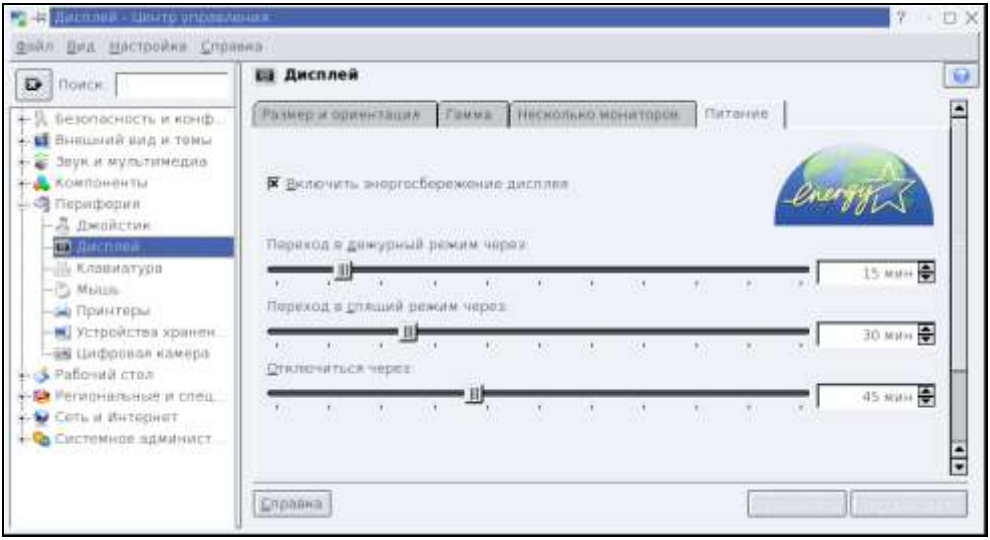


Рис. 3.5. Окно **Дисплей — Центр управления**

Рис. 3.6. Окно **Центр управления Mandriva Linux**

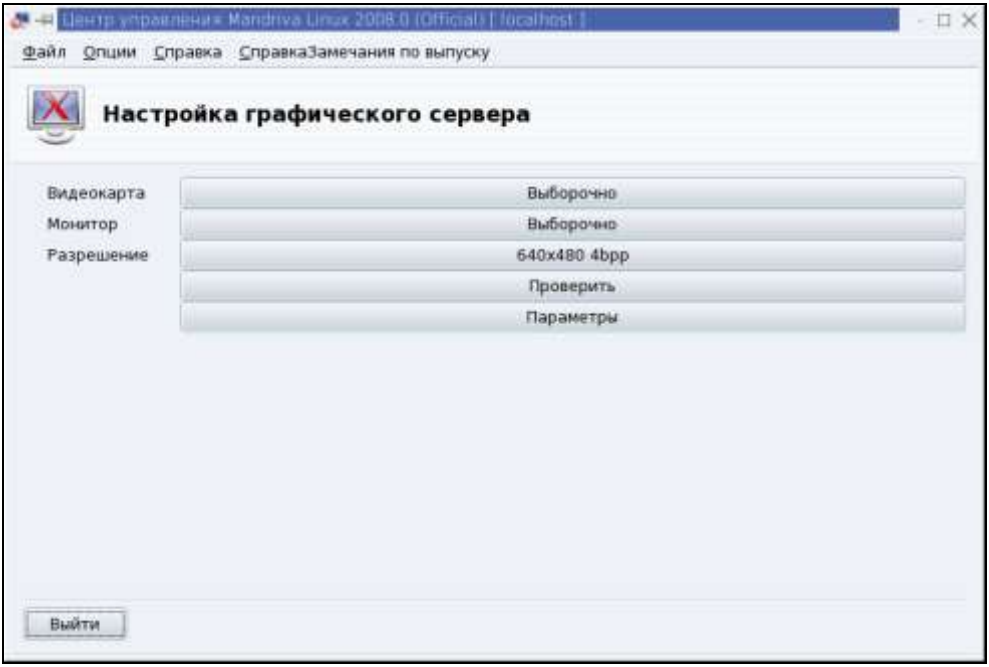


Рис. 3.7. Раздел **Настройка графического сервера** центра управления Mandriva Linux

Здесь вы можете изменить разрешение экрана и драйвер монитора и видеокарты. После внесенных изменений есть возможность проверить работоспособность видеосистемы с данным сочетанием параметров. Если после нажатия кнопки **Проверить** вы увидите изображение экрана, то настройки можно сохранить. Если будет выведено сообщение об ошибке, то выбранное сочетание параметров не поддерживается системой. В некоторых версиях Linux выбор несовместимого сочетания параметров может быть сохранен… В этом случае ситуацию может спасти только обращение к терминальному режиму.

Набрав в окне терминального сеанса команду `xvidtune`, вы увидите текстовое окно программы xvidtune (рис. 3.8), в котором можно изменить настройки графического сервера.

Программу следует запускать от имени суперпользователя. Кнопка **Test** служит для проверки корректности настроек, а кнопка **Show** — для их сохранения в конфигурационный файл. Конфигурационные файлы видеосервера в разных версиях Linux могут иметь отличающиеся имена. При желании вы можете познакомиться с возможностями настройки с помощью редактирования конфигурационных файлов в статьях по адресам в Интернете **http://zero.kanet.ru/site/index.php?page=12** и **http://noteslinux.blogspot.com/**

2008/07/xorgconf.html. Для первого знакомства с конфигурационными файлами видеосервера этих статей достаточно, а мы продолжим рассмотрение графических средств настройки рабочей станции.

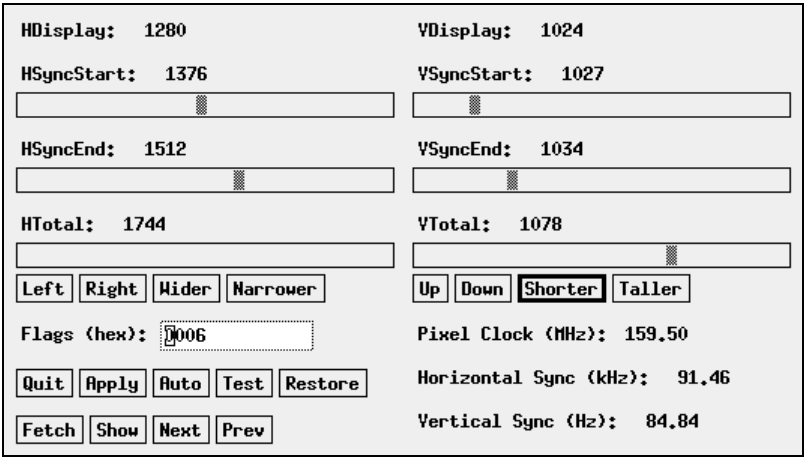


Рис. 3.8. Окно настройки графического сервера в терминальном режиме

Управление учетными записями пользователей

Первая учетная запись обычного пользователя создается еще во время инсталляции системы. Но в процессе работы с компьютером может потребоваться создание других учетных записей. Для управления учетными записями в Mandriva Linux откройте центр управления Mandriva Linux (**Меню** | **Утилиты** | **Системные** | **Настройка компьютера**) и перейдите в раздел **Система** (рис. 3.9).

Найдите в нем значок **Управление пользователями** и щелкните по нему мышью.

В открывшемся окне **Пользователи и группы** (рис. 3.10) вы увидите список уже существующих пользователей. Скорее всего, вы увидите только одну учетную запись. Для того чтобы увидеть всех системных пользователей, надо в меню **Действия** снять отметку напротив пункта **Отфильтровать системных пользователей**. Идентификаторы обычных пользователей как правило начинаются с 500. Меньшие идентификаторы соответствуют системным пользователям. Редактировать системных пользователей обычно не требуется, но некоторые программы при установке создают учетные записи пользователей, которые необходимы для верного распределения прав.

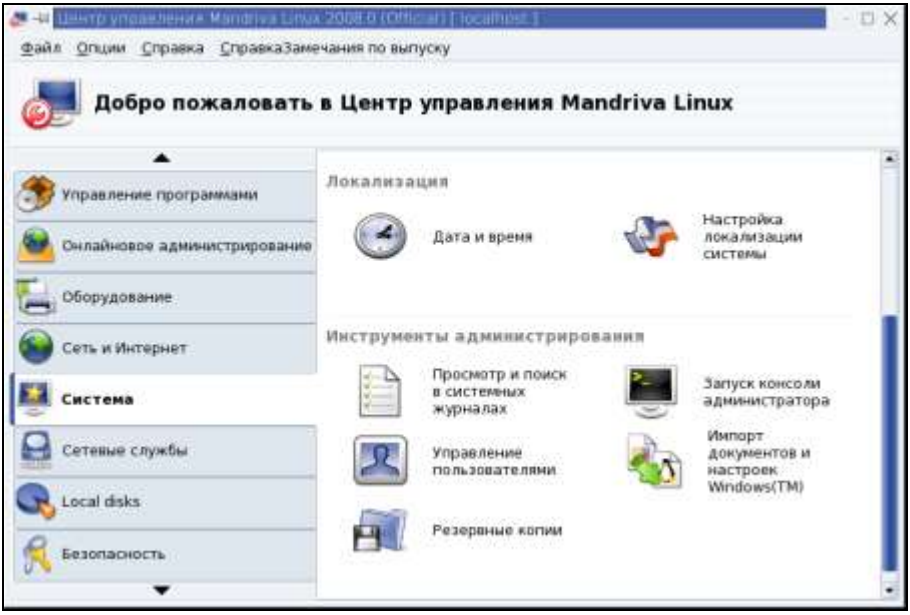


Рис. 3.9. Раздел **Система** центра управления Mandriva Linux

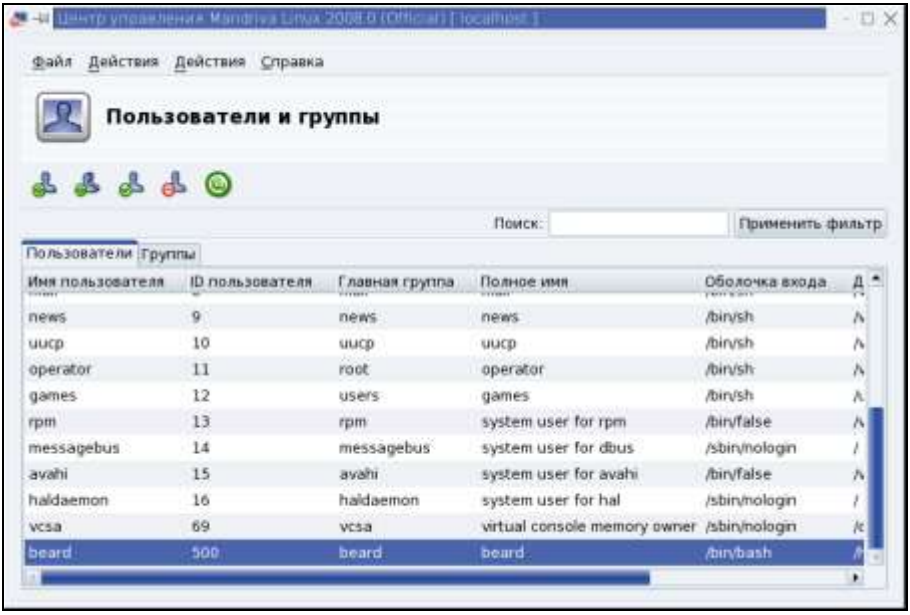


Рис. 3.10. Раздел **Пользователи и группы** центра управления Mandriva Linux

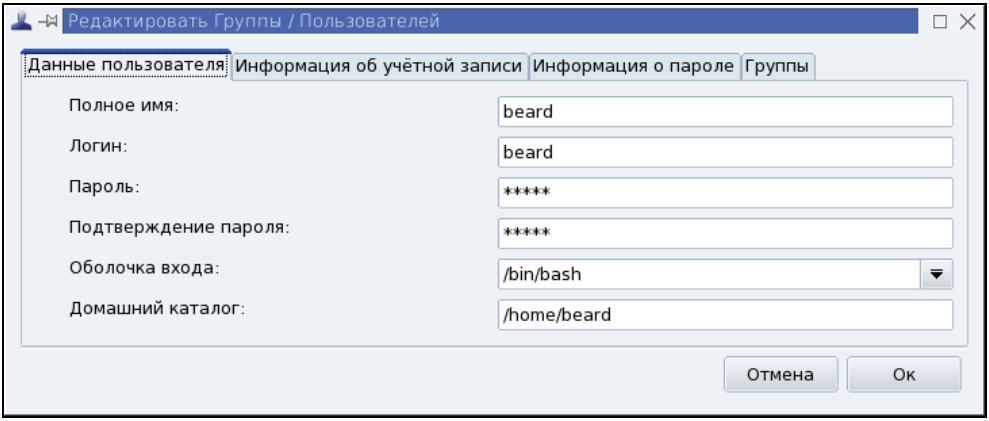


Рис. 3.11. Окно **Редактировать Группы / Пользователей**

Например, такого пользователя создает для себя сервер баз данных MySQL. Создать новую учетную запись просто — достаточно выбрать в меню **Действия** пункт **Добавить пользователя**. После этого необходимо внести некоторый минимум сведений об учетной записи, которые потребует система. Впоследствии, воспользовавшись меню **Действия** | **Редактировать**, вы можете изменить свойства выделенной учетной записи в окне **Редактировать Группы / Пользователей** (рис. 3.11).

Исследуйте самостоятельно средства работы с учетными записями пользователей Linux. Вы увидите много сходства с возможностями управления учетными записями пользователей в Windows, но обнаружите и отличия. Так, например, в Linux есть возможность выбора оболочки входа пользователя. По умолчанию используется оболочка bash, но существуют и другие, узнать о которых можно из статьи по адресу **http://www.opennet.ru/base/dev/linux_shells.txt.html**.

Настройка параметров сети и доступа в Интернет

Это одна из важнейших функций администрирования рабочей станции. Без локальной сети и без Интернета опытный пользователь компьютера чувствует себя крайне не уютно. Но работая в локальной сети и подключившись к Интернету, нельзя забывать о защите информации. Если вирусов для Linux практически нет, любителей порыться в чужих файлах всегда хватает, поэтому предусмотреть хотя бы самые простые средства защиты необходимо.

На этот раз рассмотрим пример настройки параметров сети в операционной системе CentOS с установленной графической оболочкой KDE. В Mandriva Linux вы без труда сможете найти соответствующие инструменты настройки

после рассмотрения данного примера. В CentOS нет такого удобного центра управления, как в Mandriva Linux. Тем не менее, настроить сеть для рабочей станции не сложно.

Переходим по пути **Меню | Администрирование | Сеть**, затем вводим пароль суперпользователя и получаем окно **Настройка сети** на экране монитора (рис. 3.12).

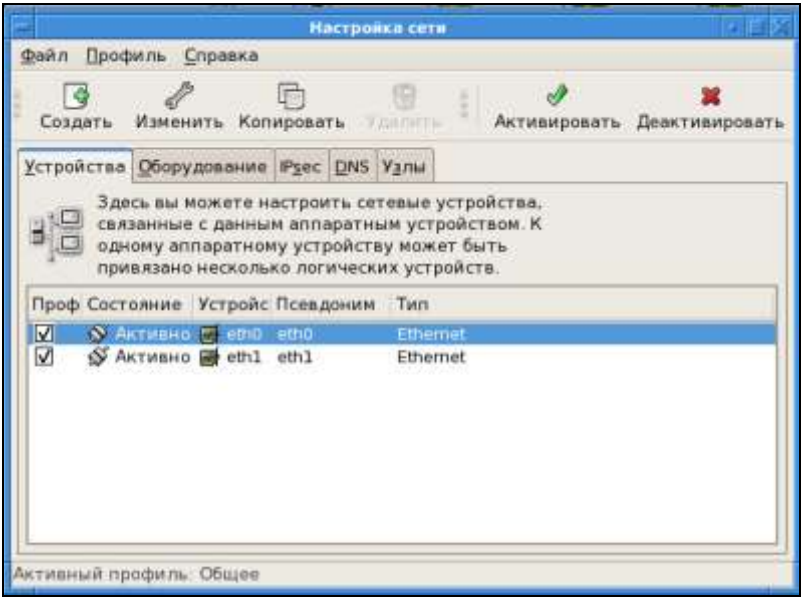


Рис. 3.12. Окно **Настройка сети**. Вкладка **Устройства**

В Linux все устройства имеют специальные обозначения. Сетевые адаптеры не исключение и обозначаются как eth*N*, где *N* — номер. Отсчет номеров устройств начинается с нуля. Первый сетевой адаптер обозначается как eth0, второй — eth1 и так далее. На вкладке **Оборудование** (рис. 3.13) можно увидеть, какие именно сетевые карты соответствуют нашим устройствам. На этой вкладке можно назначить имя устройству, соответствующему определенному экземпляру оборудования.

Настройки можно выполнять только для устройства. Выделив необходимую строку на вкладке **Устройства** и нажав кнопку **Изменить** (с изображением гаечного ключа), можно открыть окно **Устройство Ethernet** для выбранного адаптера. Два адаптера на рассматриваемой рабочей станции выполняют каждый свою задачу. Так eth0 обеспечивает связь с внутренней локальной сетью 10.20.1.1/24 (рис. 3.14), а eth1 — с внешней сетью 192.168.1.0/24 с выходом в Интернет через шлюз 192.168.1.1 (рис. 3.15).

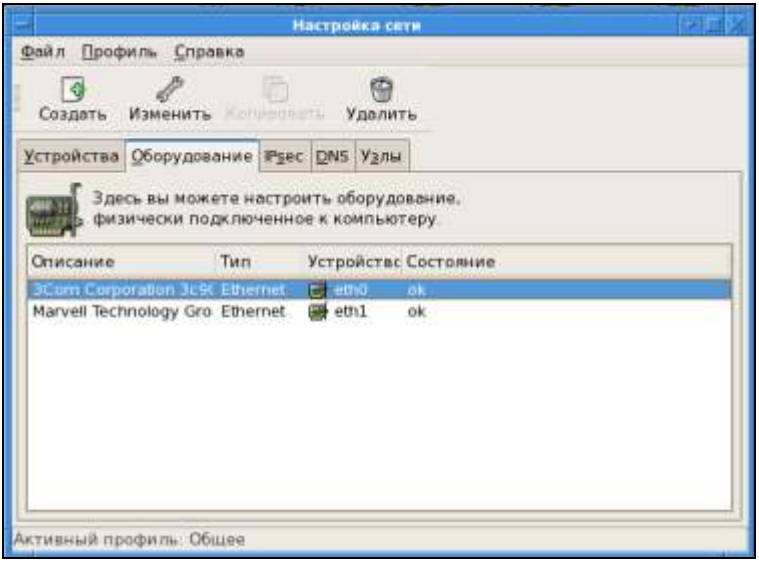


Рис. 3.13. Окно **Настройка сети**. Вкладка **Оборудование**

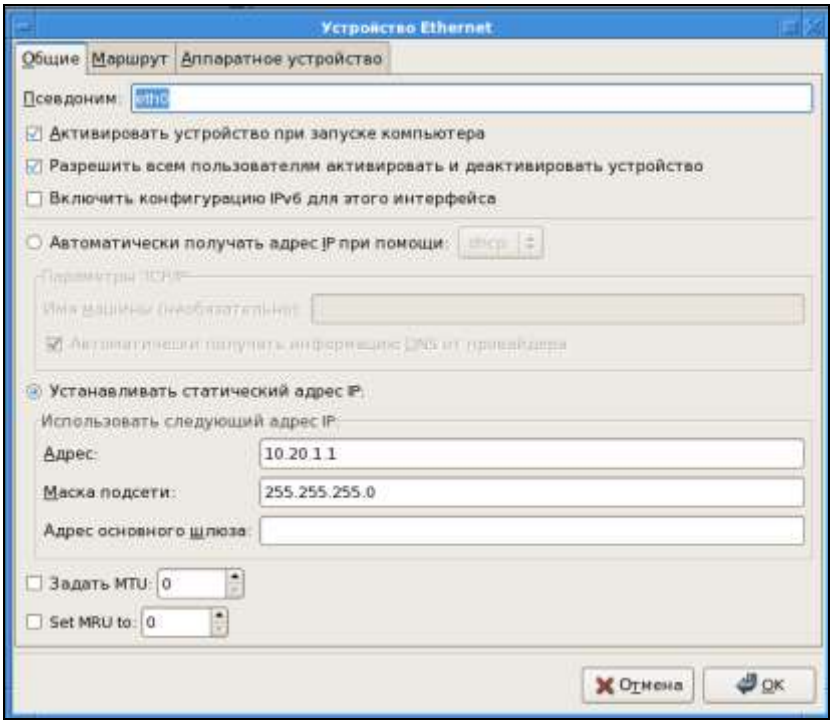


Рис. 3.14. Окно **Устройство Ethernet** (eth0)

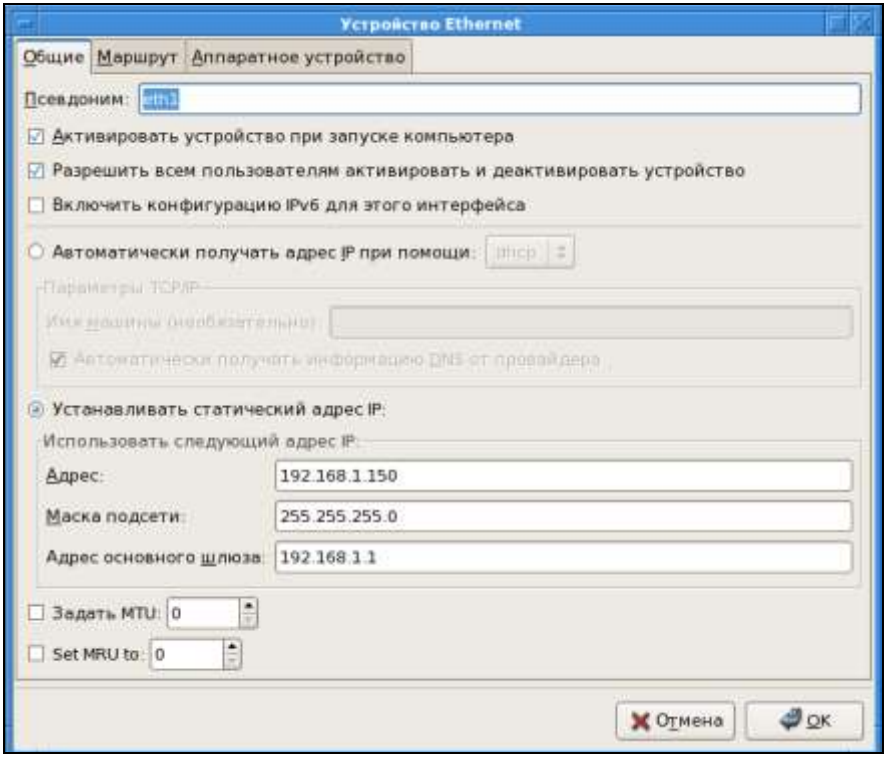


Рис. 3.15. Окно **Устройство Ethernet** (eth1)

Такая конфигурация сети позволяет использовать эту рабочую станцию в качестве шлюза в Интернет для сети 10.20.1.1/24. Для этого достаточно в окне терминала от имени root выполнить три команды, которые для удобства можно включить в исполняемый файл. Команды нужны следующие:

- `modprobe iptable_nat` — для активации модуля ядра, который отвечает за преобразование сетевых адресов;
- `iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE` — указание на то, что на интерфейсе eth1 должно осуществляться преобразование адресов и перенаправление пакетов;
- `echo "1" > /proc/sys/net/ipv4/ip_forward` — разрешение маршрутизации пакетов между сетевыми интерфейсами рабочей станции.

Теперь, когда внутренняя сеть получила возможность выхода в Интернет, стоит подумать о защите. Условно будем считать внутреннюю сеть безопасной и защищаться будем от возможных проникновений из внешней сети 192.168.1.0/24 и Интернета.

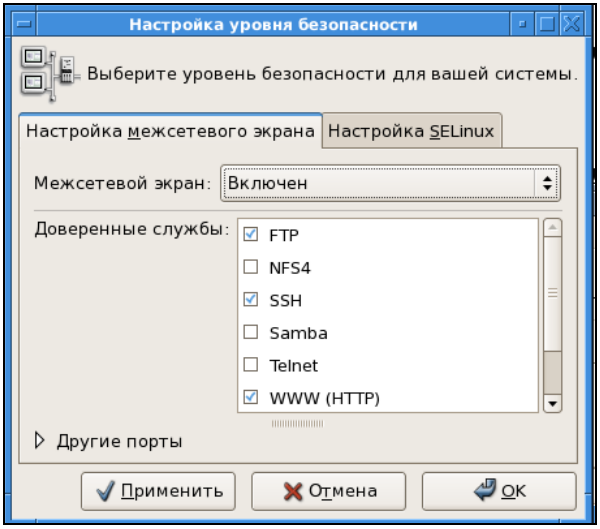


Рис. 3.16. Окно **Настройка уровня безопасности**

Защитить рабочую станцию можно, настроив межсетевой экран. Для этого пройдите по пути **Меню** | **Администрирование** | **Уровень безопасности и сетевой экран** и установите необходимые опции в окне **Настройка уровня безопасности** (рис. 3.16), разрешив доступ к рабочей станции для отдельных портов, служб и сервисов.

К сожалению, и здесь не обойтись без использования консоли (терминала), если необходимо установить различный уровень защиты по разным сетевым интерфейсам. Внутреннюю сеть мы считаем безопасной и не стремимся защититься от нее, а если для нее необходимо обеспечить свободный доступ для какой-либо службы, то автоматически доступ будет открыт и для внешней сети. Чтобы избежать этого, придется прописывать правила для firewall. Пример настройки с использованием подготовленного заранее исполняемого файла можно посмотреть в разделе "Настройка брандмауэра" в статье по адресу в Интернете **http://sys-adm.org.ua/www/squid-transparent.php**. В исполняемый файл записывается набор команд `iptables`, необходимых для создания правил брандмауэра. После выполнения всех команд брандмауэр будет настроен. Если ваша рабочая станция имеет только один сетевой адаптер, то возможностей графического интерфейса для настройки брандмауэра вполне достаточно.

В некоторых версиях Linux, например OpenSUSE или SLES, графический интерфейс предоставляет более широкие возможности для настроек брандмауэра.

Настройка доступа к ресурсам рабочей станции из сети

Если брандмауэр разрешает доступ к рабочей станции по протоколу Samba, это не значит, что сам доступ к файлам и принтерам возможен. Необходимо настроить службу Samba на рабочей станции.

> ***Примечание***
>
> Есть и другие протоколы и службы для предоставления доступа к файлам. Но здесь мы рассматриваем только те протоколы и службы, которые совместимы с сетями под управлением Windows.

Еще в процессе установки системы можно было выбрать сервер и клиент Samba. Эти компоненты обязательно присутствуют в любом дистрибутиве Linux и их установка не должна вызывать никаких проблем. Графические средства настройки сервера Samba в различных версиях Linux могут отличаться числом настраиваемых функций. Могут быть включены настройки доступа к принтерам, к каталогу имен LDAP, но суть процедуры настройки всегда одинакова. Окно настройки сервера Samba в CentOS показано на рис. 3.17. Графические средства настройки Samba в CentOS содержат необходимый минимум возможностей файлового сервера небольшой сети. **Меню | Администрирование | Настройка сервера | Samba** — по этому пути можно вызвать показанное на рисунке окно.

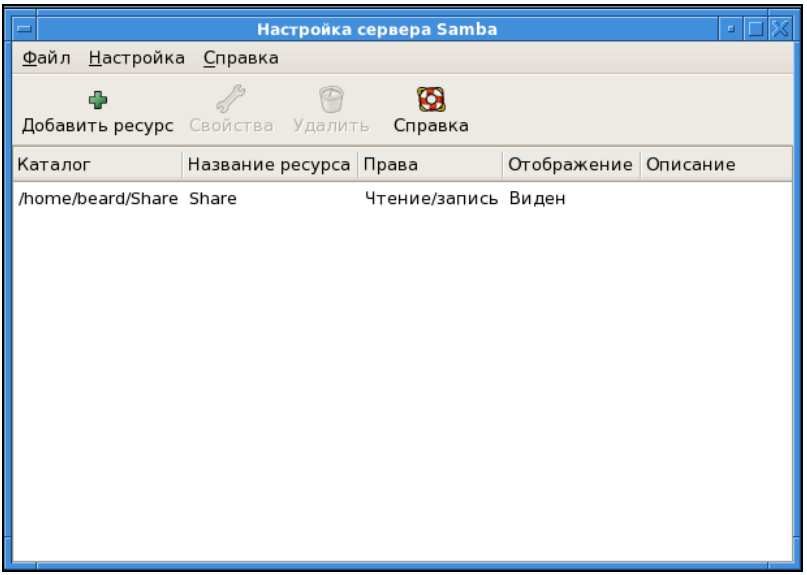


Рис. 3.17. Окно **Настройка сервера Samba**

Выбрав в меню окна **Настройка | Параметры сервера** и в открывшемся окне (рис. 3.18) вкладку **Основной**, можно указать имя рабочей группы, в которой работают компьютеры вашей сети, и описание сервера. По умолчанию указана рабочая группа mygroup, а в описании сервера — его текущая версия.

На вкладке **Безопасность** этого окна (рис. 3.19) следует указать режим аутентификации. Для небольшой сети вполне может подойти режим **Ресурс**. В этом режиме доступ к папкам и принтерам определяется разрешениями, которые установлены в системе. Шифрование паролей повышает безопасность в сети, поэтому можно указать **Да**, согласившись с этой возможностью. Для доступа к ресурсам пользователей, которые не имеют учетных записей на вашей рабочей станции, должна быть указана учетная запись, права которой будут получать гости. Можно создать отдельную учетную запись и давать ей права на все открываемые для доступа ресурсы.

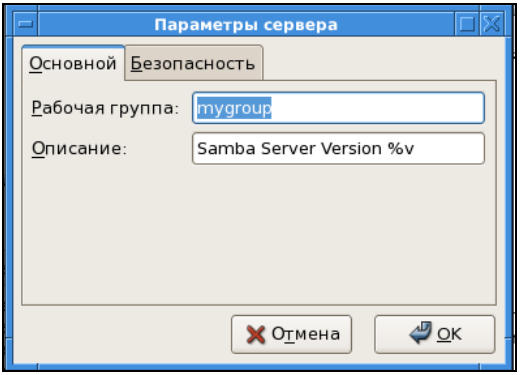


Рис. 3.18. Окно **Параметры сервера**

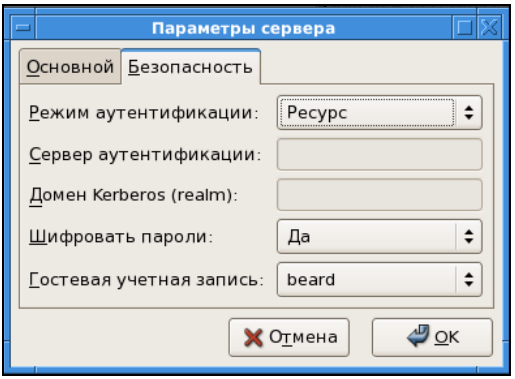


Рис. 3.19. Окно **Параметры сервера**. Вкладка **Безопасность**

По пути **Настройка | Пользователи Samba** можно вызвать окно **Пользователи Samba** (рис. 3.20). В этом окне показан список уже существующих пользователей, а также есть возможность управления учетными записями.

Для каждой учетной записи пользователей Samba необходимо указать пароль доступа к ресурсам сервера (рис. 3.21). Этот пароль не обязательно совпадает с паролем учетной записи в системе. Более того, для учетной записи может не быть разрешения входа в систему, но доступ к ресурсам Samba может быть открыт.

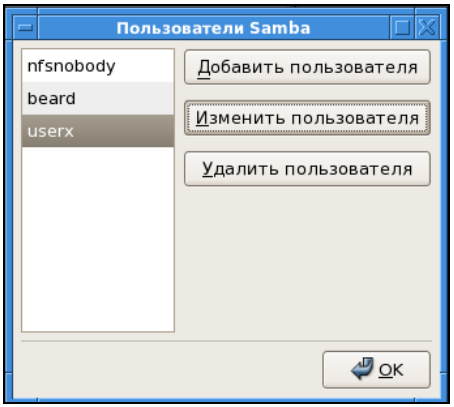


Рис. 3.20. Окно **Пользователи Samba**

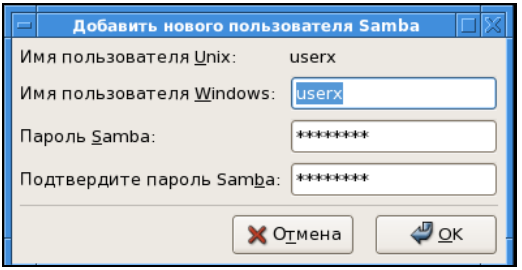


Рис. 3.21. Окно **Добавить нового пользователя Samba**

Нажав кнопку **Добавить ресурс** в окне **Настройка сервера Samba** (рис. 3.17), можно вызвать окно **Создать ресурс Samba** (рис. 3.22), в котором с помощью кнопки **Обзор** следует выбрать каталог, к которому предполагается открыть доступ, указать название ресурса, под которым он будет виден в сети, ввести описание ресурса. Описание также будет показано сетевым пользователям.

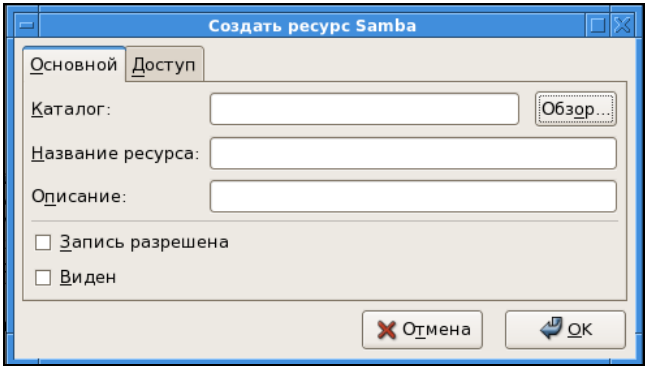


Рис. 3.22. Окно **Создать ресурс Samba**

В этом же окне можно указать разрешение записи в каталог и возможность видеть его в средствах просмотра сети. Вполне вероятно, что вы не хотите предоставлять пользователям возможность видеть каталог, но при точном знании его сетевого имени они могут войти в него. На вкладке **Доступ** можно выбрать пользователей, для которых разрешен доступ, или предоставить его всем пользователям.

Как видим, возможностей много. Конкретный вариант настроек зависит от ваших потребностей.

Настройка доступа к ресурсам сети

Эта процедура очень похожа во всех версиях Linux. Встречаются некоторые особенности, присущие определенным дистрибутивам, но в общем случае доступ обеспечивается обозревателями сети, а также простым вводом адреса ресурса в адресную строку файлового менеджера.

На рис. 3.23 приведено окно Браузер Konqueror в Mandriva Linux, в адресной строке которого введен адрес ресурса Samba на компьютере с CentOS. Как обычно, адрес начинается с указания протокола (smb), а перед IP-адресом компьютера или его именем указывается имя учетной записи пользователя и знак @. Если для доступа требуется пароль, то система его запросит.

Пользователи Windows в вашей сети тоже могут получить доступ к ресурсам Samba. На рисунке рис. 3.24 приведено окно обозревателя файлов Windows Vista, в адресной строке которого указано имя компьютера и имя ресурса Samba. Имя компьютера может быть заменено на его IP-адрес. Обратите внимание, что слеши в адресе обратные, это одно из отличий Windows от Linux.

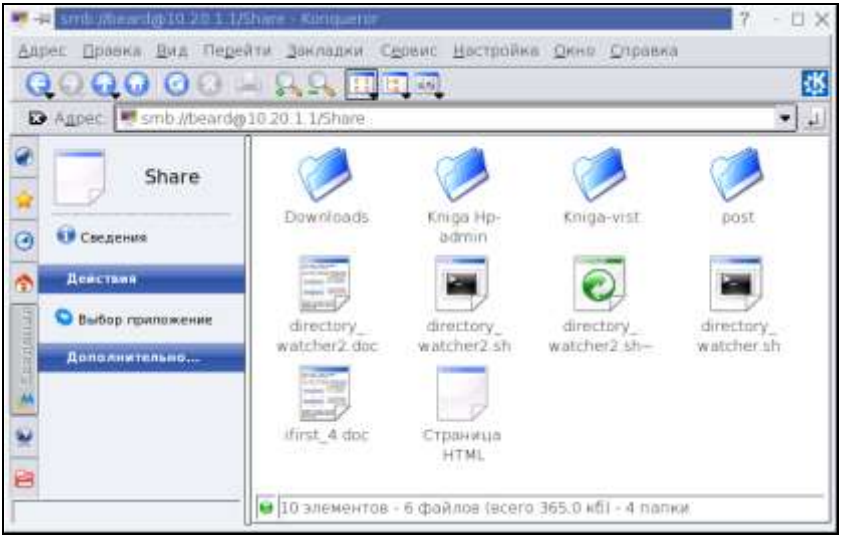


Рис. 3.23. Браузер Konqueror в Mandriva Linux

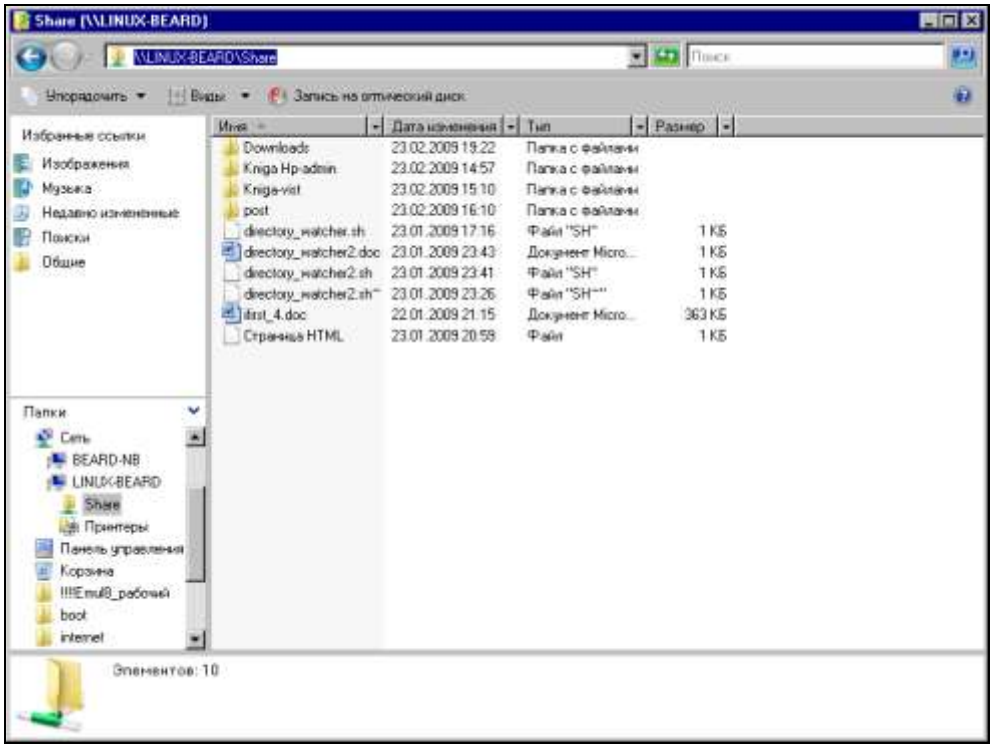


Рис. 3.24. Windows Explorer

Webmin

Для объединения всех средств администрирования компьютера в одно разработан программный комплекс Webmin (**http://webmin.com**), который позволяет администрировать UNIX-подобную операционную систему, не притрагиваясь к командной строке и не помня ни одной команды. Все управление сервером происходит через веб-интерфейс. Webmin состоит из веб-сервера и небольшого количества скриптов, которые собственно и осуществляют связь между приказаниями владельца компьютера через веб-интерфейс и их исполнением на уровне операционной системы и прикладных программ. Webmin написан полностью на языке Perl и не использует никаких дополнительных нестандартных модулей. Простота, легкость и быстрота выполнения команд — одно из самых больших преимуществ данной панели управления.

Webmin бесплатно распространяется для коммерческого и некоммерческого использования. Именно благодаря этому вокруг Webmin сложился мощный пласт сторонних добровольных помощников-программистов, которые дописывают данную программу, исправляют неудачные места, пишут дополнительные модули, производят перевод на другие языки. Благодаря этому Webmin оброс большой функциональностью, огромным количеством подключаемых модулей и переведен практически на все европейские языки, включая русский.

Уже рассмотренные выше настройки, выполненные с помощью графических средств Linux, могли быть выполнены и через веб-интерфейс. Мы не будем подробно рассматривать все возможности Webmin. Это средство обычно не включено в дистрибутивы по умолчанию, но может быть установлено дополнительно. Программный комплекс может быть установлен из окна терминала путем ввода следующих команд:

```
# cd /usr/local/src
# wget http://prdownloads.sourceforge.net/webadmin/
webmin-1.400-1.noarch.rpm
# rpm -U webmin-1.400-1.noarch.rpm
```

По первой команде изменяем текущую директорию на папку, в которую сохраним установочный пакет.

Вторая команда — запуск программы `wget`. Это прекрасное средство для загрузки файлов из Интернета. Оно не требует графического интерфейса, поскольку очень просто в использовании. Версию пакета для загрузки проверьте на сайте **http://webmin.com** и укажите актуальную на данный момент.

Третьей командой выполним установку Webmin. Версию пакета укажите актуальную.

По окончании процедуры установки достаточно в браузере ввести адрес **http://localhost:1000**, и вы увидите страницу авторизации Webmin (рис. 3.25).

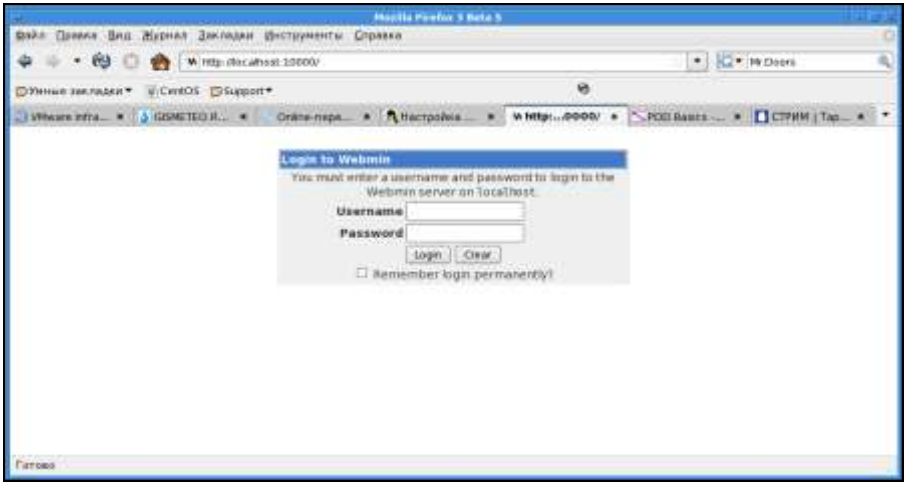


Рис. 3.25. Окно браузера со страницей авторизации Webmin

Рис. 3.26. Окно браузера. Средства настройки системы программного комплекса Webmin

После авторизации в качестве суперпользователя вы получите все права для настройки системы и сможете воспользоваться для этого средствами Webmin (рис. 3.26).

На рисунке показана страница настройки сервера Samba, который мы только что настроили. Как видите, здесь возможностей существенно больше. Скорее всего, вы проведете не один час в изучении возможностей Webmin. Если какого-либо модуля системы, который вас заинтересовал, нет на вашем компьютере, то программа при попытке перейти к его настройке предложит установить его.

Веб-интерфейсы очень удобны для проведения настроек программ и управления ими. В Linux есть такие интерфейсы, которые входят в дистрибутивы по умолчанию. Один из таких стандартных интерфейсов — средство настройки системы печати.

Настройка печати

Для работы с принтерами в Linux наибольшее распространение получила система печати CUPS — Common UNIX Printing System (**http://www.cups.org**). Создавать принтеры и очереди печати, управлять ими очень удобно, воспользовавшись веб-интерфейсом CUPS. Для этого достаточно ввести в адресной строке браузера **https://localhost:631** (рис. 3.27). К сожалению, веб-интерфейс CUPS не имеет пока перевода на русский язык, но по адресу **http://wiki.archlinux.org/index.php/CUPS** можно прочитать руководство на английском, русском, польском и китайском языке. Здесь мы рассмотрим только процедуру установки принтера, как самую необходимую для обеспечения возможности выполнять печать документов.

Перейдя на вкладку **Administration** (администрирование), найдите кнопку веб- (добавить принтер) и нажмите ее (рис. 3.28). В полях ввода на открывшейся странице **Add New Printer** (рис. 3.29) введите информацию об устанавливаемом принтере. Здесь можно вписать все, что вам заблагорассудится. На дальнейшую работу принтера записи не повлияют, но в системе принтер будет описан с именем, расположением и описанием, которые вы внесли.

После нажатия кнопки **Continue** откроется страница **Device URL for <имя_принтера>** (рис. 3.30). Следует выбрать вариант связи с принтером. Один из наиболее распространенных способов установки принтеров в малых сетях — это принтеры с принтсервером, которые позволяют печатать на них с любого компьютера сети. В таком случае вводим `socket://<имя_или_IP-адрес_принтера>:9100`. 9100 — это порт связи с принтсервером по умолчанию.

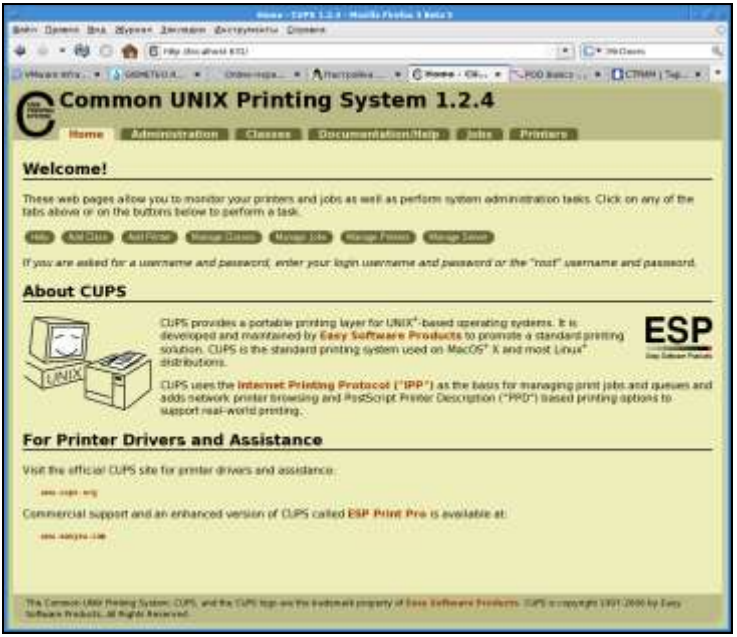


Рис. 3.27. Окно браузера с открытой главной страницей CUPS

Рис. 3.28. Вкладка **Administration** страницы CUPS

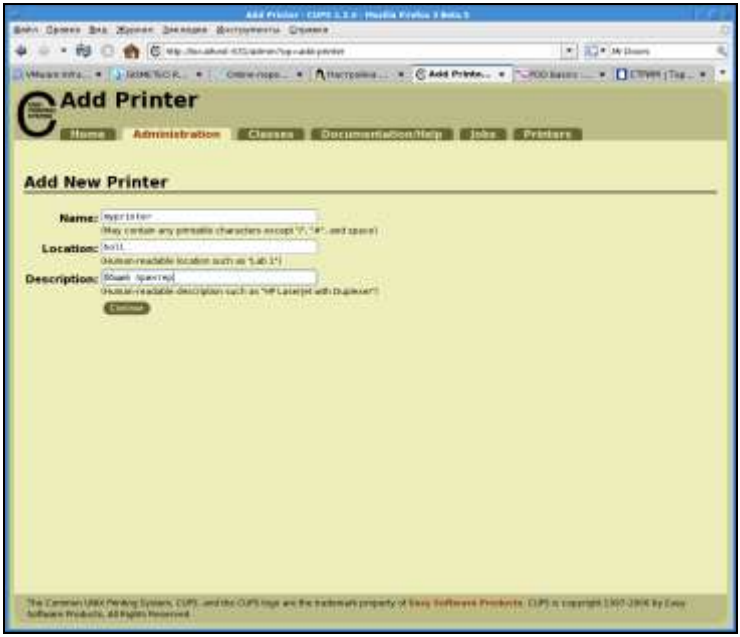


Рис. 3.29. Раздел **Add New Printer** страницы CUPS

Рис. 3.30. Пункт **Device URL for myprinter** раздела **Add Printer**

Рис. 3.31. Пункт **Model/Driver for myprinter** раздела **Add Printer**

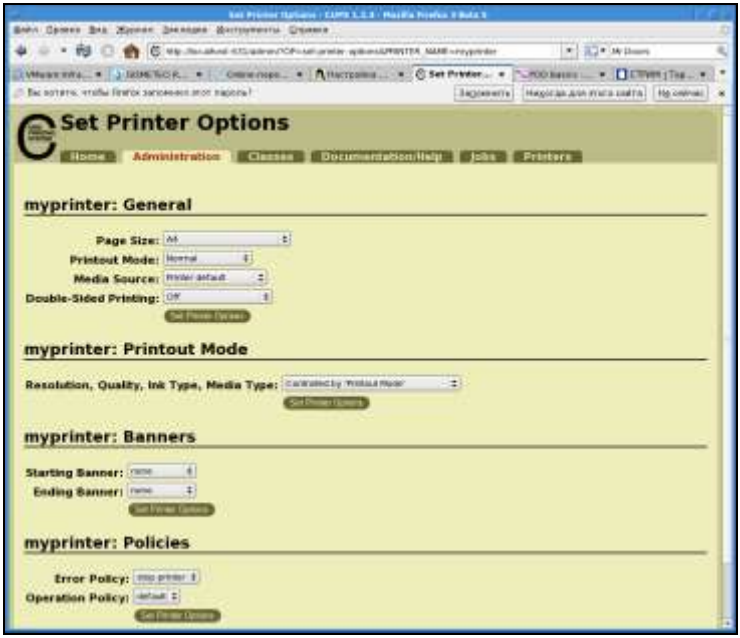


Рис. 3.32. Раздел **Set Printer Options**

На следующей странице **Model/Driver for <имя_принтера>** (рис. 3.31) необходимо выбрать драйвер принтера из предложенного системой списка или указать место расположения файла драйвера. На этом этапе потребуется авторизация в качестве суперпользователя. На этом установка принтера практически завершена.

На следующей странице (рис. 3.32) **Set Printer Options** можно установить необходимые параметры печати, которые будут использоваться по умолчанию. На вкладке **Printers** (рис. 3.33) можно увидеть все установленные принтеры, выполнить тестовую печать, управлять очередями печати, удалять и модифицировать принтеры.

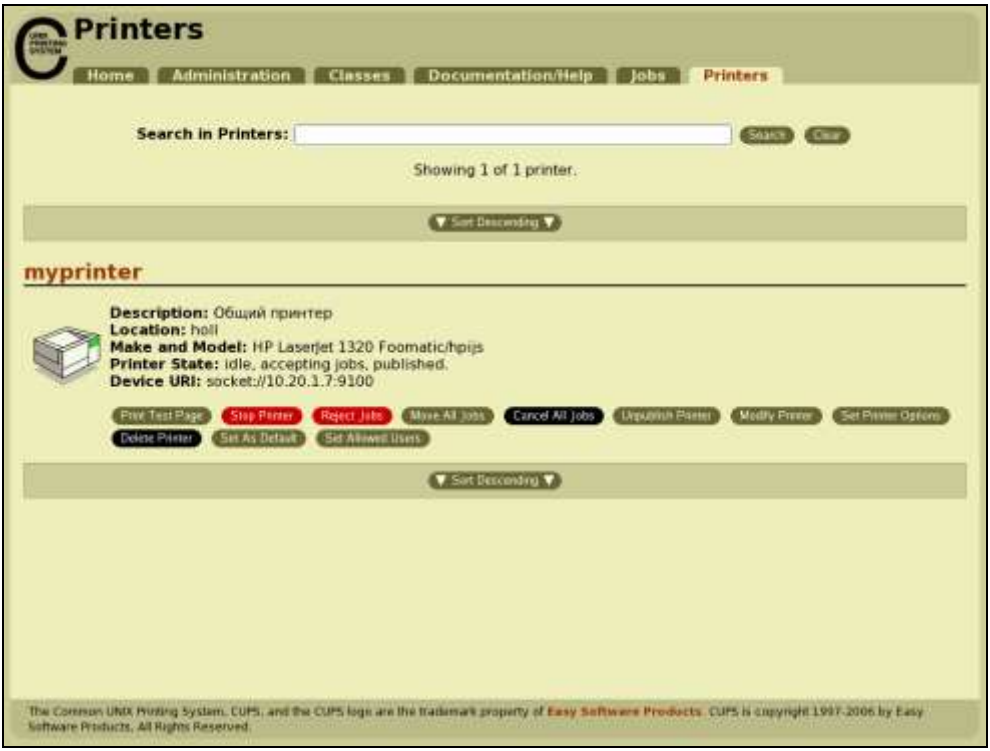


Рис. 3.33. Вкладка **Printers**

Как видим, установка принтера с помощью веб-интерфейса сервера печати CUPS не сложна. Можно в Linux найти и другие графические средства для управления принтерами, но это — самое универсальное, которое работает во всех версиях Linux одинаково.

Установка и обновление программ

Процедур установки и удаления программ в Linux несколько. В приложении можно найти команды для установки пакетов наиболее распространенных видов: RPM, YUM и DEB. Но в графический интерфейс разработчики современных дистрибутивов стараются включить удобные средства для установки и обновления программ.

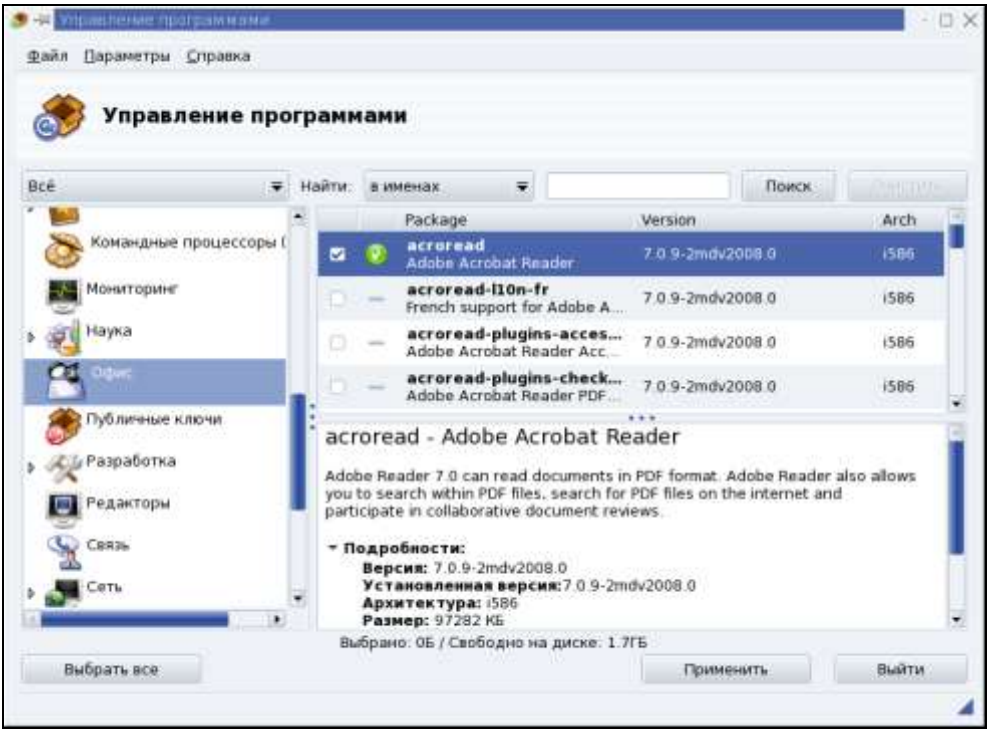


Рис. 3.34. Окно **Управление программами** в Mandriva Linux

На рис. 3.34 и 3.35 приведены изображения окон средств установки и обновления программ в Mandriva Linux и в CentOS соответственно. Несмотря на некоторые внешние отличия, суть работы с этими средствами одна и та же. Разработчики стремятся приблизить их функциональность к функциональности апплетов установки и удаления программ в Windows, но с учетом особенностей Linux. Программы для этой операционной системы могут использовать различные библиотеки функций, подобно библиотекам DLL в Windows. Разные программы могут использовать одни и те же библио-

теки. Разработчики программ для Linux пишут их для всех существующих разновидностей операционной системы, учитывая особенности каждой. Программа установки пакетов должна проверять сами пакеты и библиотеки на совместимость с теми, что уже установлены. Если обнаружена несовместимость (неудовлетворенные зависимости), система выведет предупреждение, а в ряде случаев и рекомендации о вариантах дальнейших действий.

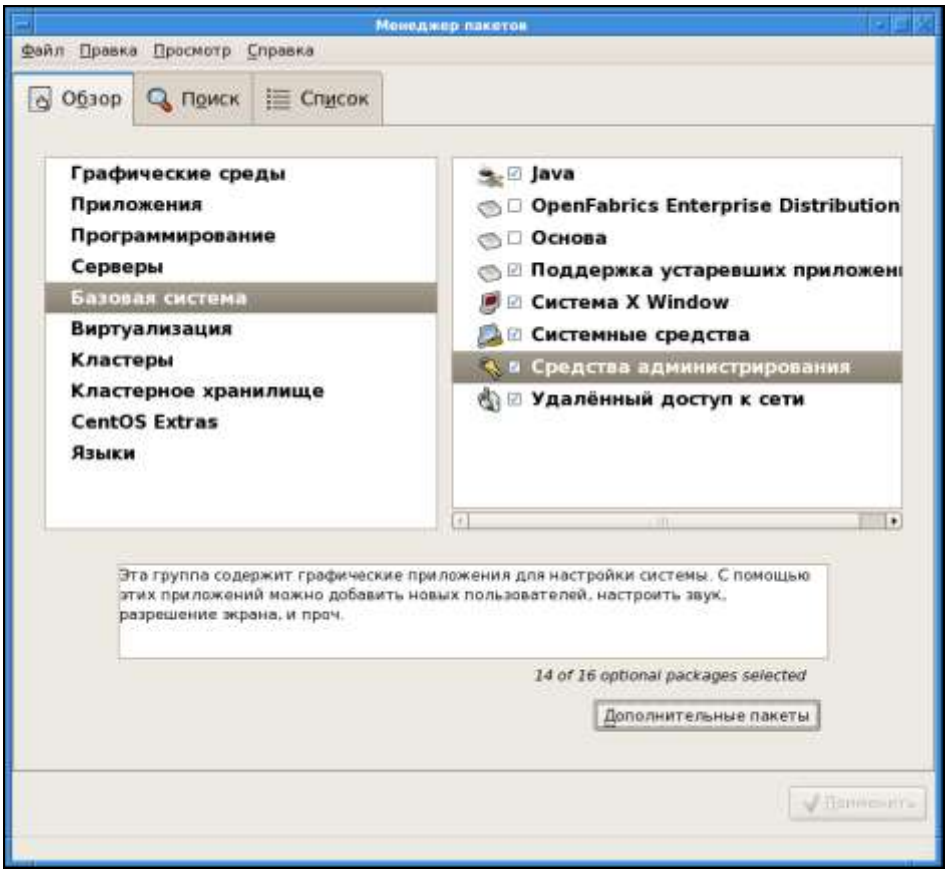


Рис. 3.35. Окно **Менеджер пакетов** в CentOS

В большинстве случаев графические средства управления программами выполняют свои функции вполне удовлетворительно, но иногда консольные средства оказываются более гибкими.

Программы для рабочей станции

Linux у вас или Windows, кроме самой операционной системы неплохо иметь еще и полезные программы, например офисный пакет. Для Windows существует Microsoft Office, Microsoft Works, а также OpenOffice.org и другие менее распространенные пакеты. Для Linux наиболее распространены StarOffice, KOffice, OpenOffice.org. Как видим, применяя OpenOffice.org, можно быть уверенным, что документы, созданные в Linux и Windows, будут совершенно совместимы. Программы OpenOffice.org осваиваются очень быстро теми, кто имел дело с другими офисными пакетами. На рис. 3.36 приведено окно программы OpenOffice.org Writer, предназначенной для создания текстовых документов со сложным форматированием. Последние версии пакета OpenOffice.org в состоянии читать и редактировать не только свои форматы файлов, но и файлы других офисных пакетов, включая Microsoft Office 2007. Учитывая бесплатность пакета OpenOffice.org, вы можете свободно использовать его в своей сети, распространять его среди новых пользователей, не нарушая никаких лицензий.

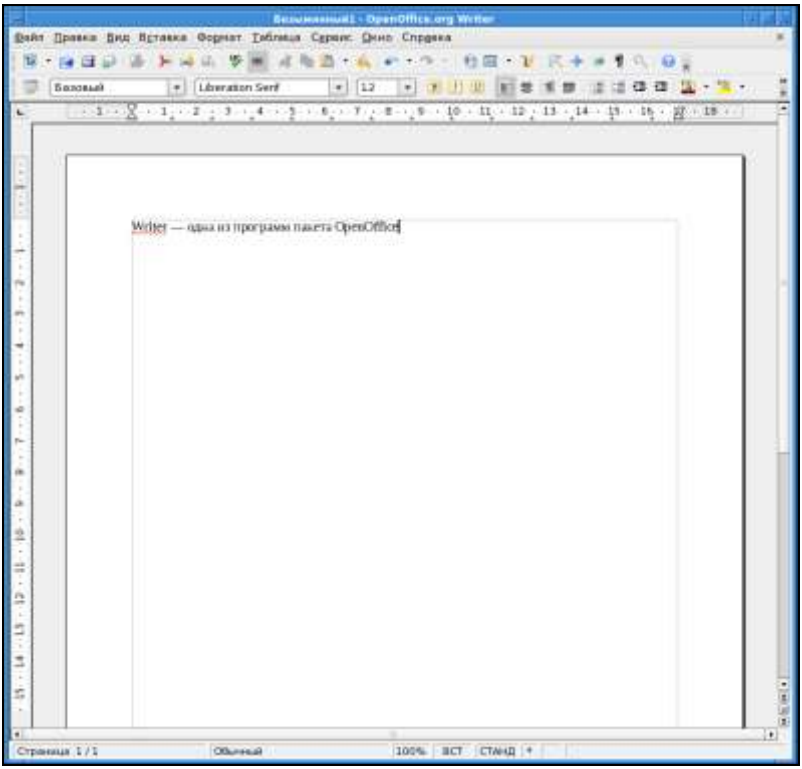


Рис. 3.36. Окно OpenOffice.org Writer

Нередко вместе с офисными программами используют средства для планирования проектов, таких как Microsoft Project. Если пользователям вашей сети необходима такая программа, то предложите OpenProj, которую можно загрузить со страницы разработчиков **http://openproj.org**. Как и OpenOffice.org, OpenProj имеет русскоязычный интерфейс и существует, версиях для Windows и Linux.

В качестве мультимедийного проигрывателя можно рекомендовать VLC media player (рис. 3.37), который тоже существует в версиях для Windows, Linux и других ОС. Можно загрузить эту программу со страницы разработчиков **http://www.videolan.org/vlc**. Этот плеер воспроизводит множество форматов аудио- и видеофайлов, а кроме того, может применяться для трансляции мультимедиа по локальной сети.

Рис. 3.37. Окно VLC media player

Многие пользователи Windows привыкли к программе Skype. И для Linux выпускается версия этой программы (рис. 3.38). Если вам не понравятся другие клиенты IP-телефонии для Linux или вы просто не захотите отказываться от привычного средства общения, то можете продолжать использовать Skype, перейдя на Linux.

Иногда случается, что не удается найти замену Windows-программы под Linux. В этом случае можно воспользоваться входящим во многие дистрибутивы Linux эмулятором Wine (рис. 3.39).

Существуют как бесплатные, так и коммерческие версии этого эмулятора. Коммерческие версии позволяют устанавливать такие программы, как 1С:Предприятие, многие игры, даже Microsoft Office. Но и бесплатная версия Wine поможет работать с множеством Windows-программ в Linux. На рис. 3.40 приведено окно текстового редактора LeoPad, написанного для Windows, но установленного в среде Linux.

Для Linux создается все больше и больше программ, функционально похожих на привычные программы для Windows или даже превосходящих Windows-аналоги по ряду параметров. В большинстве случаев работа на современной рабочей станции Linux не менее комфортна, чем под Windows. Учитывая открытость, безопасность и бесплатность Linux, многие учреждения переводят свои офисы на эту операционную систему.

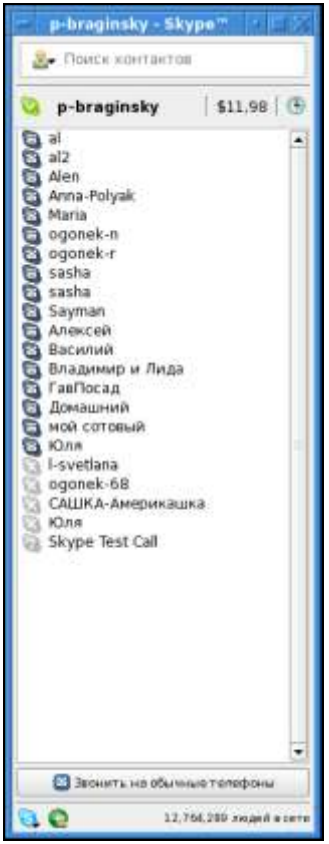


Рис. 3.38. Окно Skype

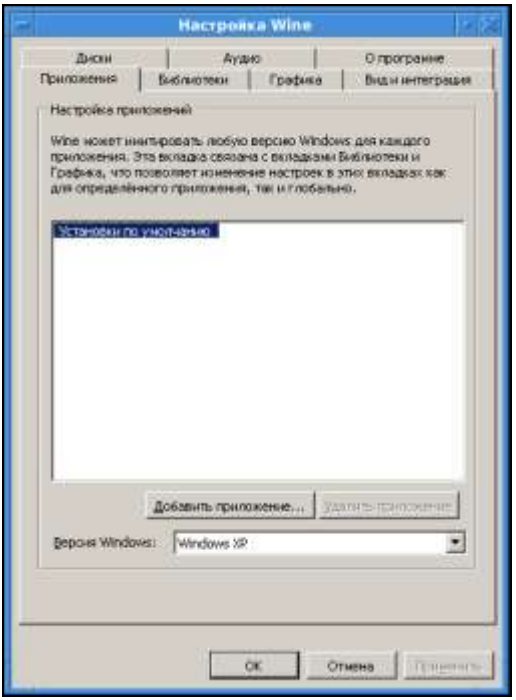


Рис. 3.39. Окно **Настройка Wine**

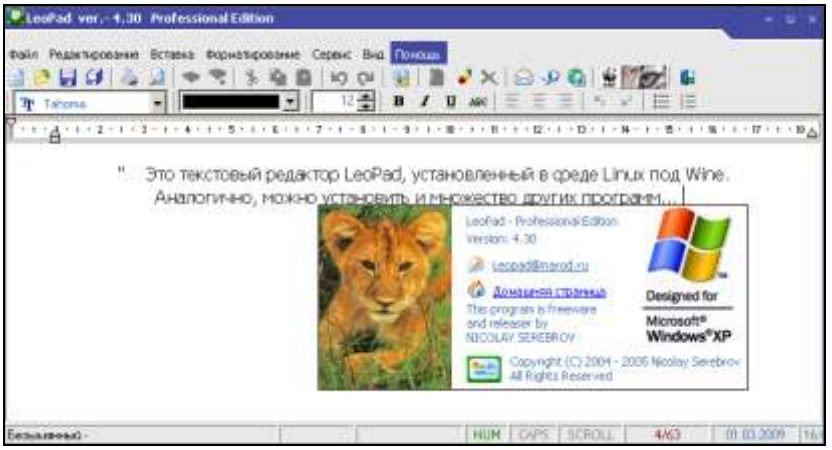


Рис. 3.40. Окно LeoPad

Глава 4

Сервер

Принимая решение о конфигурации сервера вашей сети, следует обратить внимание на возможности Linux. Правда, пока функциональность Linux-сервера, настраиваемого начинающим пользователем Linux, не может полностью повторить функциональность Windows-сервера. Особенно это касается возможностей Active Directory (AD). Настройка AD на системе Windows 2000 Server с помощью мастеров, встроенных в систему, даже для начинающих администраторов задача вполне посильная. Другое дело в Linux (пока). Тем не менее, если ваша сеть небольшая, установка AD не планируется, то настроить файловый, веб-, почтовый серверы, а также DHCP, DNS и шлюз в Интернет вполне по силам даже начинающему. Было бы желание. А желание здесь может быть подкреплено низкой ценой системы, применяемой для сервера, надежностью системы, практической неподверженностью вирусному заражению, умеренной требовательностью к ресурсам и отсутствием необходимости приобретать лицензии для пользователей сервера. В стандартной поставке Windows Server 2003, например, всего пять таких лицензий, а для обеспечения удаленного доступа пользователей к серверу также требуются отдельные лицензии.

Таким образом, если вы хотите сэкономить на лицензиях, на цене ОС для Windows-сервера, у вас есть желание самостоятельно без технической поддержки разобраться с установкой и настройкой Linux-сервера, то можете смело брать какой-либо из свободно распространяемых дистрибутивов Linux и устанавливать сервер.

Выбор дистрибутива — задача не всегда простая. На форумах в Интернете иногда разыгрываются целые баталии между сторонниками различных версий Linux. Существуют специализированные дистрибутивы с предварительно сконфигурированной серверной ОС Linux, например, Mandriva CS, ASPLinux Server ConfPoint Edition, ALT Linux 4.0 Server и другие. Все они не бесплатны, но приобретение подобных дистрибутивов предполагает техническую

поддержку в течение более или менее продолжительного периода. В то же время существуют бесплатные версии Linux, в которых есть возможность настроить серверные функции системы и достаточно успешно. Свободные дистрибутивы, такие как Debian (**http://www.debian.org/index.ru.html**), поддержка которого осуществляется интернет-сообществом, CentOS, тоже позволяют настроить операционную систему в качестве сервера. Для первого знакомства с возможностями Linux-сервера можно выбрать дистрибутив ASPLinux 11 или 12. В стандартной поставке — только свободные компоненты, и вы можете абсолютно легально установить систему с дистрибутива, скопированного у знакомых.

Сеть желательно настроить сразу по ходу установки, и компьютеру назначить статический IP-адрес.

В процессе установки системы есть возможность выбора назначения будущей системы. Один из предлагаемых вариантов — сервер. Выберите его и установите тот состав компонентов, который предложит система. После установки обновите ядро системы и компоненты, используемые сервером. Это можно выполнить, выбрав в главном меню **Приложения** | **Система** | **Обновление системы** и сняв отметки с пакетов, которые вы обновлять не будете. Или используйте программу Yum Extender, которая устанавливается с ASPLinux по умолчанию. В данном случае при обновлении пакетов нужно не снимать, а устанавливать отметки против обновляемых пакетов.

Не стремитесь устанавливать дополнительные приложения. Офисный пакет, программы для работы со звуком и изображениями должны быть установлены на рабочей станции. На сервере обычно не предполагается выполнять какие-либо работы. Если все же у вас появилась необходимость в установке программ, не связанных с функциями сервера, то после каждой установки проверяйте его работоспособность. Некоторые программы могут нарушить работу сервера.

Теперь можно приступить к настройке сервера.

Все доступные функции сервера можно настроить с помощью инструментов, доступных через меню **Система** | **Администрирование** | **Настройка сервера** | **<Имя сервера>**. Далее при описании настроек мы будем указывать только пункт подменю **Настройка сервера.**

Web-сервер

В большинстве дистрибутивов Linux содержится сервер Apache, который получил широкое распространение не только в малых сетях, но и на серьезных серверах в Интернете. ASPLinux также содержит этот сервер, и его настройку мы рассмотрим далее.

Выберите пункт подменю **HTTP**. После щелчка мышью по этому пункту откроется окно **HTTP Server Configuration** — настройка HTTP-сервера (рис. 4.1).

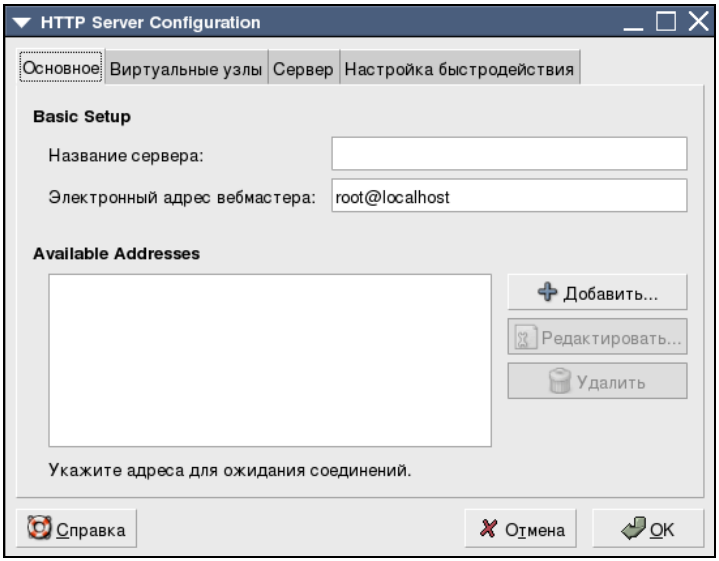


Рис. 4.1. Окно **HTTP Server Configuration**, вкладка **Основное**

На вкладке **Основное** этого окна можно указать:

- **Название сервера** — это необходимо, если предполагается делать перенаправление с одного сервера на другой (если у вас их несколько), в противном случае указывать имя сервера не обязательно;
- **Электронный адрес вебмастера** — это тоже не влияет на работоспособность сервера и при знакомстве с ним указывать не обязательно;
- **Available Addresses** — допустимые адреса. В этом поле можно указать один или несколько адресов, с которых будет возможно подключение к серверу. Эти адреса имеет смысл указывать, если вы хотите ограничить доступ к серверу из сети.

На вкладке **Виртуальные узлы** (рис. 4.2) для первого опыта можно не изменять ничего, если вы не хотите добавить новый виртуальный узел или изменить параметры существующего.

Но, даже не изменяя параметры узла, есть смысл заглянуть в окно **Свойства виртуального узла** (рис. 4.3), где вы сможете узнать или изменить, если такое желание возникнет, название виртуального узла, его корневой каталог

и другие параметры. Название узла необходимо локальному администратору для идентификации узлов, когда их несколько, а в корневом каталоге должны располагаться все файлы узла, которые будут использоваться веб-сайтом.

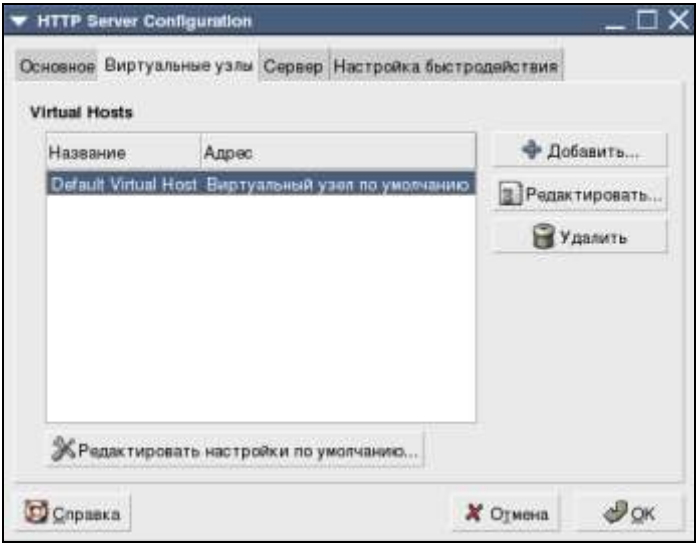


Рис. 4.2. Окно **HTTP Server Configuration**, вкладка **Виртуальные узлы**

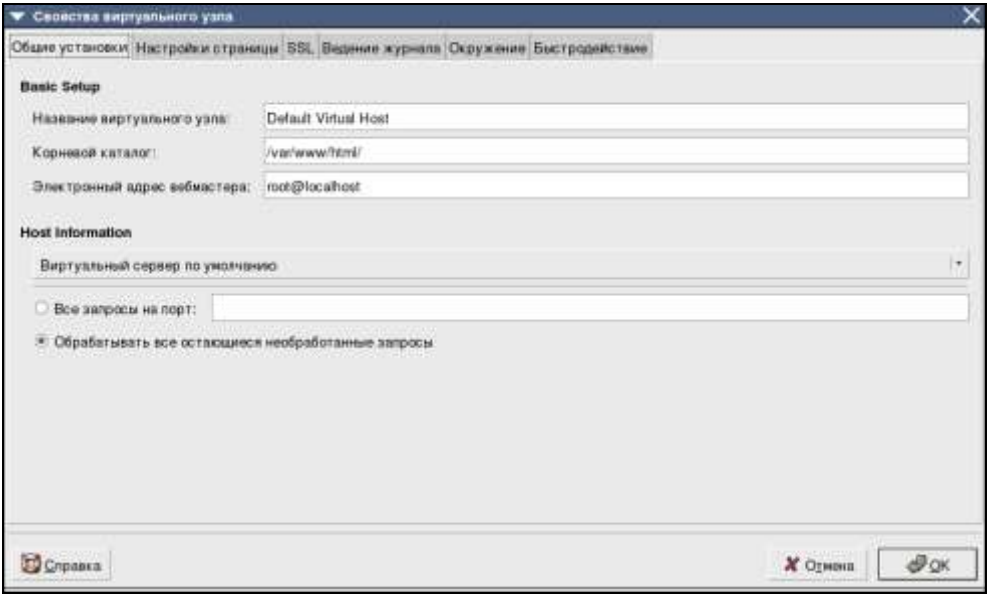


Рис. 4.3. Окно **Свойства виртуального узла**, вкладка **Общие установки**

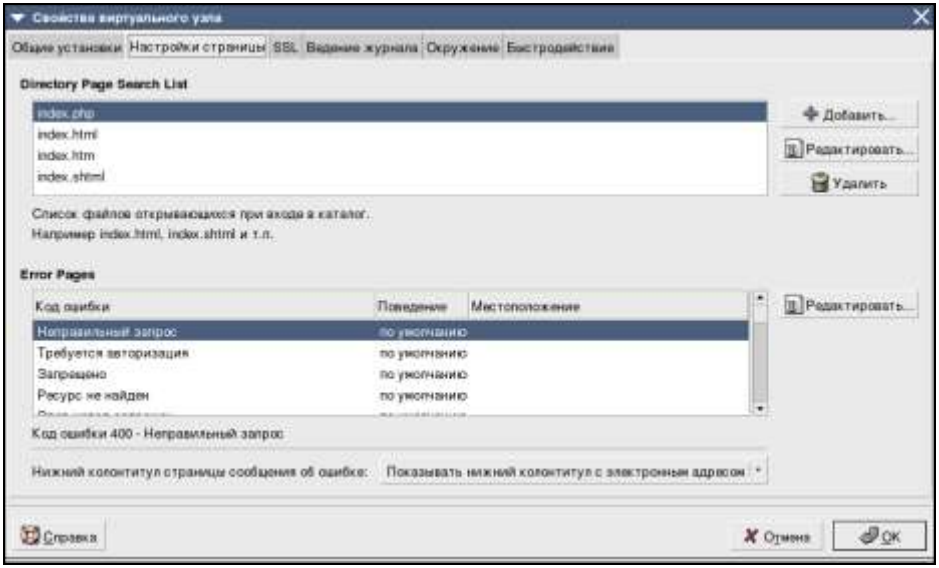


Рис. 4.4. Окно **Свойства виртуального узла**, вкладка **Настройки страницы**

На вкладке **Настройки страницы** рассматриваемого окна (рис. 4.4) можно определить, какие форматы файлов будут опознаваться нашим сервером в качестве главных веб-страниц. По умолчанию уже определено четыре формата, которые наиболее часто используются на серверах Apache. Имена таких файлов обычно устанавливаются как index, но вы можете использовать любые другие, внеся изменения в разделе **Directory Page Search List.** Страницы ошибок (**Error Pages**) оставьте как есть. Впоследствии, осваивая практику создания веб-сайтов, вы сможете создавать свои страницы ошибок или изменять существующие по своему усмотрению. Для тех, кто не знает, сообщим только, что эти страницы необходимы для информирования посетителей сайта о проблемах, связанных с его функционированием и использованием.

На вкладке **SSL** окна **Свойства виртуального узла** можно включить поддержку SSL — защищенных соединений с узлами Интернета (рис. 4.5). Поддержка SSL требуется для защиты конфиденциальных данных при передаче через Интернет. Подробное рассмотрение этой технологии не входит в задачу книги, поэтому пока можно не включать или не настраивать SSL. Для обычных веб-страниц поддержка защищенных соединений не требуется.

На вкладке **Ведение журнала** (рис. 4.6) можно изменить параметры журналов **Transfer Log** и **Error Log**, в которых фиксируются подключения к серверу и ошибки сервера. Эти журналы требуются администратору для анализа работы сервера. Для обоих журналов доступно три варианта сохранения дан-

ных: записывать в файл, передать ведение журнала указанной программе или использовать системный журнал. Первый вариант установлен по умолчанию, и изменять его без необходимости не надо.

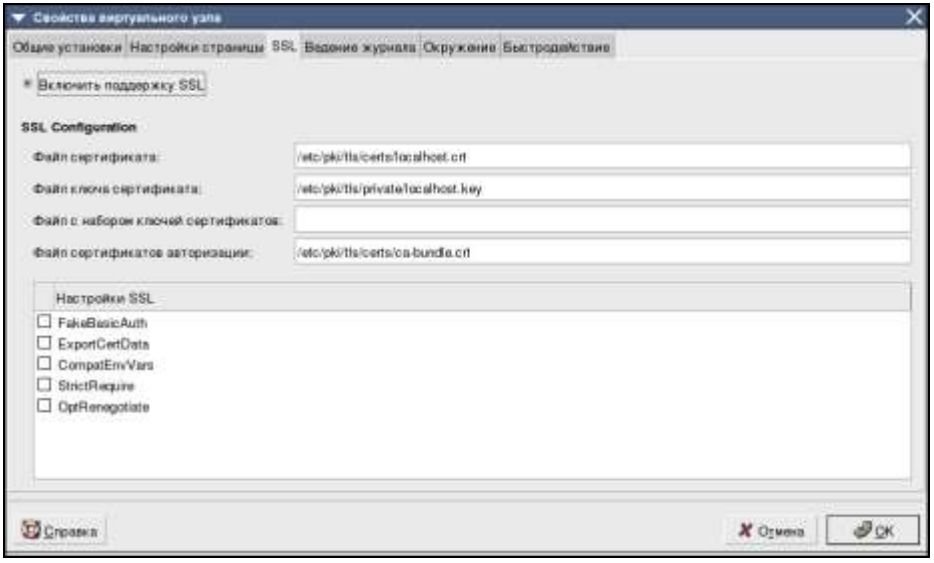


Рис. 4.5. Окно **Свойства виртуального узла**, вкладка **SSL**

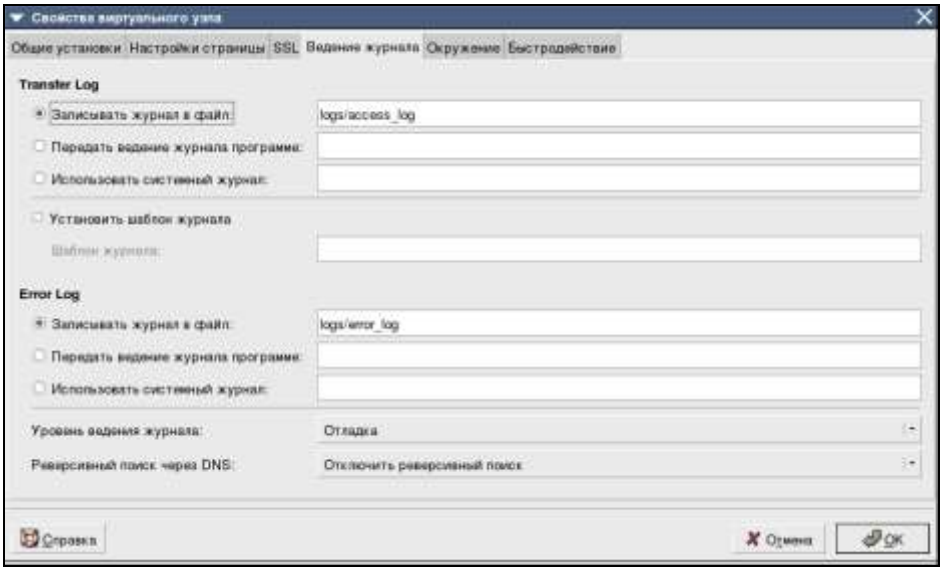


Рис. 4.6. Окно **Свойства виртуального узла**, вкладка **Ведение журнала**

Перед запуском сервера вы можете поместить в его корневой каталог, заранее созданную стартовую страницу. Если у вас еще нет такой страницы, сервер содержит тестовую страницу, которую вы сможете увидеть и убедиться, что сервер работает. Но для того чтобы подключение к серверу стало возможным, необходимо запустить службу httpd. Для ее запуска через пункт меню **Службы** откройте окно **Настройка служб** (рис. 4.7) и отметьте **httpd** в списке служб. После этой операции httpd будет запускаться при старте системы.

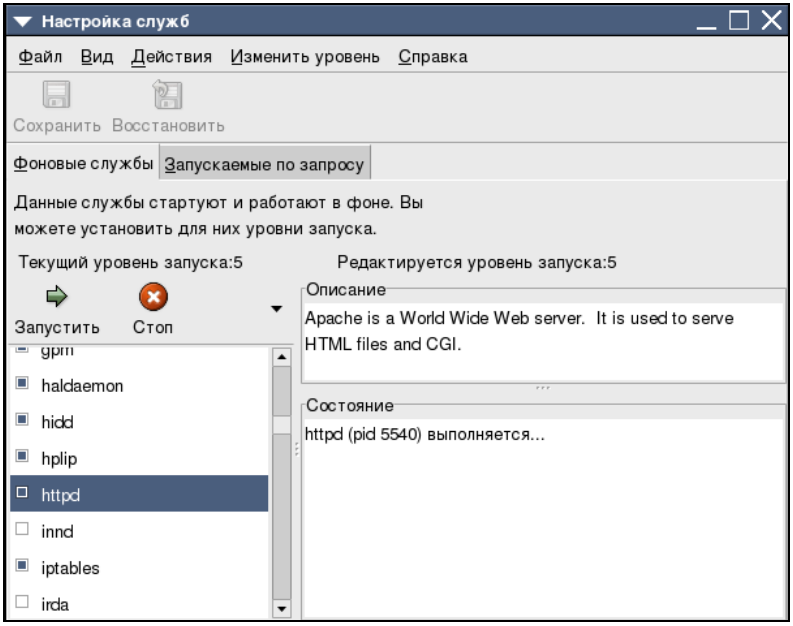


Рис. 4.7. Окно **Настройка служб**

Теперь, когда вы ознакомились с настройками сервера, а может быть и изменили какие-либо из них, можно подключиться к серверу для проверки его работоспособности. Это можно сделать как с другого компьютера сети по сетевому имени или IP-адресу, так и прямо через браузер вашего сервера, набрав в строке адреса **http://localhost/**. Браузер отобразит тестовую страницу (рис. 4.8).

Повторите подключение с другого компьютера и убедитесь, что сервер доступен для компьютеров сети. Если все эксперименты оказались успешны, можно загружать на сервер файлы вашего сайта и организовывать доступ к нему.

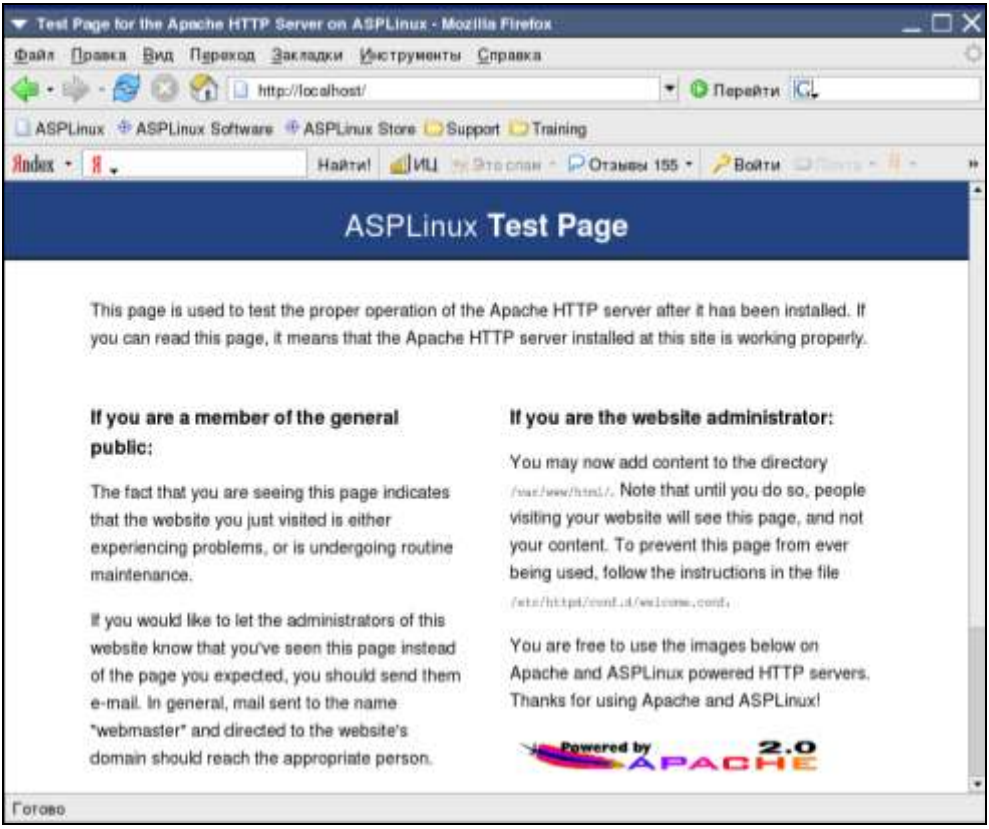


Рис. 4.8. Окно **ASPLinux Test Page**

Сервер NFS

Пункт меню **NFS** позволяет получить доступ к настройкам сервера сетевой файловой системы (Network File System, NFS). Эта файловая система применяется преимущественно в сетях, где работают компьютеры под управлением Linux или UNIX. Особенность сетевой файловой системы заключается в том, что для приложений, которые могут работать только с локальными файлами, доступны и файлы из NFS. Сервер может предоставлять доступ к файлам, расположенным как на любых носителях, работающих на самом сервере, так и на других компьютерах сети или даже в Интернете. Щелкнув пункт меню **NFS**, вы откроете окно **Настройка сервера NFS** (рис. 4.9). В показанном на рисунке окне уже есть строка с указанием доступного по NFS ресурса, процедуру добавления которого мы и рассмотрим. Для добавления нового ресурса следует выбрать в оконном меню кнопку **Добавить.**

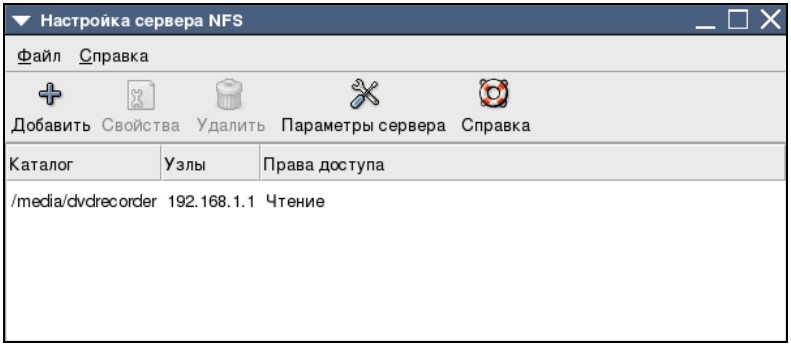


Рис. 4.9. Окно **Настройка сервера NFS**

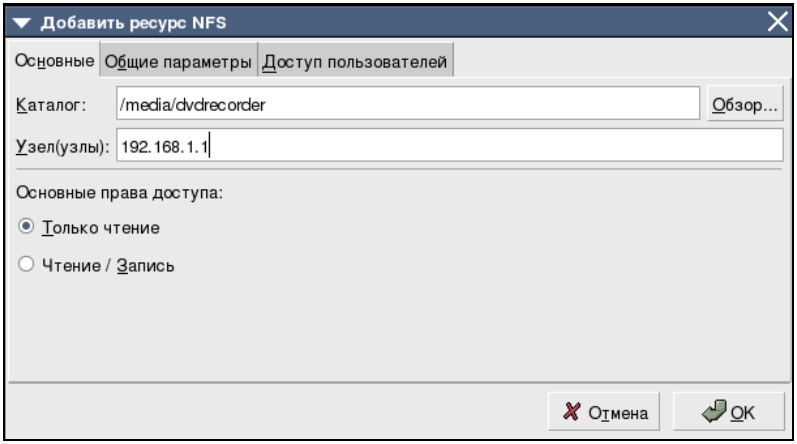


Рис. 4.10. Окно **Добавить ресурс NFS**, вкладка **Основные**

Откроется окно **Добавить ресурс NFS** (рис. 4.10), где в соответствующих полях следует указать каталог, к которому открывается доступ, и узлы, которым этот доступ предоставляется. Можно указать IP-адрес отдельного узла или указать адрес сети и маску подсети, например `192.48.1.0/24`, или указать имя узла или рабочей группы в виде `*@<имя_рабочей_группы>` или `*@<имя_домена>.<суффикс_домена>`. Звездочка вместо имени обозначает все доступные имена.

В этом же окне можно указать основные права доступа.

Еще несколько параметров нового ресурса можно настроить на вкладках **Общие параметры** (рис. 4.11) и **Доступ пользователей** (рис. 4.12).

Смысл параметров, настраиваемых в этих вкладках, понятен из их формулировок. При первых экспериментах их можно не изменять.

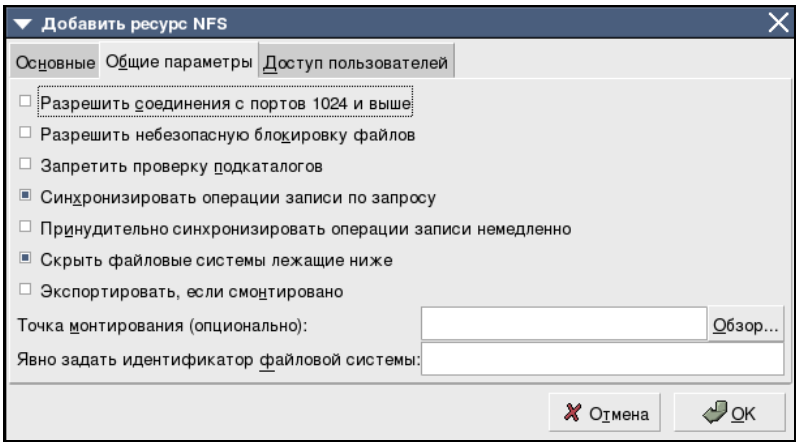


Рис. 4.11. Окно **Добавить ресурс NFS**, вкладка **Общие параметры**

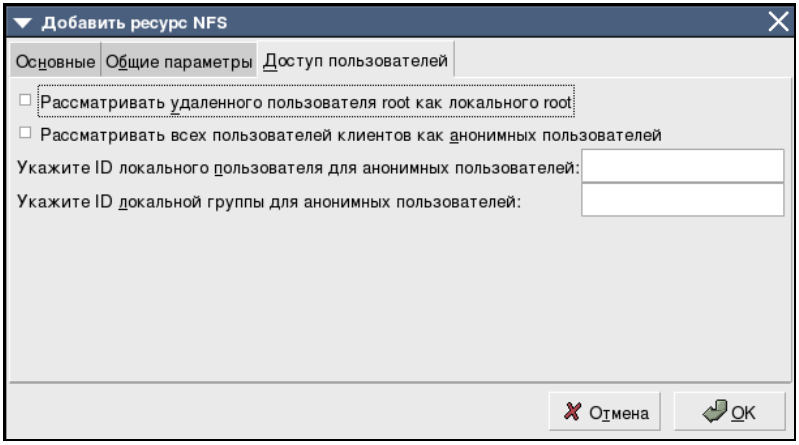


Рис. 4.12. Окно **Добавить ресурс NFS**, вкладка **Доступ пользователей**

Поэкспериментировав, поиграв с этими параметрами, вы сможете выбрать необходимые для вашей сети настройки.

Файловый сервер

Настройки этого сервера скрываются за пунктом меню **Samba**. В отличие от NFS доступ к ресурсам этого сервера может быть осуществлен с Windows-машин стандартными для них средствами. Linux-машины с установленным клиентом Samba также без проблем могут получить доступ к этому серверу.

Решив установить файловый сервер, вы должны определиться с местом хранения общедоступных файлов. Каталоги, к которым предполагается дать общий доступ, могут уже существовать, можно создать их перед установкой сервера, а можно создать в процессе настройки сервера средствами программы его настройки. В последнем случае локальные права на эти каталоги будут определены для доступа администратора компьютера. В примере выберем второй вариант — создадим новый каталог общего доступа share в папке текущего пользователя (рис. 4.13).

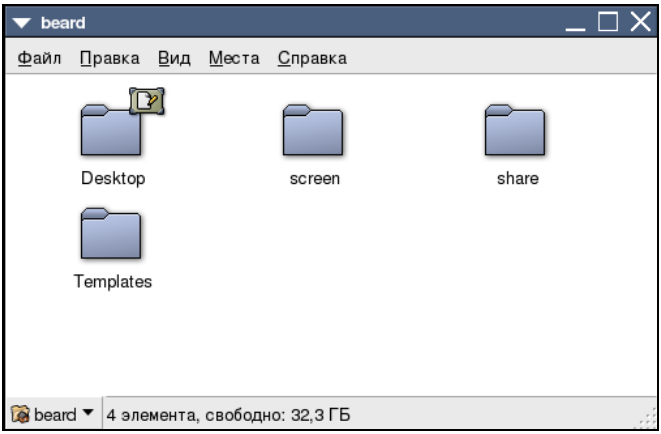


Рис. 4.13. Окно домашнего каталога пользователя

Конечно, общедоступный каталог можно создать в любом месте файловой системы, но в данном случае мы создали его в домашней директории текущего пользователя с тем расчетом, что этот пользователь будет иметь все права на каталог и вложенные в него папки и файлы.

Теперь откроем окно утилиты **Настройка сервера Samba** через пункт меню **Samba** (рис. 4.14) и настроим параметры сервера, выбрав в оконном меню **Настройка** | **Параметры сервера**. В открывшемся окне **Параметры сервера** на вкладке **Основной** (рис. 4.15) следует указать имя рабочей группы и произвольное описание сервера.

На вкладке **Безопасность** того же окна (рис. 4.16) укажите режим аутентификации, выбрав его из ниспадающего списка. Режим **Пользователь** предполагает аутентификацию по имени пользователя, зарегистрированном на данном сервере, и паролю. Шифрование пароля предотвращает возможность перехвата пароля злоумышленником при прослушивании сети. Правда, в небольшой домашней сети вряд ли найдется такой злоумышленник.

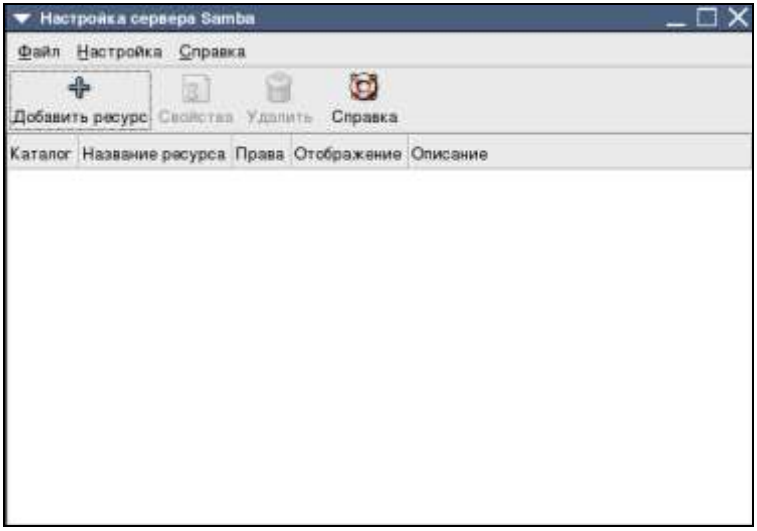


Рис. 4.14. Окно **Настройка сервера Samba**

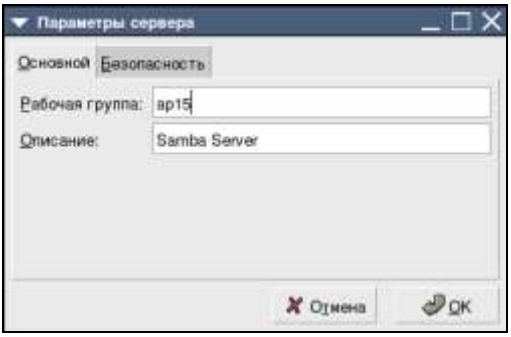


Рис. 4.15. Окно **Параметры сервера**, вкладка **Основной**

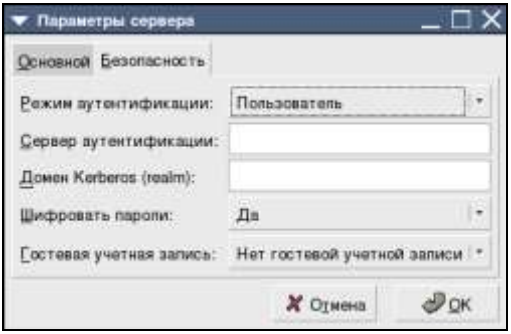


Рис. 4.16. Окно **Параметры сервера**, вкладка **Безопасность**

Выбрав в оконном меню **Настройка | Пользователи Samba**, необходимо добавить пользователей сервера в открывшемся окне **Пользователи Samba** (рис. 4.17). Кнопкой **Добавить пользователя** откройте окно **Добавить нового пользователя** (рис. 4.18), где в ниспадающем списке **Имя пользователя Unix** выберите имя пользователя уже зарегистрированного на этом компьютере. Укажите имя пользователя Windows для этой учетной записи, которое может совпадать с именем пользователя UNIX. Укажите также пароль нового пользователя Samba. Пароль может отличаться от того, что требуется для входа в систему.

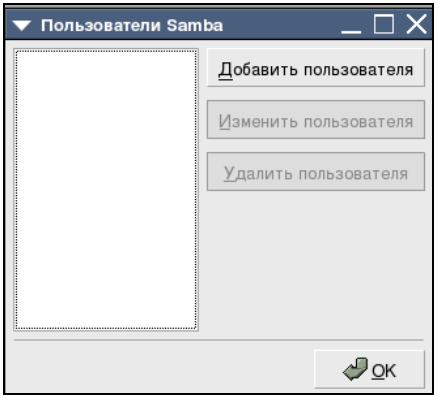


Рис. 4.17. Окно **Пользователи Samba**

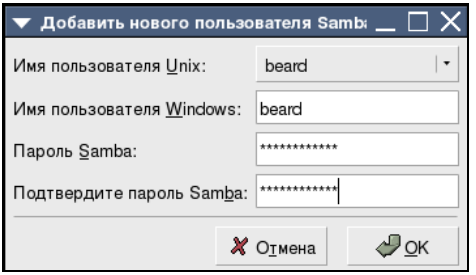


Рис. 4.18. Окно **Добавить нового пользователя**

Теперь пришла очередь сделать доступным по сети созданный ранее каталог share.

В окне **Настройка сервера Samba** (рис. 4.14) нажмите кнопку **Добавить ресурс**. В открывшемся окне **Создать ресурс Samba** (рис. 4.19) с помощью кнопки **Обзор** и открывшегося при ее нажатии окна **Каталог** (рис. 4.20) найдите в файловой системе каталог share и щелкните по его имени.

При этом, если внутри выбранного каталога нет других папок, окно **Каталог** не будет содержать каких-либо имен ресурсов в поле **Папки** (рис. 4.21). После нажатия кнопки **OK** в окне **Создать ресурс Samba** на вкладке **Основной** в поле **Каталог** появится строка, указывающая полный путь к выбранному каталогу (рис. 4.22).

Остается указать название ресурса, которое будет видно в сети, и его описание.

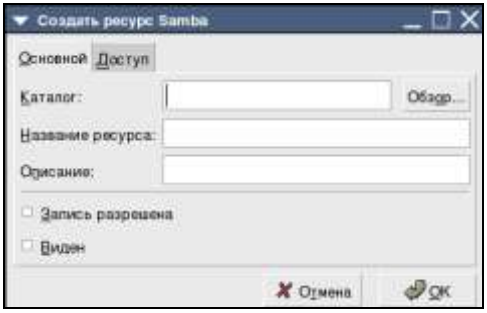


Рис. 4.19. Окно **Создать ресурс Samba**

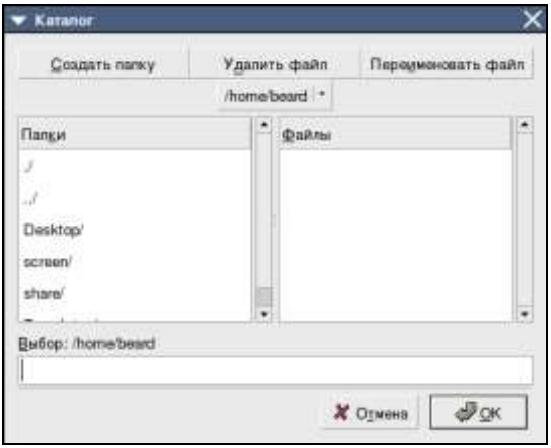


Рис. 4.20. Окно **Каталог**

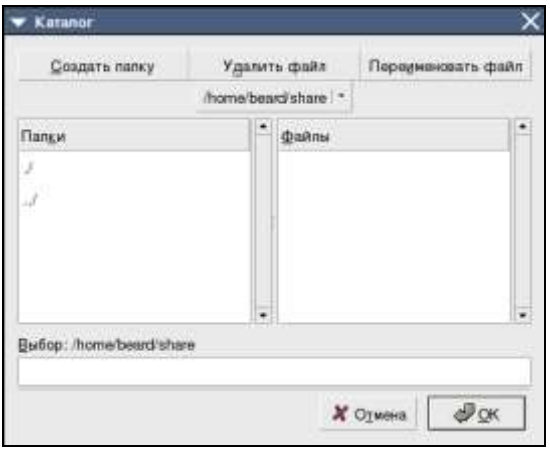


Рис. 4.21. Окно **Каталог** (ресурс выбран)

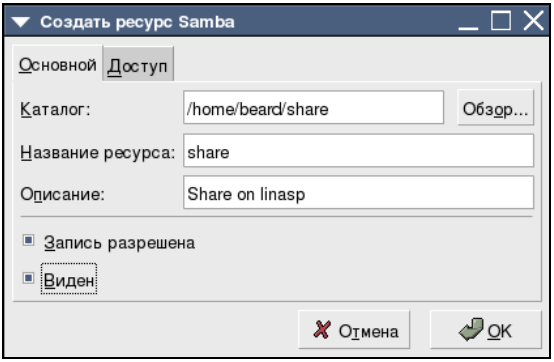


Рис. 4.22. Окно **Создать ресурс Samba** (каталог выбран)

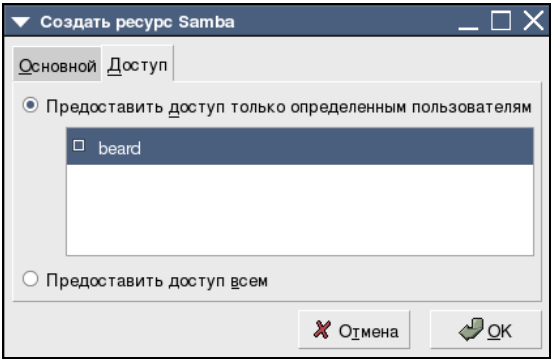


Рис. 4.23. Окно **Создать ресурс Samba**, вкладка **Доступ**

Перейдя на вкладку **Доступ** окна **Создать ресурс Samba** (рис. 4.23), вы увидите имя добавленного ранее пользователя сервера Samba. При выборе опции **Предоставить доступ только определенным пользователям** следует пометить имена учетных записей пользователей, которым предоставляется доступ (в данном случае у нас только один пользователь), и нажать кнопку **OK**.

Теперь в окне **Настройка сервера Samba** появится информация о добавленном ресурсе (рис. 4.24). Выделив его и нажав кнопку **Свойства**, можно установить или снять видимость ресурса в сети и возможность записи в него.

При наличии доступных по сети ресурсов, к ним можно будет обращаться с любых компьютеров сети. Сам сервер будет виден в сетевом окружении других компьютеров, в том числе, работающих под управлением Windows. На рис. 4.25 показано окно **Сеть,** открытое на компьютере под управлением Windows Vista, в котором можно увидеть и наш сервер Samba как компьютер ASPLIN.

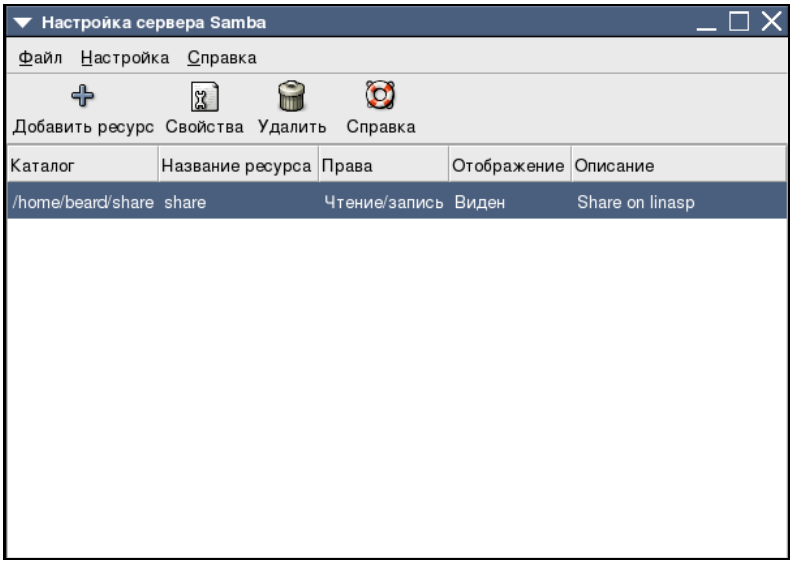


Рис. 4.24. Окно **Настройка сервера Samba**
(с информацией о добавленном ресурсе)

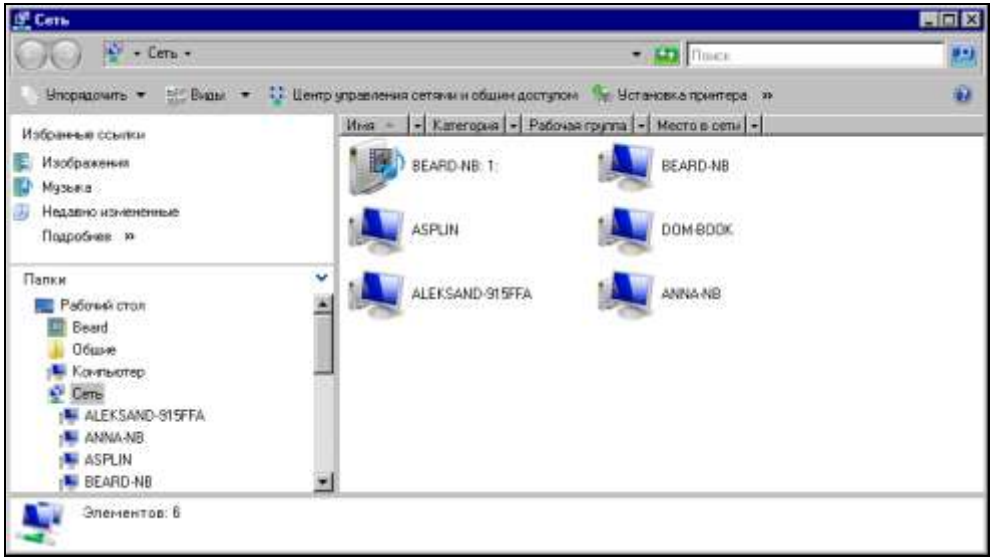


Рис. 4.25. Окно **Сеть** проводника Windows

Сервер DNS

Щелкнув пункт меню **Система доменных имен** (DNS), можно открыть утилиту настройки DNS-сервера. При небольшом числе компьютеров, конечно, не сложно внести все их имена и IP-адреса в файл hosts, имеющийся на каждой машине Linux и Windows. Но если компьютеров становится много, то искать друг друга в сети им легче с помощью DNS-сервера.

При первом запуске утилиты настройки DNS-сервера (рис. 4.26), она предупредит об отсутствии конфигурации BIND (Berkeley Internet Name Domain).

Примечание

BIND или Berkeley Internet Name Domain — это пакет программного обеспечения для поддержки DNS, реализованный в университете Беркли. Он широко применяется при работе в Интернете. Основная масса серверов DNS — это серверы различных версий BIND.

Нам ничего не остается, как нажать кнопку **OK**.

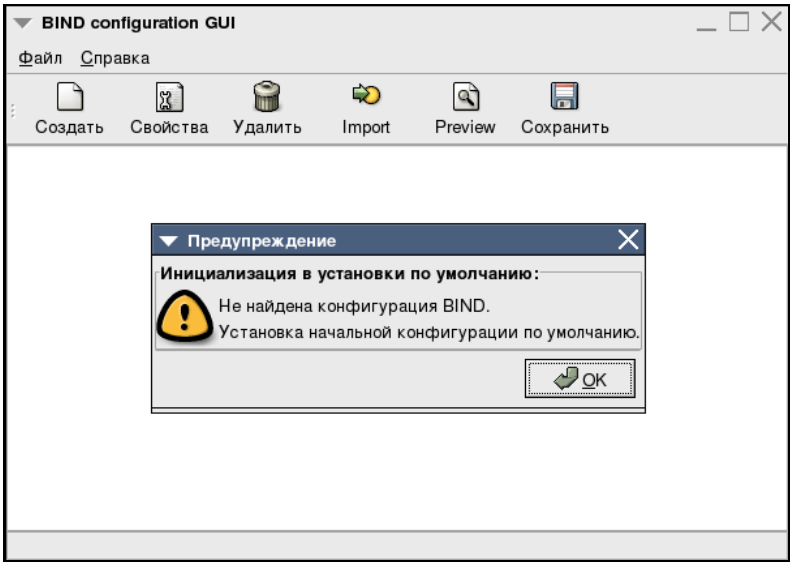


Рис. 4.26. Окно **BIND configuration GUI** (первый запуск)

Автоматически будет выполнена начальная конфигурация DNS-сервера с использованием локального имени компьютера и его локального IP-адреса (рис. 4.27). Далее необходимо вручную создать необходимые зоны и записи. Есть возможность импортировать записи объектов сети из файла hosts кноп-

кой **Import**, если в нем уже есть информация о компьютерах вашей сети. При этом все необходимые записи будут созданы автоматически.

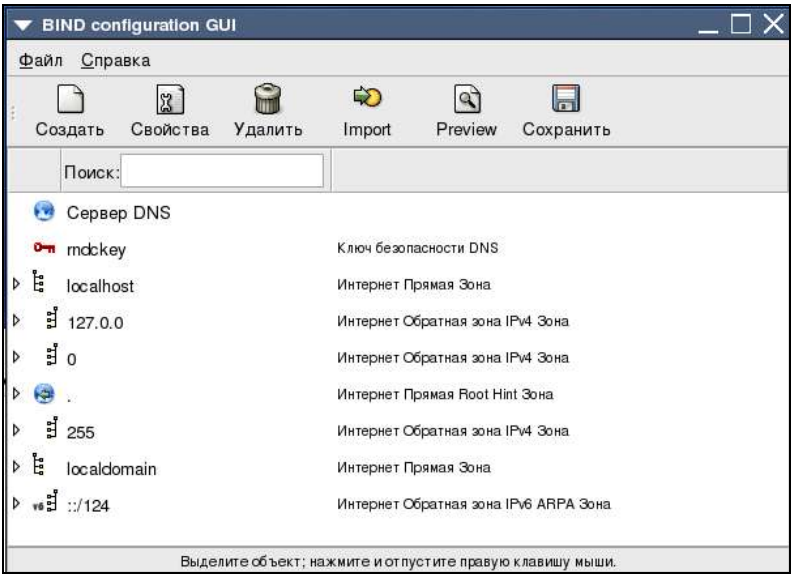


Рис. 4.27. Окно **BIND configuration GUI** (начальная конфигурация)

Описывать подробно настройку DNS-сервера мы не будем. Для начала работы с ним в локальной сети достаточно импортировать заранее подготовленный файл hosts. Но в дальнейшем у вас может появиться необходимость в настройке этого сервера.

Поскольку настройка полноценного DNS-сервера — достаточно сложный процесс, требующий определенных знаний, вам потребуется время для их освоения. Приведем здесь две ссылки на ресурсы в Интернете, которые позволят вам получить необходимую информацию.

По ссылке **http://www.opennet.ru/docs/RUS/dns2/** находится обширное руководство по настройке BIND.

По ссылке **http://hostinfo.ru/articles/57** находится описание принципов работы DNS-сервера и определяются все основные понятия и термины. Далее приведено несколько сокращенное изложение этой статьи.

Как работает DNS-сервер

Основной задачей DNS-сервера является трансляция доменных имен в IP-адреса и обратно.

Эту задачу позволяют решить и файлы hosts, если их заполнять на каждом компьютере, но с ростом сети эта работа может стать непосильной — ведь эти файлы надо еще и синхронизировать, не говоря уж об их размере… Помочь может только DNS-сервер.

DNS — иерархическая структура имен. Существует "корень дерева" с именем "." (точка). Так как корень един для всех доменов, то точка в конце имени обычно не ставится (но она используется в описаниях DNS — тут надо быть очень внимательным!). Ниже корня лежат домены первого уровня. Их немного: com, net, edu, org, mil, int, biz, info, gov (есть еще несколько) и домены государств, например, ru. Еще ниже находятся домены второго уровня, например, listsoft.ru. Еще ниже — третьего и т. д. В локальной сети могут существовать и мнимые домены первого уровня, например dom. Их нет в Интернете, и DNS-сервер не будет искать в нем имена компьютеров сети.

Каждому DNS-серверу известны адреса корневых DNS-серверов, после их опроса запрос на трансляцию имени узла в IP-адрес начинает спускаться вниз — корневой сервер пересылает запрос серверу первого уровня, тот — серверу второго уровня и т. д. Таким образом, каждый DNS-сервер работает как хороший компьютерщик: он всегда либо знает ответ, либо знает, у кого спросить…

Помимо "вертикальных связей", у серверов есть еще и "горизонтальные" отношения "первичный — вторичный". Действительно, если предположить, что сервер, обслуживающий какой-то домен и работающий "без страховки", вдруг перестанет быть доступным, то все машины, расположенные в этом домене, окажутся недоступны! Именно поэтому при регистрации домена второго уровня выдвигается требование указать минимум два сервера DNS, которые будут этот домен обслуживать. В небольшой локальной сети это не настолько существенно и может применяться единственный DNS-сервер.

DNS-серверы бывают рекурсивные и нерекурсивные. Первые всегда возвращают клиенту ответ — они самостоятельно отслеживают отсылки к другим DNS-серверам и опрашивают их. Нерекурсивные серверы возвращают клиенту эти отсылки, так что клиент должен самостоятельно опрашивать указанный сервер. Рекурсивные серверы удобно использовать на низких уровнях, в частности, в локальных сетях. Дело в том, что они кэшируют все промежуточные ответы, и при последующих запросах ответы будут возвращаться намного быстрее. Нерекурсивные серверы обычно стоят на верхних ступенях иерархии — поскольку они получают очень много запросов, то для кэширования ответов никаких ресурсов не хватит.

Полезным свойством DNS является умение использовать "пересыльщиков" (forwarders). "Честный" DNS-сервер самостоятельно опрашивает другие сер-

веры и находит нужный ответ, но если ваша сеть подключена к Интернету по медленной (например, dial-up) линии, то этот процесс может занимать довольно много времени. Вместо этого можно перенаправлять все запросы, скажем, на сервер провайдера, а затем принимать его ответ. Использование "пересыльщиков" может оказаться интересным и для больших компаний с несколькими сетями: в каждой сети можно поставить относительно слабый DNS-сервер, указав в качестве "пересыльщика" более мощную машину, подключенную по быстрой линии. При этом все ответы будут кэшироваться на этом мощном сервере, что ускорит разрешение имен для целой сети.

Для каждого домена администратор ведет базу данных DNS. Эта база данных представляет собой набор простых текстовых файлов, расположенных на основном (первичном) сервере DNS (вторичные серверы периодически копируют к себе эти файлы). В файлах конфигурации сервера указывается, в каком именно файле содержатся описания каких зон и является ли сервер первичным или вторичным для этой зоны.

Элементы базы DNS часто называют RR (сокращение от Resource Record). Базовый формат записи выглядит так:

```
[имя] [время] [класс] тип данные
```

`Имя` может быть относительным или абсолютным (FQDN — Fully Qualified Domain Name). Если имя относительное (не заканчивается точкой — помните про корневой домен?), то к нему автоматически добавляется имя текущего домена. Например, если в домене listsoft.ru я опишу имя "www", то полное имя будет интерпретироваться как "www.listsoft.ru.". Если же это имя указать как "www.listsoft.ru" (без последней точки), то оно будет считаться относительным и будет интерпретировано как "www.listsoft.ru.listsoft.ru.".

`Время` задает интервал времени в секундах, в течение которого данные могут сохраняться в кэше сервера.

`Класс` определяет класс сети. Практически всегда это будет `IN`, обозначающее INternet. Интересно, что и в локальных сетях используется этот класс.

`Тип` может быть одним из следующих:

- `SOA` — определяет DNS-зону;
- `NS` — сервер имен для зоны;
- `A` — преобразование имени в IP-адрес;
- `PTR` — преобразование IP-адреса в имя;
- `MX` — почтовая станция;
- `CNAME` — имена машины;

- `HINFO` — описание "железа" компьютера;
- `TXT` — комментарии или какая-то другая информация.

Есть также некоторые другие типы, но они намного менее распространены.

В записях можно использовать символы `#` и `;` для комментариев, `@` для обозначения текущего домена, `()` — скобки — для написания данных на нескольких строках. Кроме того, можно использовать метасимвол `*` в имени. Порядок записей не имеет значения за одним исключением: запись SOA должна идти первой. Дальнейшие записи считаются относящимися к той же зоне, пока не встретится новая запись SOA. Как правило, после записи зоны указывают записи DNS-серверов, а остальные записи располагают по алфавиту, но это не обязательно.

SOA — описание зоны

Теперь попробуем рассмотреть записи. Первой описываем зону:

```
mycompany.ru. IN SOA ns.mycompany.ru. admin.mycompany.ru. (1001 ; serial
2400 ; Refresh — 6 часов
1800 ; Retry — 30 мин
1209600 ; Expire — 2 недели
432000) ; Minimum — 5 дней
```

Сначала идет имя домена: mycompany.ru. (обратите внимание на точку в конце имени). Вместо имени можно было (и чаще всего так и делают) поставить знак *@*.

`ns.mycompany.ru.` — основной сервер имен.

`admin.mycompany.ru.` — почтовый адрес администратора в формате имя(точка)машина.

Затем в круглых скобках идут поля, необходимые для правильного "восприятия" вашей зоны другими серверами. Первое число — serial — является "версией" файла зоны. При внесении изменений это число надо увеличить — если вторичный сервер увидит, что его версия зоны меньше, чем у первичного сервера, то он перечитает данные. Типичной ошибкой является обновление зоны без обновления этого числа. Очень удобно в качестве serial использовать текущую дату, например, 2003040401 — 4 апреля 2003 года, первое обновление.

`Refresh` говорит вторичным серверам, как часто они должны проверять значение serial.

`Retry` говорит о том, как часто вторичный сервер должен пытаться прочитать данные, если первичный сервер не отвечает.

Expire говорит вторичным серверам, в течение какого времени они должны обслуживать домен, если первичный сервер не отвечает. По истечении этого времени вторичные серверы будут считать свои данные устаревшими.

Minimum задает время жизни записей по умолчанию для данной зоны.

NS описывает серверы имен

Теперь опишем серверы имен, обслуживающие наш домен:

```
mycompany.ru. IN NS ns.mycompany.ru.
mycompany.ru. IN NS ns.provider.ru.
```

Здесь ничего сложного нет. Так как имя зоны совпадает с указанным в поле именем записи SOA, то его можно оставить пустым.

A описывает хосты

Дальше идут записи A, описывающие ваши компьютеры и позволяющие преобразовать имена в IP-адреса.

```
major IN A 192.48.0.1
colonel IN A 192.48.0.2
IN HINFO "2xPIV-1.7 Win2K"
general.mycompany.ru. IN A 192.48.0.3
```

Здесь сложного тоже ничего нет — имена могут быть относительные или "абсолютные", можно добавить записи о конфигурации машины (пропущенное имя в записи HINFO говорит о том, что имеется в виду предыдущее имя). Не забудьте добавить записи:

```
localhost. IN A 127.0.0.1
localhost IN CNAME localhost.
mycompany.ru. IN A 192.48.0.1
```

Первая отдает адрес 127.0.0.1 любой машине, запросившей имя localhost, вторая — localhost.mycompany.ru, а третья говорит, куда послать клиента, который хочет попасть на mycompany.ru.

CNAME — короткие имена серверов

Записи CNAME позволяют дать машинам удобные или значащие имена. Например:

`ftp IN CNAME general` говорит, что ftp.mycompany.ru живет по адресу 192.48.0.3. CNAME удобно использовать, если вы меняете имя машины, но хотите оставить доступ для клиентов, которые помнят старое имя. Удобный трюк с использованием CNAME заключается в назначении коротких имен часто используемым адресам. Например, прописав `ls IN CNAME www.listsoft.ru.`, вы сможете заходить на ListSoft, просто набирая `ls` в качестве адреса.

MX описывает пересылку почты

Записи MX нужны для того, чтобы указать, куда пересылать почту. В этих записях добавляется приоритет — чем он меньше, тем выше приоритет машины. Приоритеты нужны для того, чтобы можно было задать несколько записей и перенаправить почту на альтернативный сервер, если основной не работает. Запись MX должна быть указана для домена в целом и, возможно, для каждой машины в отдельности. Сложного тут тоже ничего нет за одним исключением: очень часто встречается неправильное использование метасимвола "*". Запись *.mycompany.ru. означает не "любая машина домена mycompany.ru", а "любая машина, которая еще не была описана". Причем даже если использовалась не MX-, а, например, A-запись, то звездочка все равно не будет работать для этой машины. В принципе, метасимволы нужны только для того, чтобы принимать почту для сети, находящейся за брандмауэром, и чтобы пересылать почту в сéти, не подключенные к Интернету (например, работающие через UUCP). Так как записи DNS меняются довольно редко, то имеет смысл прописать MX-записи для всех машин, описанных записями A.

```
mycompany.ru. IN MX 10 relay
mycompany.ru. IN MX 20 mycompany.ru.
mycompany.ru. IN MX 30 mail.provider.ru.
general.mycompany.ru. IN A 192.48.0.3
IN MX 10 mycompany.ru.
```

Реверсная зона

На этом создание файла зоны можно считать законченным. Но остается более увлекательное занятие: описание реверсной зоны. Если предыдущий файл позволяет определить IP-адрес по имени, то теперь надо сделать так, чтобы по IP-адресу можно было "вычислить" имя. Отсутствие реверсной зоны является довольно типичной ошибкой и может приводить к самым разным ошибкам — начиная от сбоев FTP-серверов и заканчивая классификацией отправленных писем как спама.

PTR преобразовывает адрес в имя

Для обратного преобразования используются записи PTR. Но не торопитесь их вписывать — тут есть одна хитрость: они пишутся в отдельном специальном домене верхнего уровня, с названием IN-ADDR.ARPA. Домен этот был создан для того, чтобы и для прямого, и для обратного преобразований можно было использовать одни и те же программные модули. Дело в том, что "мнемонические" имена пишутся слева направо: www.listsoft.ru означает, что www находится в listsoft, а listsoft — в ru. IP-адреса пишутся наоборот: 195.242.9.4 означает, что машина 4

находится в подсети 9, которая является частью 195.242. И для сохранения "единого стиля" адресов для обратного преобразования используются имена вида 4.9.242.195.IN-ADDR.ARPA (обратите внимание, что IP-адрес записан в обратном порядке).

Итак, мы создаем еще один файл зоны (для зоны, например, 0.48.192.IN-ADDR.ARPA), копируем в него запись `SOA` (а заодно и `NS`), после чего начинаем писать:

```
1 IN PTR major.mycompany.ru.
2 IN PTR colonel.mycompany.ru.
...
```

Можно задавать не только относительные, но и абсолютные имена:

```
3.0.48.192.IN-ADDR.ARPA. IN PTR general.mycompany.ru.
```

Не забудьте еще задать обратное преобразование для 127.0.0.1.

Обратите внимание на то, что право на ведение "прямого" домена не зависит от провайдера — его выдает организация, ведающая распределением имен в нужном вам домене. А вот пул IP-адресов находится в ведении провайдера, и именно провайдер делегирует (или не делегирует) вам права на ведение реверсной зоны. В связи с тем, что зачастую клиентам выдается не целая сеть класса "C", а ее часть, то и реверсная зона находится на сервере провайдера. Так что вам придется наладить с ним взаимодействие в области обновления данных.

Настройте трансфер зоны

Напоследок — одно маленькое замечание. Исследование DNS является одним из первых этапов "изучения сети" при подготовке ее взлома. Чаще всего используется перенос зоны, при котором все записи зоны передаются на компьютер "исследователя", где он их может изучать в спокойной обстановке. Поэтому имеет смысл (помимо всего прочего) настроить брандмауэр на запрет TCP-соединений по 53 порту с несанкционированных адресов (в запросах на определение имен используется UDP, а для переноса зоны — TCP).

Для того чтобы посмотреть, что записано в DNS, используется команда `nslookup` (она есть и в UNIX, и в Windows).

Веб-интерфейс для управления сервером

Для серверов на базе Linux, как и для Windows-серверов, разработаны средства для удаленного управления. В том числе есть средства для управления через Интернет, так называемые веб-интерфейсы. Заслуживает внимания тот факт, что эти средства могут применяться и локально. Причем в некоторых случаях веб-интерфейс оказывается удобнее локального, позволяет увидеть множество параметров сервера, доступ к которым стандартными средствами

не так прост. Один из самых распространенных веб-интерфейсов для управления Linux-сервером — Webmin. Вы можете посетить сайт **www.webmin.com**, где можно ознакомиться с этой замечательной системой, что называется, из первых рук. Webmin может использоваться в нескольких десятках версий Linux. Клиентская часть работает из любого браузера с любого компьютера, где есть браузер и доступ в сеть.

Простое перечисление функций Webmin займет не одну страницу, поэтому подробно рассмотреть работу с этим интерфейсом в этой книге не представляется возможным. Тем не менее, приведем здесь небольшой пример работы через Webmin с уже знакомым нам сервером Samba.

Для того чтобы можно было использовать Webmin, как и для веб-сервера, должна быть запущена служба httpd. Открыв браузер, введите в адресной строке IP-адрес компьютера или его имя в сети и укажите порт 10000. Для локального подключения это **http://localhost:10000**, а для удаленного, например, — **http://192.48.1.200:10000**. При подключении откроется страница авторизации, где следует указать имя пользователя и пароль. До определения пользователей Webmin по умолчанию может быть пользователь root с пустым паролем. После авторизации откроется окно Webmin, в его меню выберем **Службы**. Страница, которую вы увидите, показана на рис. 4.28.

Среди значков, расположенных на этой странице, выберите **Файл-сервер Samba.** При этом откроется окно **Менеджер ресурсов Samba** (рис. 4.29).

Выбрав под таблицей ресурсов сервера ссылку **Просмотр всех соединений**, вы увидите страницу **Текущие пользователи** с таблицей (рис. 4.30), где показаны все текущие подключения к серверу. В столбце **Открытые файлы** описаны все открытые каталоги и файлы. На этой странице вы имеете возможность отключить пользователей от сервера.

Если в окне **Менеджер ресурсов Samba** (рис. 4.29) выбрать значок **Настройка автоматической синхронизации пользователей Unix и Samba**, то в открывшемся окне **Синхронизация пользователей** (рис. 4.31) можно указать серверу автоматически добавлять пользователей компьютера в число пользователей сервера Samba. Эта возможность доступна только через Webmin.

Рассмотрите внимательно страницы Webmin, вы увидите еще много удобств, которые система предоставляет администратору.

> ***Примечание***
>
> В некоторых версиях Linux Webmin по умолчанию устанавливается с применением протокола SSL, обеспечивающего безопасный доступ к компьютеру через локальную сеть и Интернет. В этом случае доступ к Webmin с локальной машины возможен по адресу **https://localhost:10000**. Также для входа в Webmin от имени пользователя по умолчанию (root) может понадобиться и его пароль.

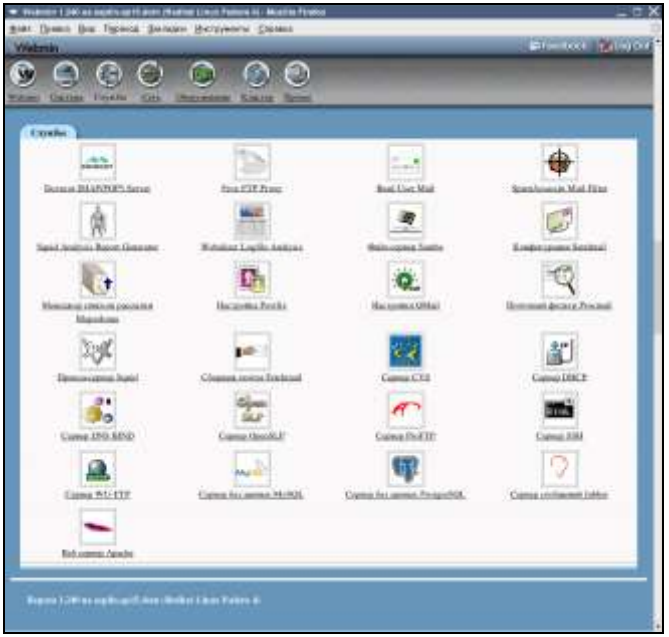


Рис. 4.28. Окно **Webmin**, страница **Службы**

Рис. 4.29. Окно **Менеджер ресурсов Samba**

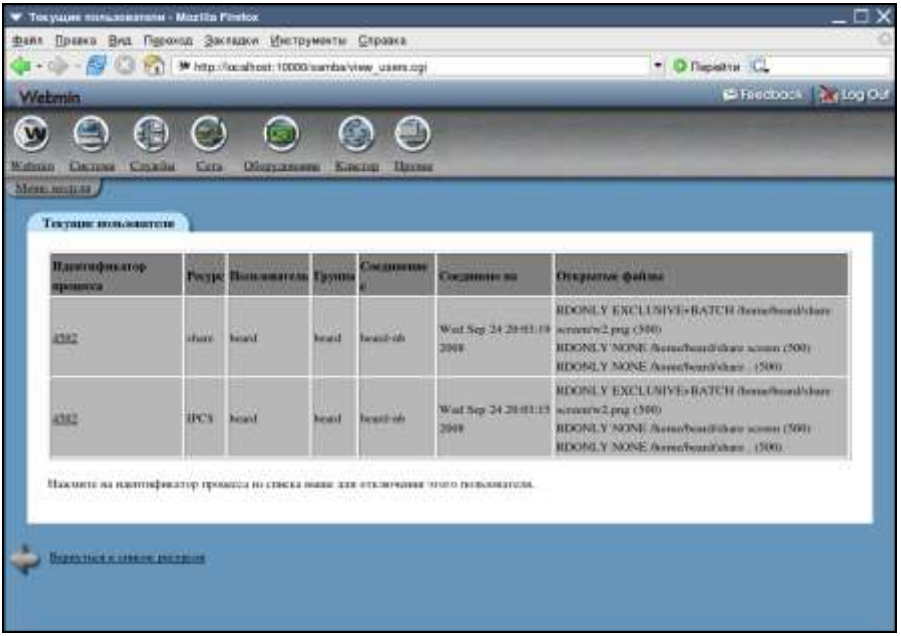


Рис. 4.30. Окно **Текущие пользователи**

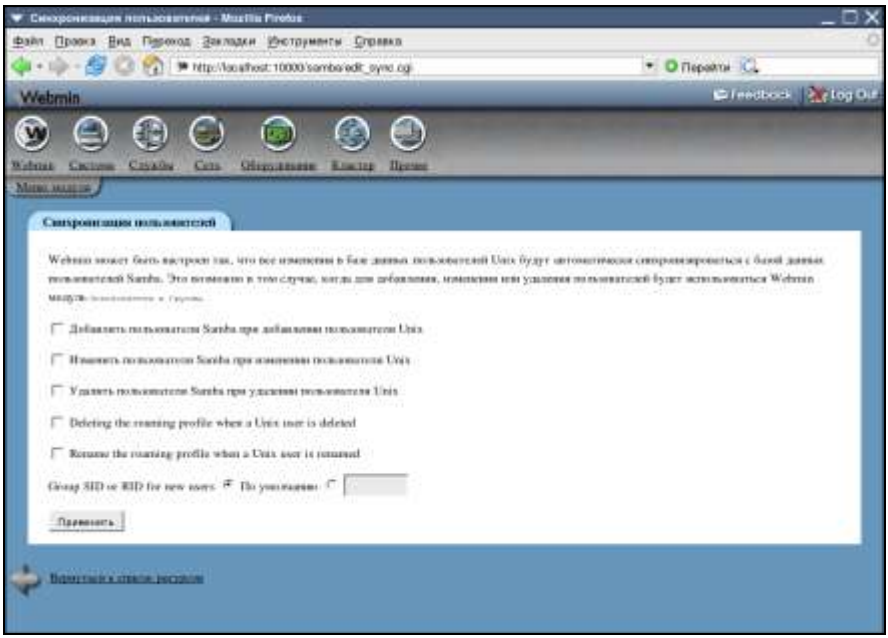


Рис. 4.31. Окно **Синхронизация пользователей**

Сервер общего доступа в Интернет

Компьютер на базе ОС Linux с успехом можно применить для обеспечения подключением к Интернету рабочих станций локальной сети, — создания шлюза в Интернет. Здесь возможностей нисколько не меньше, чем в Windows. Важно только обеспечить сервер двумя сетевыми интерфейсами. Один должен смотреть в сторону Интернета, а другой — в локальную сеть. Каким образом шлюз будет подключен к глобальной сети, значения не имеет. Это может быть модем для коммутируемых линий, выделенная линия, ADSL-модем и другие варианты. Возможно, что компьютер подключен к Интернету через другую локальную сеть, — и в этом случае он может быть шлюзом в Интернет для вашей локальной сети. В данном примере сервер небольшой локальной сети во внешней ЛВС играет роль рядового компьютера. Такой вариант работы вашего сервера возможен, если доступ в Интернет осуществляется через районную или городскую сеть, а у вас задача — обеспечить подключением к Интернету все домашние компьютеры и гостевые ноутбуки.

Настройка доступа возможна штатными средствами системы через графические утилиты или путем редактирования конфигурационных файлов. Но для пользователей Windows удобнее производить настройки средствами утилиты Firestarter, предоставляющей графический интерфейс к настройкам маршрутизации и сетевого экрана (iptables). Утилита доступна на сайте **http://www.fs-security.com/**, где представлены версии для нескольких версий Linux. Для ASPLinux 11 следует выбирать установочные файлы для Red Hat Enterprise Linux 4. На момент написания этих строк файл для скачивания имел имя firestarter-1.0.3-1.i386.rpm. Устанавливается утилита стандартными средствами системы. Если вы используете более поздние выпуски ASPLinux, для установки можно выполнить команду `# yum install firestarter`.

На сайте программы сказано, что Firestarter может использоваться для настройки шлюза или выделенного межсетевого экрана (firewall). В Firestarter есть мастер настройки, монитор событий реального времени, настройка общего доступа к Интернету, настройка DHCP-сервера и настройка внешних и внутренних политик. Эти дополнения делают программу весьма удобным инструментом для настройки сервера общего доступа к Интернету для небольшой сети.

Мастер настройки

После завершения установки выберите в меню **Программы** | **Firestarter** (в других версиях Linux возможно другое расположение этого пункта меню). При первом запуске Firestarter запустится мастер настройки. Так как межсе-

тевой экран (firewall) должен запускаться от имени администратора, т. е. root, мастер потребует ввести пароль суперпользователя. Мастер настройки проведет вас через простой процесс базовой настройки системы. После приветствия программы, нажмите кнопку **Forward** (Вперед). Появится диалоговое окно **Network Device Setup**, где будет приведен список найденных сетевых устройств, а также два флажка. Первый флажок означает, запускать ли firewall при дозвоне (если используется модем). Установка второго флажка означает, что IP-адрес будет получен динамически: либо от DHCP-сервера интернет-провайдера, либо от DHCP-сервера вашей сети. Выберите из списка сетевое устройство, которое расположено на стороне Интернета, и нажмите **Forward**. Мастер настройки запускается сам при первом запуске, а также его можно запустить из Страницы статуса **Firestarter**, меню **Firewall | Run wizard.** Вы всегда можете его использовать для корректировки основных настроек программы.

Диалоговое окно **Internet Connection Sharing** позволяет настроить общий доступ к Интернету, используя систему в качестве шлюза. Для второго сетевого адаптера следует указать, что это устройство обращено к внутренней сети. Единственный флажок здесь позволяет включить или выключить DHCP-сервер в локальной сети. Последнее диалоговое окно **Ready to start your firewall** (Ваш firewall готов к запуску) позволяет сохранить указанные настройки с помощью кнопки **Save** (Сохранить) и запустить firewall, после чего появляется окно **Firestarter**, где можно включить настройку **Minimize to tray on windows close** (Минимизировать в лоток при закрытии окна). После этого нажатие на кнопке закрытия окна будет приводить не к завершению программы, а к минимизации ее в лоток. В лотке появится значок, отображающий статус межсетевого экрана: запущен, остановлен или заперт. Запирание firewall приводит к запрещению всех входящих и исходящих соединений. Чтобы включить функцию минимизации, выберите **Edit | Preferences** либо нажмите кнопку **Preferences** (рис. 4.34). Затем в разделе **Interface** включите **Minimize to tray on windows close** и нажмите **Accept** (Принять).

Просмотр событий

Одна из наиболее полезных функций Firestarter — это способность в реальном времени отображать происходящие сетевые события. Для просмотра событий выберите вкладку **Events** на странице статуса (рис. 4.32). По умолчанию показаны пять (время, порт, источник, протокол и сервис) из 11 столбцов. Столбцы могут быть настроены в разделе **Show Column** пункта

меню **Events**. События раскрашены в разные цвета в зависимости от серьезности события:

- серые события безобидны (например, широковещательные пакеты);
- черные события — постоянные попытки подключения к случайному порту;
- красные события — возможные попытки обращения к закрытым службам.

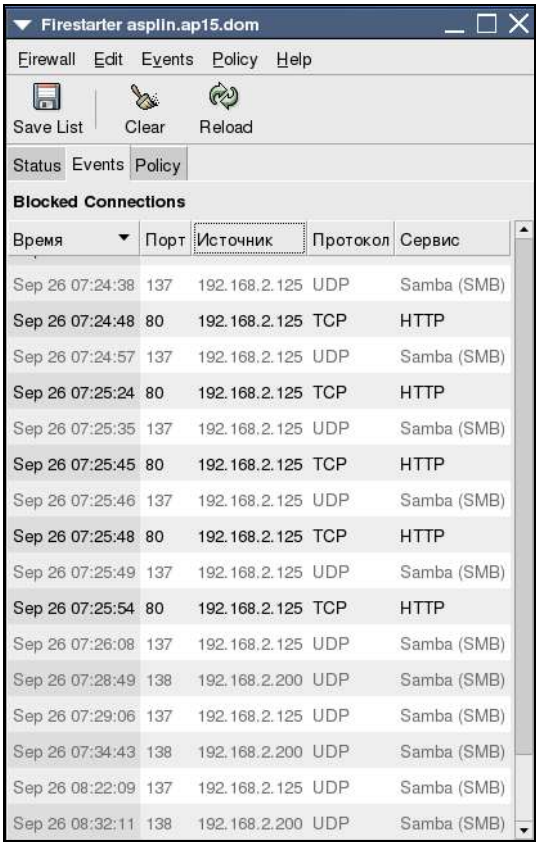


Рис. 4.32. Окно **Firestarter**, вкладка **Events**

Количество отображаемых событий может быть уменьшено с помощью настроек **Skipping redundant entries** (Пропускать повторяющиеся события) и **Skip entries where the destination is not the firewall** (Пропускать записи, приемником которых является не файрволл). На рисунке видны события обращения компьютера малой сети с IP-адресом 192.48.2.200 к серверу по портам 80 (подключение к веб-серверу), 137 и 138 (обращение к файловым

ресурсам сервера). Красных строк нет, поскольку все эти события описывают разрешенные обращения.

Разрешение доступа

Разрешить доступ в оснащенной файрволлом системе возможно двумя путями: либо посредством страницы **Policy** (Политики), либо **Events** (События). Чтобы разрешить HTTP-соединения с определенного компьютера, щелкните правой кнопкой мыши на компьютере-источнике и выберите **Allow inbound service for source** (Разрешить эту службу для источника). Это приведет к созданию политики разрешения HTTP-соединения только с выбранного компьютера; можете проверить это, посмотрев вкладку **Policy** (Политики) (рис. 4.33).

Рис. 4.33. Окно **Firestarter**, вкладка **Policy**

Так как SMB (служба обмена файлами в Windows) использует несколько портов, легче разрешить доступ, создав соответствующее правило на странице политик. Выберите вкладку **Policy**, затем выберите раздел **Allow service** (Разрешить службу) и нажмите кнопку **Add Rule** (Добавить правило). В диалоговом окне **Add new inbound rule** выберите **Samba (SMB)** из выпадающего меню и оставьте значение по умолчанию **Anyone** (Доступно всем). Наконец, нажмите кнопку **Add** для добавления правила и закрытия окна. Нажатие кнопки **Apply Policy** (Применить политику) включает действие только что добавленного правила.

Страница политик также позволяет включить полный доступ с определенных компьютеров или подсетей. Хотя более безопасно открывать лишь службы, которые нужны отдельным машинам, вместо открытия полного доступа группе машин.

На вкладке **Status** (рис. 4.34) всегда можно увидеть общую информацию о работе Firewall, информацию о принятых и переданных пакетах по сетевым интерфейсам, а также информацию об активных подключениях (**Active connections**).

Рис. 4.34. Окно **Firestarter**, вкладка **Status**

В рассматриваемом примере активны подключения к сервису в Интернете по порту 2041 (Mail.ru агент), подключение к веб-сайту по адресу 77.242.193.129 и по порту 445, который используется службой lanman (клиент для сетей Microsoft).

Другие возможности

Настроив шлюз в Интернет, можно настроить еще одну полезную функцию на вкладке политик в разделе **Forward Service** (Служба переадресации) (на рис. 4.33 нижний раздел). Все компьютеры в локальной сети разделяют один IP-адрес посредством трансляции сетевого адреса (Network Address Translation, NAT). NAT позволяет направить пакеты отдельных служб из внешних сетей к определенным компьютерам локальной сети. Это может быть установленный на одном из компьютеров сети веб-сервер или почтовый сервер или любой другой сервис, который вы решите предоставить для пользователей внешних сетей, включая Интернет.

Таким образом, возможности сервера на базе ОС Linux во многих случаях совпадают с возможностями Windows-сервера. И только от вашего решения зависит — Linux или Windows будут управлять вашей сетью. Иногда на решение может повлиять случайно обнаруженный факт, подробность из опыта других пользователей. Известно, что настройка почтового сервера Sendmail в Linux — задача весьма трудоемкая, в то же время под Windows существует несколько популярных почтовых серверов, включая встроенный в Windows Server 2003. Но и для Linux существуют другие решения, например почтовый сервер Qmail, который считается более безопасным, чем Sandmail. Также распространен сервер Postfix, который обычно устанавливается в небольших сетях и даже просто на рабочих станциях, вполне может работать и на серверах в Интернете. Это полноценная почтовая система, предназначенная для замены сервера Sendmail. Postfix, в отличие от Sendmail, разработанного как монолитная программа, состоит из нескольких небольших программ, каждая из которых выполняет свою задачу. В этом сходство Postfix с Qmail, но по сравнению с ним он более экономно распоряжается ресурсами системы. Подробно о Postfix можно почитать на официальном сайте разработчиков программы по ссылке **http://www.postfix.org**. Кроме того, есть форум на **http://www.postfix.ru**. Очень хорошая статья "Настраиваем почтовый сервер на Debian" находится по адресу в Интернете: **http://www.drivermania.ru/articles/nastraivaem-pochtovij-server-na-debian.html**. В этой статье описывается настройка полноценного почтового сервера на базе Debian Linux. В зависимости от потребностей сети Postfix может быть установлен в различных вариантах, каждый из которых требует для реализации своего набора

модулей. В одних случаях процесс настройки сервера может быть длительным, в других можно уложиться за 10 минут. По адресу **http://www.linuxrsp.ru/artic/postfix.html** находится еще одна полезная статья Колисниченко Дениса — "Postfix за 10 минут", которую и приведем здесь.

Postfix за 10 минут

Postfix является агентом доставки почты (Mail Transfer Agent, MTA), который используется по умолчанию во многих дистрибутивах, например, дистрибутиве ALT Linux. Мы знаем, что кроме Postfix существует другой MTA — Sendmail, который является стандартом де-факто на почтовые агенты. Если Sendmail в основном используется на крупных почтовых серверах (в основном из-за традиции, поскольку Postfix при надлежащей настройке будет выполнять большинство функций Sendmail), то Postfix в основном устанавливается на рабочих станциях для выхода в Internet.

В этой статье мы не будем рассматривать настройку Postfix для сервера, а займемся решением простой практической задачи, с которой может столкнуться любой домашний пользователь Linux. Если на предприятии настройка сервера возложена на плечи администратора, то дома "сам себе root", поэтому если сам не настроишь, никто за тебя не настроит.

Предположим, что у нас есть два локальных пользователя: ivanov и petrov. У Иванова есть два почтовых ящика — один на сервере провайдера (ivanov@isp.ru) и один на Mail.Ru (ivanov2004@mail.ru). У Петрова только один почтовый ящик — на сервере провайдера (petrov@isp.ru). Нужно настроить почтовую подсистему так, чтобы письма Иванова получал локальный пользователь ivanov, а письма Петрова — пользователь petrov. Также нужно обеспечить отправку писем, а именно чтобы письма отправлялись, когда установлено соединение с Интернетом. Другими словами, Иванов и Петров могут в любое время написать письмо, но оно будет отправлено только, если установлено соединение.

Почему мы будем использовать Postfix, а не Sendmail? Во-первых, Postfix, скорее всего, уже установлен, поскольку сейчас он устанавливается в большинстве дистрибутивов по умолчанию, и нам не нужно тратить время на его установку. Во-вторых, Postfix очень прост в настройке, в чем вы сейчас убедитесь.

Начнем с настройки Postfix, который будет отвечать за доставку писем. Откройте файл /etc/postfix/mail.cf и измените параметры (если их там нет, добавьте):

```
defer_transport=smtp
relayhost = smtp.isp.ru
```

Эти две строчки говорят Postfix, что для отправки писем будет использован протокол SMTP (Simple Mail Transfer Protocol) и письма будут отправляться через почтовый сервер провайдера — smtp.isp.ru.

Теперь приступим к настройке программы fetchmail, которая будет получать письма Иванова и Петрова и раскладывать их "по полочкам". Если у вас не установлена программа fetchmail, самое время ее установить. После установки в домашнем каталоге пользователя root создайте файл .fetchmailrc:

```
set postmaster "postmaster"
set bouncemail
set no spambounce
poll pop.isp.ru with proto POP3
       user 'ivanov' there with password 'passwd77' is ivanov here

poll pop.mail.ru with proto POP3
       user 'ivanov2004' there with password 'mailru-passwd' is iva-
nov here

poll pop.isp.ru with proto POP3
       user 'petrov' there with password 'my_pAsWd' is petrov here
```

Теперь осталось установить алиас для пользователя root: чтобы почту root'а читал пользователь ivanov. Для этого в файл /etc/postfix/aliases добавьте строку:

```
root: ivanov
```

Перезапустите `postfix: service postfix restart`.

Все, настройка завершена. После установления соединения с Интернетом, зарегистрировавшись как ivanov, введите команду (в терминале) `su -c fetchmail`. Затем нужно ввести пароль пользователя root, и программа fetchmail получит письма Иванова и Петрова. В это же время Postfix автоматически отправит исходящие сообщения, если таковые имеются. Вывод программы fetchmail выглядит так:

```
1 message for ivanov at pop.isp.ru (6050 octets).
reading message 1 of 1 (6050 octets) ...... flushed
1 message for ivanov at pop.mail.ru (2077 octets).
reading message 1 of 1 (2077 octets) .. flushed
fetchmail: No mail for petrov at pop.isp.ru
```

Как видите, в данном случае не используется графический интерфейс. Все настройки выполняются в окне терминала или консоли. Это может поначалу отпугнуть пользователей Windows, но, освоившись в Linux, вы увидите, что это не самый сложный способ общения с компьютером. Более того,

в программах, имеющих множество параметров для настройки, с множеством предусмотренных разработчиками режимов работы, пожалуй, командная строка и конфигурационные файлы окажутся более удобным инструментом, чем GUI. Ранее в этой главе мы упоминали о графическом веб-интерфейсе Webmin. Если вы установили его, то рассмотрите его возможности по настройке Postfix. Огромное число параметров, где необходимо установить их значение или указать вариант применения. Все равно потребуется чтение дополнительной литературы, нужно будет вникать в описания конфигурационных файлов… Проще, возможно, настроить систему, установив необходимые компоненты и отредактировав конфигурационные файлы. Впрочем, "Каждому фрукту — свой овощ".

Linux — ретранслятор файлов

В Windows и Linux файловые системы имеют существенные отличия. Особенности файловой системы Linux позволяют иногда простым путем решать задачи, которые в Windows не имеют таких простых решений.

Конечно, файловые ресурсы всех компьютеров, работающих в сети, могут иметь общий доступ. Но, если каталоги общего доступа с разных машин должны быть постоянно доступны любому пользователю сети, есть возможность упростить для них эту задачу, создав видимость расположения всех ресурсов на одном файловом сервере. Это позволит не только упорядочить доступ к файлам и каталогам, но и упростить настройку доступа к ним. Все компьютеры сети настраиваются для доступа к каталогам сервера, к которым монтируются новые сетевые ресурсы. При этом пользователь сети может не знать истинного расположения ресурсов, да ему это и не очень надо. Важно, что, однажды настроив компьютеры пользователей, администратору не придется повторно выполнять эту работу, если появятся новые файлы для общего доступа на новых компьютерах. Кроме того, можно на сервере монтировать каталоги FTP-серверов, различные диски и т. п.

Общие каталоги будут одинаково доступны пользователям с любыми операционными системами. Файловый сервер становится ретранслятором ресурсов сети. Возможно, что кого-то заинтересует, что адреса ретранслируемых ресурсов скрыты от конечного пользователя.

В рассматриваемом примере участвуют три компьютера:

- BeardM — компьютер под управлением Mandriva Linux, выполняющий роль файлового сервера;
- Beard-NB — компьютер под управлением Windows Vista, файлы которого необходимо предоставить в общий доступ через сервер;

- BeardMM — компьютер под управлением Linux, получающий доступ к общим ресурсам.

Процедура настройки ретранслятора состоит в следующем.

1. На компьютере Beard-NB создан каталог общего доступа с сетевым именем share.
2. На компьютере BeardM в домашнем каталоге текущего пользователя создан каталог //home/beard/shrvista/, для него определен общий доступ.
3. От имени пользователя root в окне терминала или в консоли введена команда

   ```
   mount -t cifs //BEARD-NB/share -o us-
   er=username,pass=password,domain=DOMAIN //home/beard/shrvista
   ```

   с помощью которой монтируется сетевой ресурс.
4. Через **Центр управления Mandriva Linux | Сетевые службы | Настройка SAMBA** смотрим сетевое имя каталога //home/beard/shrvista/.
5. Теперь по этому имени он будет виден при подключении к компьютеру BeardM по сети с любого другого компьютера, в том числе и с BeardMM.

Если потребуется прекратить доступ к файлам компьютера Beard-NB, достаточно в терминале на BeardM ввести команду `umount -t cifs //BEARD-NB/share`.

Удаленное подключение к Linux из Windows с помощью Xming и SSH

Нет, это не вариант VNC. И подключаться будем не к рабочему столу, а сразу запускать требуемые приложения. Эта технология основана на том, что в Linux графическая оболочка не является частью ядра системы. Оконная система для Linux — X Window System берет на себя отрисовку графических элементов и взаимодействие с устройствами ввода/вывода. Эта система имеет клиент-серверную архитектуру. Оконная система выполняет роль сервера, а графические приложения — роль клиентов, которые подключаются к серверу и взаимодействуют с ним, получая рисунки своих окон и события мыши и клавиатуры.

Раз уж сервер и клиент, то и работать они могут на разных машинах, общаясь через сеть. Значит, должна быть возможность запускать приложение на удаленном компьютере, получая его окна на локальном. Или запускать программу на одном удаленном компьютере, а интерфейс программ показать на другом удаленном компьютере.

Для реализации этой возможности требуется совсем не много. На удаленном компьютере необходимо установить SSH-сервер, который вы найдете в программе установки и удаления по имени openssh-server. На локальном компьютере следует установить SSH-клиент и X-сервер для Windows.

Теперь можем переходить к подготовке компьютера Windows. Здесь нужно установить две программы.

- SSH-клиент PuTTY, который можно найти на странице **http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html**.

  Программа не требует инсталляции, просто поместите ее в каталог, из которого будете ее запускать.

- X Server для Windows Xming, загрузив его со страницы **http://www.straightrunning.com/XmingNotes/**.

  Для работы X-сервера необходимо загрузить и установить два файла — Xming и Xming-portable-PuTTY.

Теперь можно установить соединение с удаленным компьютером по SSH. Для этого запустите PuTTY и введите IP-адрес компьютера Linux в поле **Host Name (or IP addres)** в разделе **Session** (рис. 4.35).

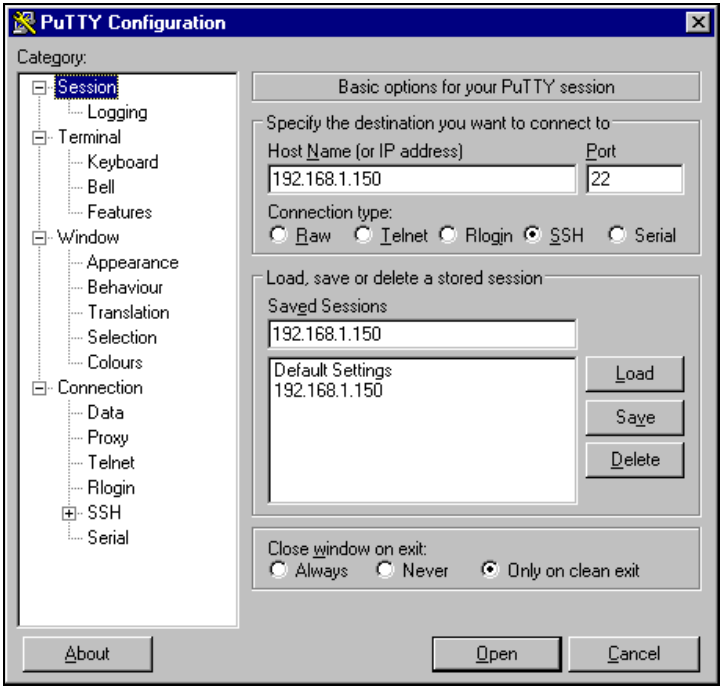


Рис. 4.35. Окно **PuTTY Configuration**

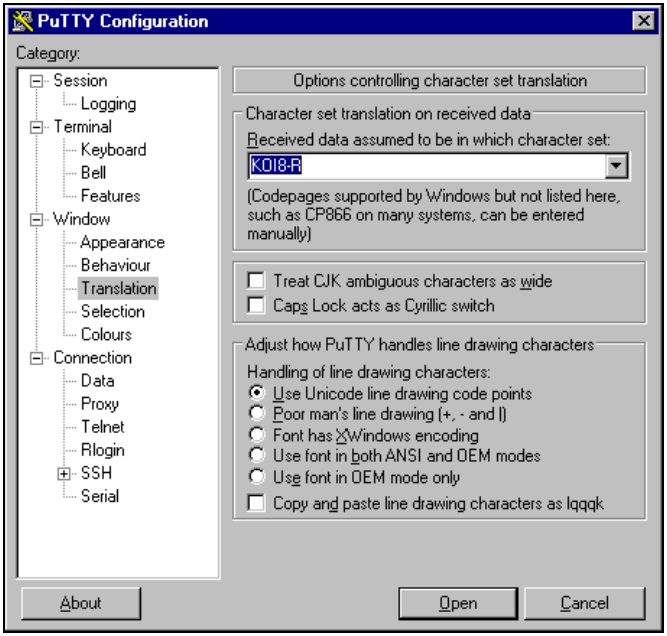


Рис. 4.36. Окно **PuTTY Configuration**, раздел **Window | Translation**

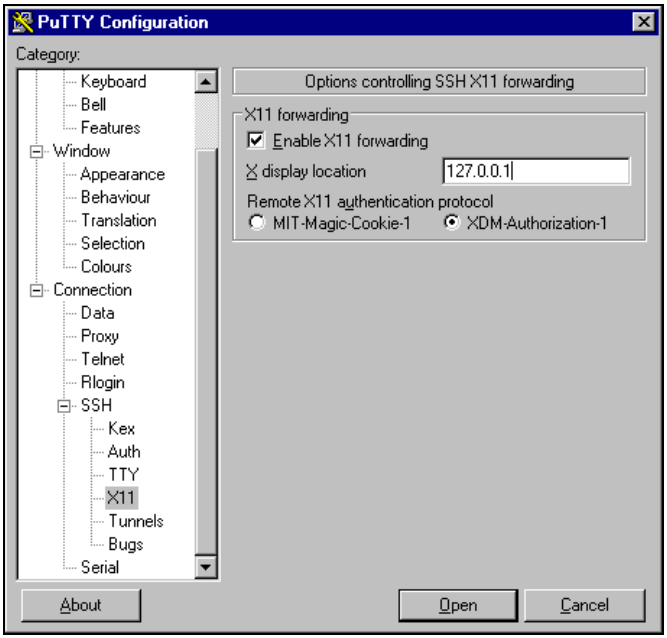


Рис. 4.37. Окно **PuTTY Configuration**, раздел **Connection | SSH | X11**

Для корректного отображения кириллицы, желательно в разделе **Window | Translation** установить кодировку, которая применяется на удаленной машине (рис. 4.36).

В разделе **Connection | SSH | X11** включаем перенаправление графического интерфейса. В качестве расположения X-сервера вводим IP-адрес компьютера Windows, за которым сейчас сидим (рис. 4.37).

Возвращаемся в раздел **Session**, сохраняем настройки и подключаемся к компьютеру Linux. В случае успешного подключения мы вводим логин и пароль и видим текстовую консоль, в которой можем удаленно запустить консольные программы, например, MC, как на рис. 4.38.

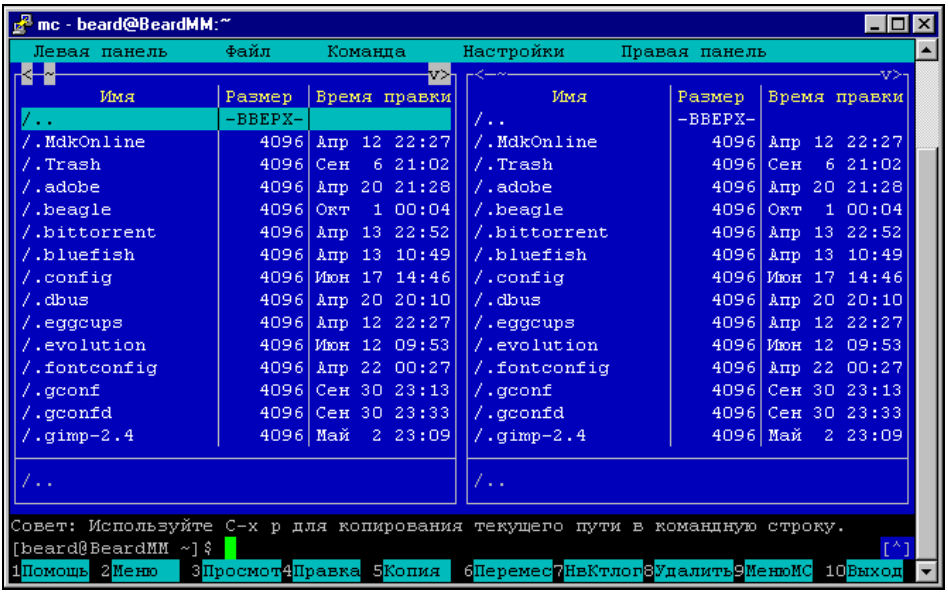


Рис. 4.38. Окно текстовой консоли с программой MC

Для графических приложений с графическим интерфейсом необходим X-сервер. Настроим Xming.

Запустите программу XLaunch — мастер настроек. На первом шаге указываем способ интеграции в графическое окружение Windows. Выберем вариант **Multiple windows**, когда каждая запущенная программа отображается в своем окне (рис. 4.39).

На втором шаге (рис. 4.40) нам предлагается автоматически запускать какое-нибудь приложение вместе с X-сервером. Пока отказываемся от этого предложения.

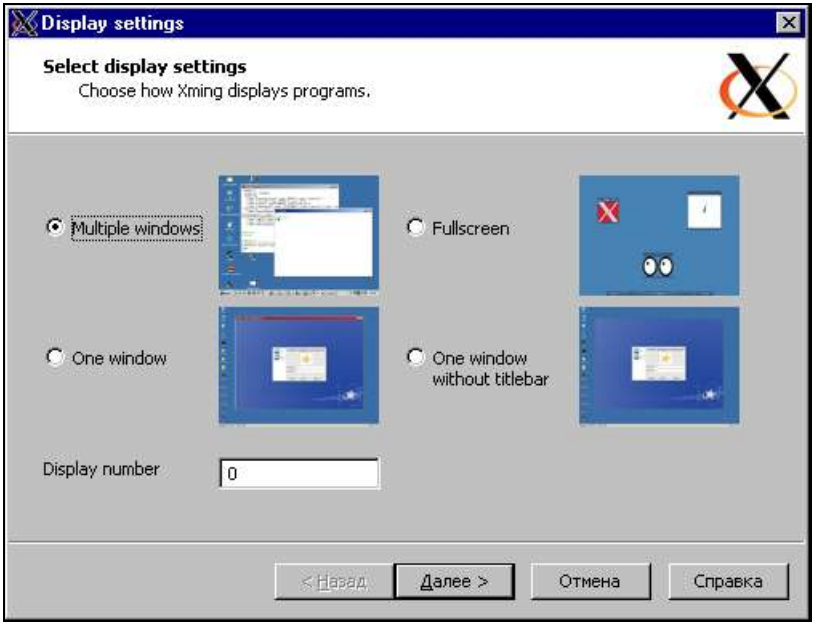


Рис. 4.39. Окно **Display settings** программы XLaunch

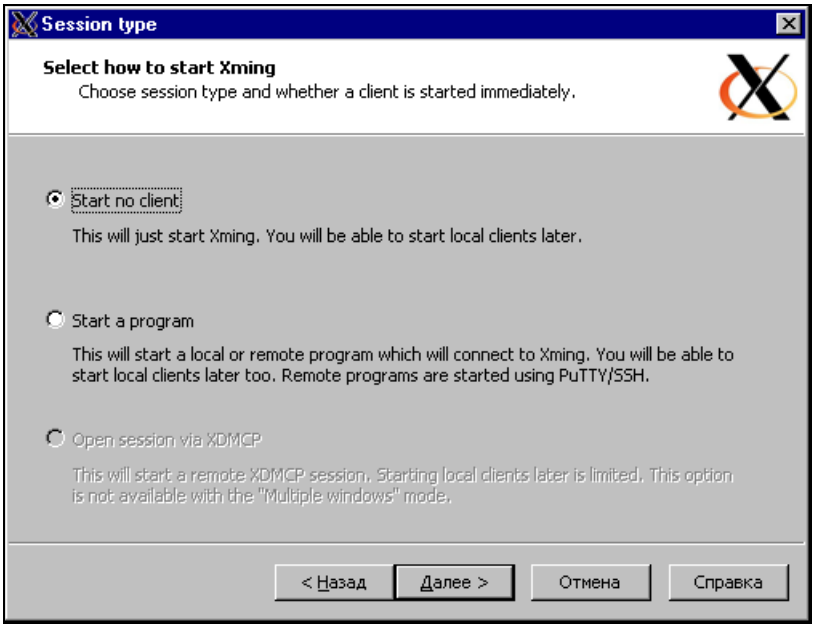


Рис. 4.40. Окно **Session type**

На третьем шаге требуется указать параметры запуска Xming (рис. 4.41). Опция **Clipboard** позволяет интегрировать буфер обмена. Для обеспечения комфортной работы в удаленном режиме в поле **Additional parameters for Xming** введите через пробелы следующие параметры:

- `-dpi 96` — чтобы поправить размер шрифтов;
- `-xkblayout us,ru` — для работы с двумя раскладками клавиатуры;
- `-xkbvariant basic,winkeys` — вид клавиатуры;
- `-xkboptions grp:caps_toggle` — переключение раскладки клавишей <Caps Lock>.

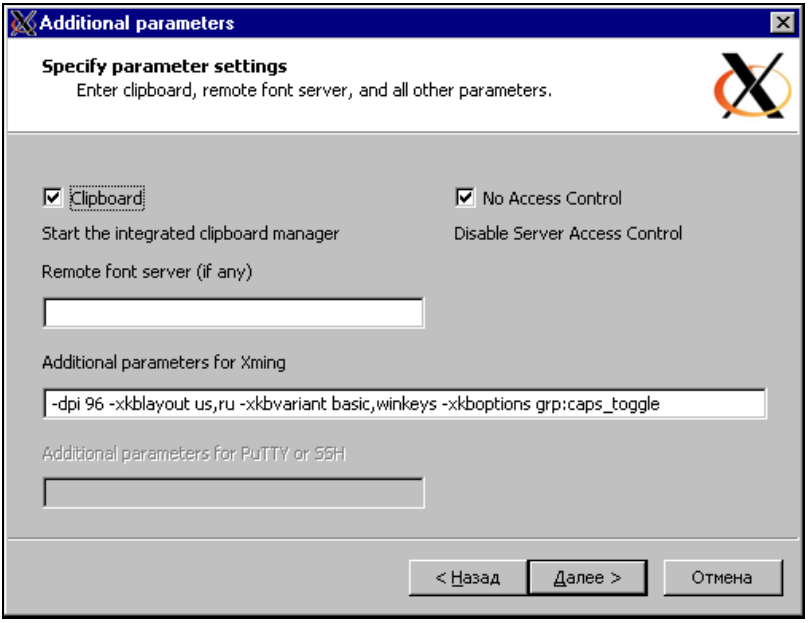


Рис. 4.41. Окно **Additional parameters**

И, наконец, на следующем шаге в окне **Finish configuration** (рис. 4.42) сохраняем настройки кнопкой **Save configuration** и запускаем X-сервер кнопкой **Готово**. В системном лотке появится иконка Xming. В дальнейшем запустить сервер с теми же настройками можно просто путем открытия сохраненного файла. Изменить настройки можно через контекстное меню файла.

X-сервер запущен. Возвращаемся в консоль, предоставленную соединением SSH. Попробуйте набрать команду запуска оконного приложения, например `kwrite &`, `gedit &` или `firefox &` (рис. 4.43). Одна из этих программ навер-

няка есть на вашем удаленном компьютере. Амперсанд в конце команды указывает, что программу запускаем в фоновом режиме, чтобы во время ее работы консоль была доступна для других действий.

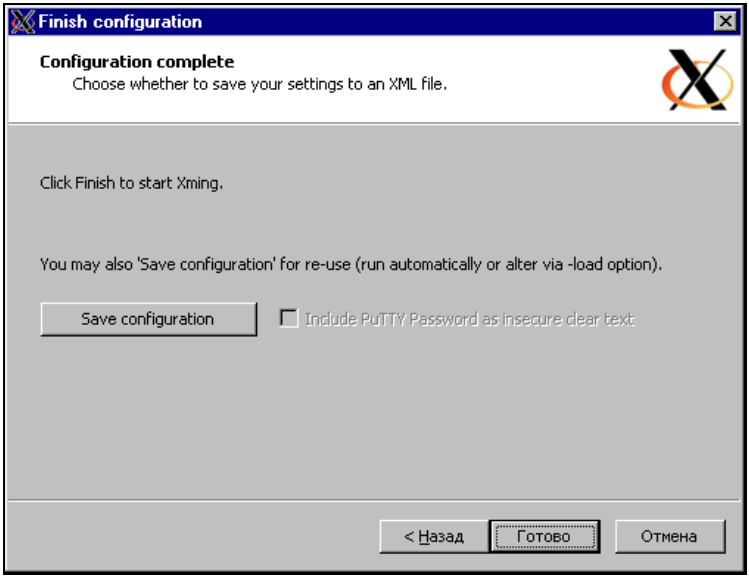


Рис. 4.42. Окно **Finish configuration**

Рис. 4.43. Окно консоли SSH — команда запуска приложения

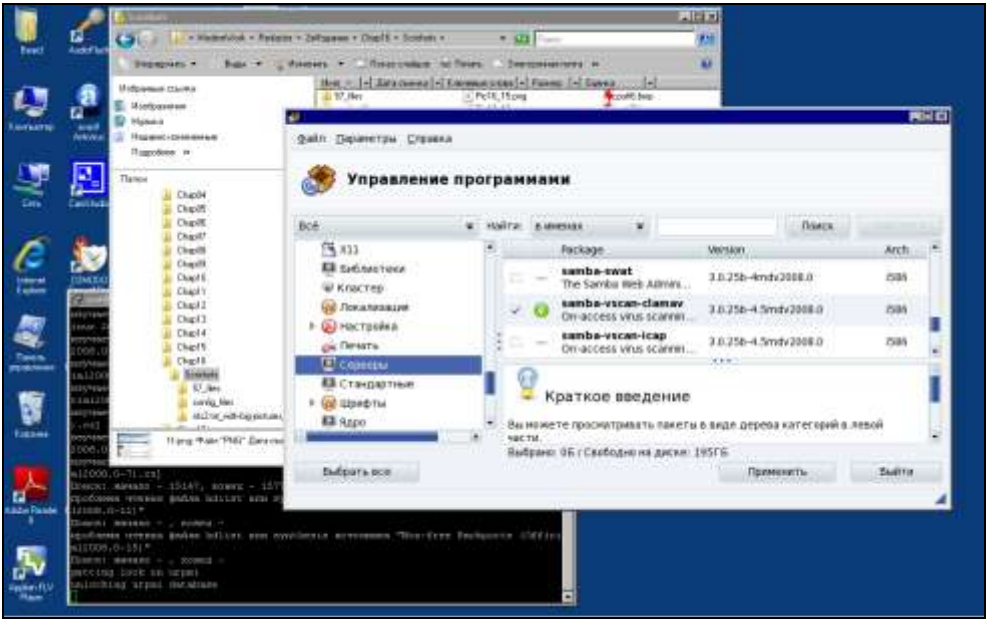


Рис. 4.44. Рабочий стол Windows Vista и окно **Управление программами** Mandriva Linux

Если получилось, пробуйте запустить и другие приложения. Вполне возможно получить доступ к графическим средствам управления системой. Так на рис. 4.44 показано окно **Управление программами** Mandriva Linux на рабочем столе Windows Vista. Эту программу можно вызвать командой `/usr/bin/rpmdrake`, введя ее в окне консоли SSH и нажав <Enter>.

Описанный способ удаленной работы с Linux-приложениями из Windows расширяет возможности Linux-сервера. Его теперь можно использовать и как сервер приложений. Каждый зарегистрированный на сервере пользователь может получить доступ к своим каталогам и приложениям в соответствии с назначенными ему правами.

Глава 5

Еще о сервере

В небольшой сети может быть достаточно функций сервера, описанных в *главе 4*. Тем не менее, вам могут потребоваться другие серверы. Например, сервер виртуальных машин, где могут работать в виртуальном виде несколько компьютеров с какими-либо особенными настройками, или сервер авторизации с единой для всей сети базой данных пользователей. Эти серверы могут быть созданы, если установлены соответствующие компоненты или программы.

Сервер виртуальных машин

Пожалуй, наиболее подходящим для малой сети можно считать VMware Server 2. Это хотя и не открытый, но бесплатный продукт, который можно загрузить с сайта **http://www.vmware.com**, бесплатно зарегистрировавшись на нем. Доступны дистрибутивы как для Windows, так и для Linux. Процедура установки из RPM-пакета в операционной системе CentOS наиболее проста по сравнению с другими бесплатными версиями Linux. В Windows установка сервера совсем не вызывает проблем. Существуют и другие программы для организации виртуального сервера, например Virtual Box, которая очень хорошо работает под управлением Linux Debian, Linux Ubuntu, Linux Mint 7. Устанавливая виртуальный сервер под ОС Windows, можно испытать несколько версий Linux, не переустанавливая систему на базовой машине. И наоборот, установив его под Linux, можно при необходимости использовать виртуальный компьютер Windows.

Зачем столько внимания какой-то виртуальной системе? — спросите вы. На самом деле, что, кроме возможности проводить эксперименты с различными ОС, может дать виртуальная машина серверу?

А дать она может много, и даже очень много. Попробуем перечислить преимущества, которые можно получить, используя виртуальную машину для сервера.

- Возможность моментального восстановления сервера в рабочее состояние после вирусной атаки, атаки хакеров или другой причины, приведшей к серьезным проблемам на сервере. Эта возможность достигается всего лишь копированием рабочего файла диска виртуальной машины и заменой испорченного на исправленную копию, при необходимости.
- Возможность размещения на одном физическом сервере более одного виртуального сервера. Это могут быть веб-сервер и пара серверов, принадлежащих разным подсетям. Серверы, несмотря на размещение на одной машине, совершенно независимы друг от друга. Единственное ограничение — число виртуальных серверов. Это ограничение обусловлено ресурсами хост-машины. Реальный компьютер должен обладать ресурсами, достаточными для обеспечения одновременной работы виртуальных машин. Одновременно на одной базовой машине можно запускать не более четырех виртуальных машин на ядро процессора.
- Возможность быстрой замены сервера на другую версию. Это может быть полезно при обучении пользователей, когда в течение одного занятия необходимо рассмотреть работу и настройки двух-трех вариантов сервера. При этом учащиеся могут совершенно безбоязненно самостоятельно проводить настройки сервера. Даже самые грубые ошибки не приведут к серьезным проблемам, ведь заменить сервер очень просто!
- Упрощение настроек базового физического сервера (хост-машины), что, в свою очередь, ускоряет и упрощает восстановление работоспособности сервера при серьезной аварии. Повышение надежности базового сервера. Вызывающие нестабильность в работе системы установки и переустановки программ выполняются только на виртуальных машинах.
- Возможность дистанционного восстановления работоспособности серверов. Достаточно иметь удаленный доступ к базовой машине. К счастью, в наше время вариантов такого доступа может быть несколько, а один из весьма надежных — терминальный доступ — возможен средствами Windows.
- Возможность размещения на одной физической машине одновременно работающих серверов под принципиально различными операционными системами — Windows и Linux могут работать на одном компьютере одновременно.
- Возможность совершенно без риска для работы сервера испытывать различные программы, пригодность которых для ваших условий точно не ус-

тановлена. Если в результате опыта выяснилась непригодность программы, то замена файла сервера позволяет полностью уничтожить следы установки программы, сохранив систему в максимально чистом виде.

Достаточно. Надо и вам дать возможность найти свои доводы в пользу виртуального сервера. Если кому-то покажется, что уже все сказано, то это может значить только то, что вы еще не вошли во вкус, еще не опробовали работу с виртуальным сервером в полной мере. Если вы — системный администратор или собираетесь им стать, то сможете найти еще с десяток плюсов у виртуального сервера. В каждой конкретной ситуации эти плюсы могут быть разными, но они есть всегда.

Понимание полезности виртуального сервера есть. Остается понять, как же установить этот сервер? Для этого существуют специальные программы. Среди них наиболее известны программы от Microsoft и VMware.

Что можно установить?

Для кого-то покажется удивительным, но Microsoft предлагает нам виртуальный сервер Microsoft Virtual Server совершенно бесплатно! Требуется только регистрация перед загрузкой файлов. Получить этот сервер можно по адресу

http://www.microsoft.com/windowsserversystem/virtualserver/software/default.mspx.

Предварительно можно почитать описание этого сервера на странице

http://zeus.sai.msu.ru:7000/operating_systems/virtserver/.

Также бесплатно можно скачать и VMware Server, который, аналогично продукту от Microsoft, предназначен для создания виртуального сервера и управления им локально или удаленно через веб-интерфейс.

VMware также предлагает VMware Player, с помощью которого можно "проигрывать" виртуальные машины, созданные с помощью программ различных производителей (VMware GSX Server, VMware ESX Server, Microsoft Virtual PC и образы Symantec LiveState Recovery). То есть, создав виртуальную машину в доступной вам программе, вы можете перенести ее на любой другой компьютер, где установлен VMware Player. Если виртуальная машина была создана не средствами VMware, например, MS Virtual PC, то плеер автоматически импортирует файлы, преобразуя в свой формат. Подобно Adobe Acrobat Reader, который предназначен для чтения популярных PDF-файлов, VMware Player может "читать" созданные кем-либо виртуальные машины. Вы можете сами создавать виртуальные системы с помощью VMware Workstation или бесплатных виртуальных серверов от Microsoft или VMware, распространяя

их среди других пользователей ПК. Новому пользователю виртуальной системы даже не придется искать драйвера. После запуска в плеере драйверы устанавливаются автоматически. У автора не возникло проблем при переносе виртуальной машины, созданной на самостоятельно собранном персональном компьютере, на ноутбук HP Compaq.

Познакомиться с другими продуктами VMware можно на странице **http://www.vmware.com**. Фирма предлагает не только программы для создания и запуска виртуальных систем, но и сами системы. После установки VMware Player можно скачать множество примеров виртуальных машин, которые содержат в себе ОС Linux и браузер Firefox. Предназначены эти виртуальные машины для безопасного просмотра интернет-страниц. Все они замкнуты в себе, и никакие вирусы и опасные программы не смогут проникнуть в базовую или другую виртуальную систему. Эти виртуальные машины можно найти на странице **http://linhost.info/vmware/**.

Установка Microsoft Virtual Server 2005 R2

Выбор этого сервера может быть обусловлен относительной простотой его настройки. Опыт других пользователей говорит о том, что на этот сервер можно установить не только Windows XP и серверные версии Windows, но и Linux. Интерфейс сервера не очень удобен для работы в виртуальной системе, хотя и позволяет это делать, но зато системой можно управлять дистанционно через веб-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/evaluation/vsmt.mspx**. Если эта ссылка не работает или файл для скачивания недоступен, воспользуйтесь прямой ссылкой на файл: **http://download.microsoft.com/download/4/1/8/4187dc3b-4c92-41a8-b077-1367b29673b2/ADS_VSMT_1.1.exe**. С помощью VSMT можно преобразовать физические машины в виртуальные, а виртуальные машины VMware — в виртуальные машины, совместимые с Virtual Server. Компания VMware предлагает аналогичный продукт VMware P2V Assistant, который представляет собой интегрируемый программный модуль для BartPE, формирующий новые загрузочные образы виртуальных машин путем создания визуального объекта (ghosting), соответствующего физическому образу, с последующим внедрением драйверов в образ виртуальной машины VMware. Эта утилита намного проще в использовании, чем VSMT, но требует применения сторонней программы — например, Symantec Ghost или Acronis True Image — для создания образа диска. Для загрузки Ultimate-P2V

можно воспользоваться ссылкой **www.rtfm-ed.co.uk/?page_id=174**. Большинство пользователей Windows смогут без значительных проблем установить и освоить эти продукты.

Перед установкой виртуального сервера следует проверить, установлен ли у вас в системе компонент Internet Information Servises Manager из состава Internet Information Servises (IIS) (рис. 5.1). Если компонент не установлен, то установите его. В системе Windows 2003 Server этот компонент находится в составе сервера приложений. На клиентском компьютере, где будет установлен Virtual Machine Remote Control (клиент удаленного контроля), никаких дополнительных компонентов не требуется.

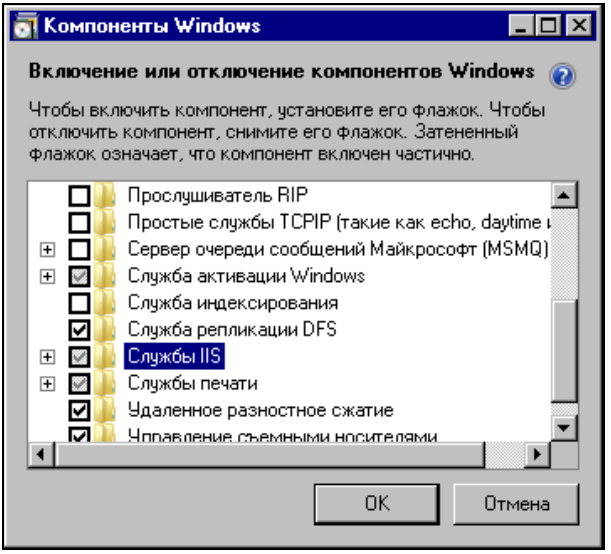


Рис. 5.1. Окно **Компоненты Windows**

Установка сервера не отличается от установки большинства обычных программ под Windows. Достаточно запустить на выполнение скачанный файл Setup.exe, и для первой установки ничего не изменять в параметрах установки по умолчанию. На физическом сервере, где будет установлен виртуальный сервер, следует выполнить полную установку. Дополнительно можно установить компонент Virtual Machine Remote Control (клиент удаленного контроля) на рабочую станцию, сняв отметки с остальных компонентов сервера во время установки.

После установки виртуального сервера в окне браузера откроется страница с информацией о результатах установки (рис. 5.2).

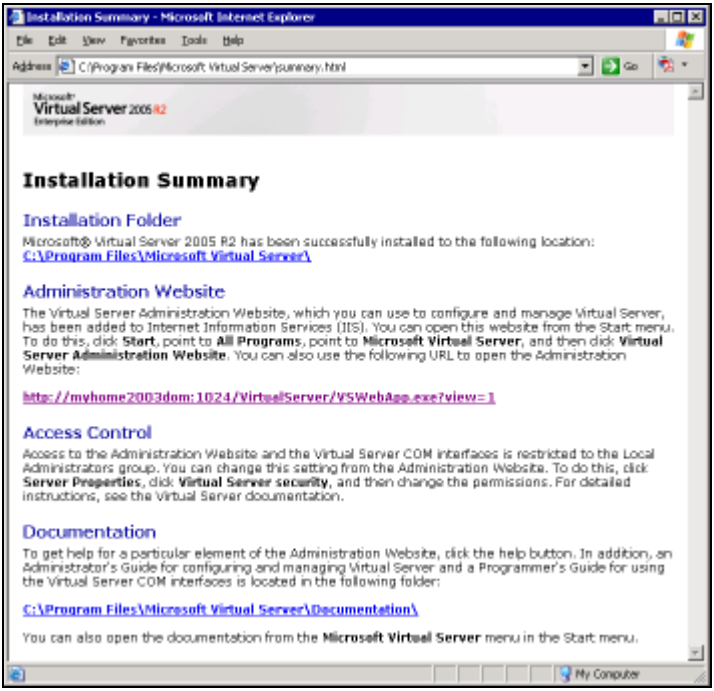


Рис. 5.2. Окно браузера **Installation Summary**

Рис. 5.3. Окно браузера **Create Virtual Machine**

В этом окне указаны пути, куда установлены компоненты программы, а также ссылка на веб-интерфейс администратора. Кликнув по ссылке, вы можете вызвать этот интерфейс. Выбрав в меню страницы пункт **Virtual Machines | Create** (Виртуальные машины | Новая), вы попадете в интерфейс создания новой виртуальной машины (рис. 5.3).

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.

После создания виртуальной машины перейдите в меню **Master Status** (Страница состояния сервера) (рис. 5.4).

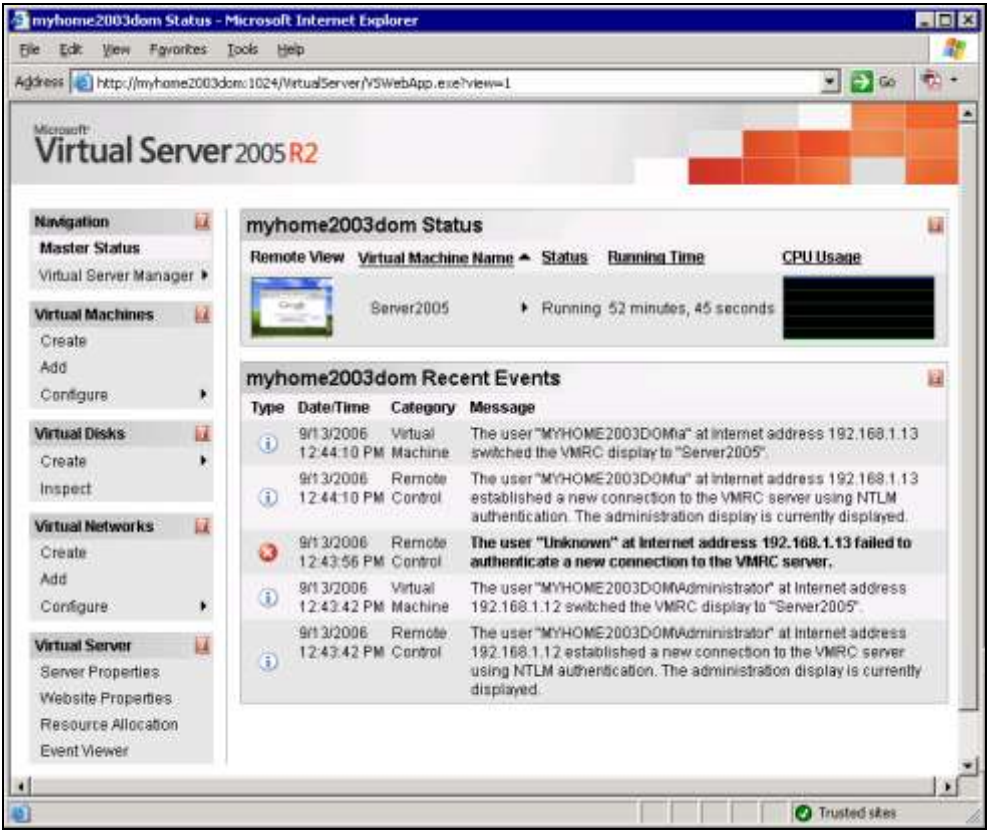


Рис. 5.4. Окно браузера **Virtual Machine Status**

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 кликнуть по маленькому изображению этого окна в интерфейсе Virtual Machine Status. Или через меню **Пуск** запустить Virtual Machine Remote Control (рис. 5.5).

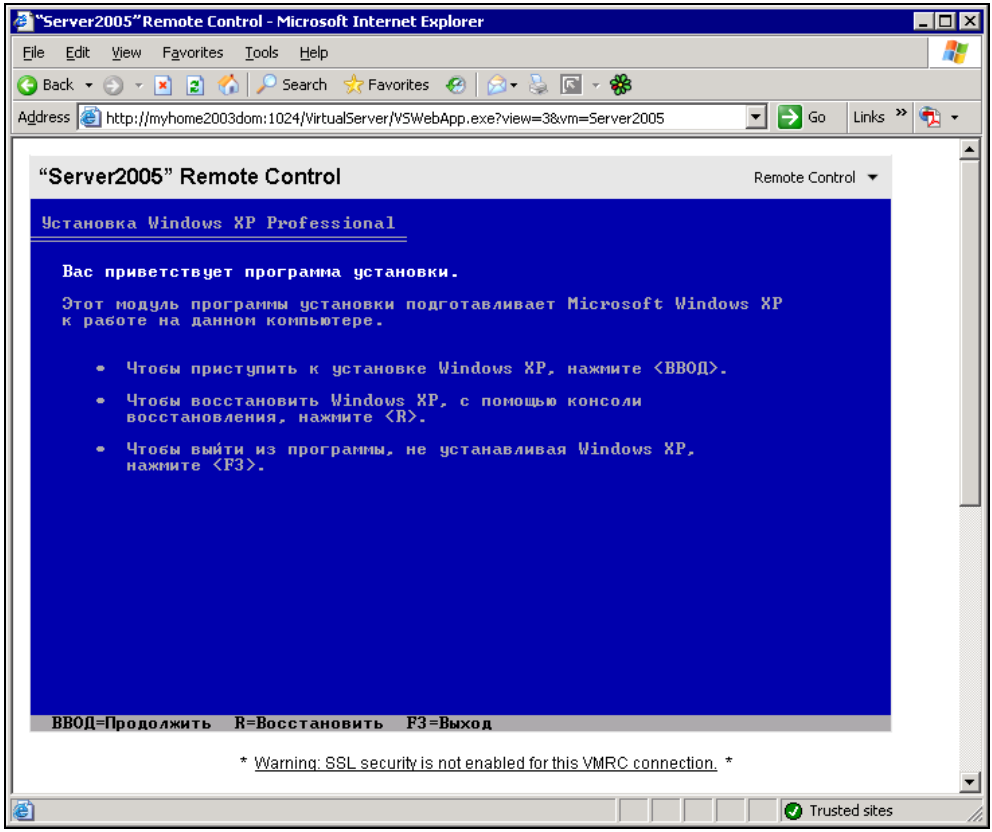


Рис. 5.5. Окно браузера **Virtual Machine Remote Control**. Установка системы

Пользуясь этим окном, вы сможете провести установку системы, а в дальнейшем просто работать в системе, производя необходимые настройки сервера (рис. 5.6).

Рис. 5.6. Окно браузера **Virtual Machine Remote Control.** Система установлена

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

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

Некоторые подробности о виртуальном сервере можно найти на страницах

http://soft.mail.ru/article_page.php?id=91
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. С этой целью можно заранее создать необходимые виртуальные машины, перенести их на физические машины, где они должны работать, а запускать их можно с помощью VMware Player.

Используем VMware Player

Установка этой программы настолько проста, что описывать ее нет смысла. Единственное, на что можно обратить внимание — если у вас уже установлена программа VMware Workstation версии ниже чем 5.0, то программа установки потребует ее удалить. Плеер входит в состав VMware Workstation 5.x, а бесплатные обновления для продуктов VMware возможны только в пределах основного номера версии программы. Но сам плеер бесплатный, а устанавливать его лучше на компьютер, где не установлена VMware Workstation.

После установки плеера и переноса на компьютер, где он установлен, файлов виртуальной машины можно запустить плеер. Программа попросит указать конфигурационный файл виртуальной машины, которую необходимо запустить (рис. 5.7).

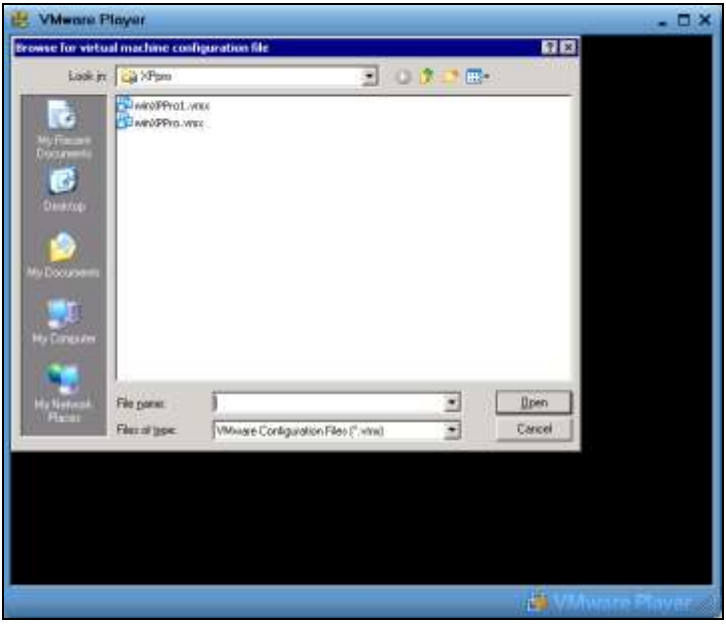


Рис. 5.7. Окно **VMware Player** (поиск файла конфигурации)

Рис. 5.8. Окно **VMware Player** (запуск виртуальной машины)

Если ваша виртуальная машина создана средствами Microsoft, то укажите соответствующий тип файла в поле **Files of type** и выберите необходимый файл. Плеер преобразует виртуальную машину в формат VMware и запустит ее (рис. 5.8).

Управление плеером ограничено возможностью отключения и подключения дисководов, сетевой карты и аудиосистемы. Все свойства виртуального компьютера определяются во время его создания. Тем не менее, вам ничто не мешает устанавливать и переустанавливать операционную систему виртуального компьютера, выполнять в ней любые настройки. Соответственно, установив серверную операционную систему, вы можете настроить полноценный сервер.

Можно установить на один физический компьютер более одного виртуального сервера. Особенно интересен вариант, когда каждый из виртуальных серверов выполняет свою определенную задачу. В этом случае вы можете, совершенно ничем не рискуя, заменить, например, почтовый сервер, оставив без изменения файловый и веб-сервер. Если не понравилась работа нового сервера — просто запустите старый файл сервера!

VMware Server

Этот виртуальный сервер может быть установлен не только на машину с Windows, но и на компьютер с ОС Linux, как и VMware Player.

Загрузить VMware Server и VMware Player в версиях для Linux можно по адресу в Интернете

http://www.vmware.com/download/server/.

Перед загрузкой потребуется регистрация. Только зарегистрировавшись, вы сможете получить серийные номера продуктов в необходимом вам количестве.

В Mandriva Linux установка VMware Player возможна с дистрибутивного диска или из 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 программа устанавливается без проблем, но затем, при попытке запуска установленной программы, система просит выполнить конфигурацию программы для работы с имеющимся ядром. В процессе конфигурации система 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. Рассмотрим решение для Mandriva Linux, для других Linux действуйте по аналогии.

Откройте утилиту установки и удаления программ (рис. 5.9). В левой части окна **Управление программами** в разделе меню **Разработка** откройте пункт **Ядро**. В правой части окна вы увидите установленные в системе пакеты. Необходимо, чтобы в числе установленных был пакет **kernel-desktop-devel-<версия_текущего_ядра_>mdv**. Если он не отмечен в числе установленных, отметьте его и нажмите кнопку **Применить**. Убедитесь также, что установлены пакеты **Libgcc1**, **gcc**, **gcc-cpp**.

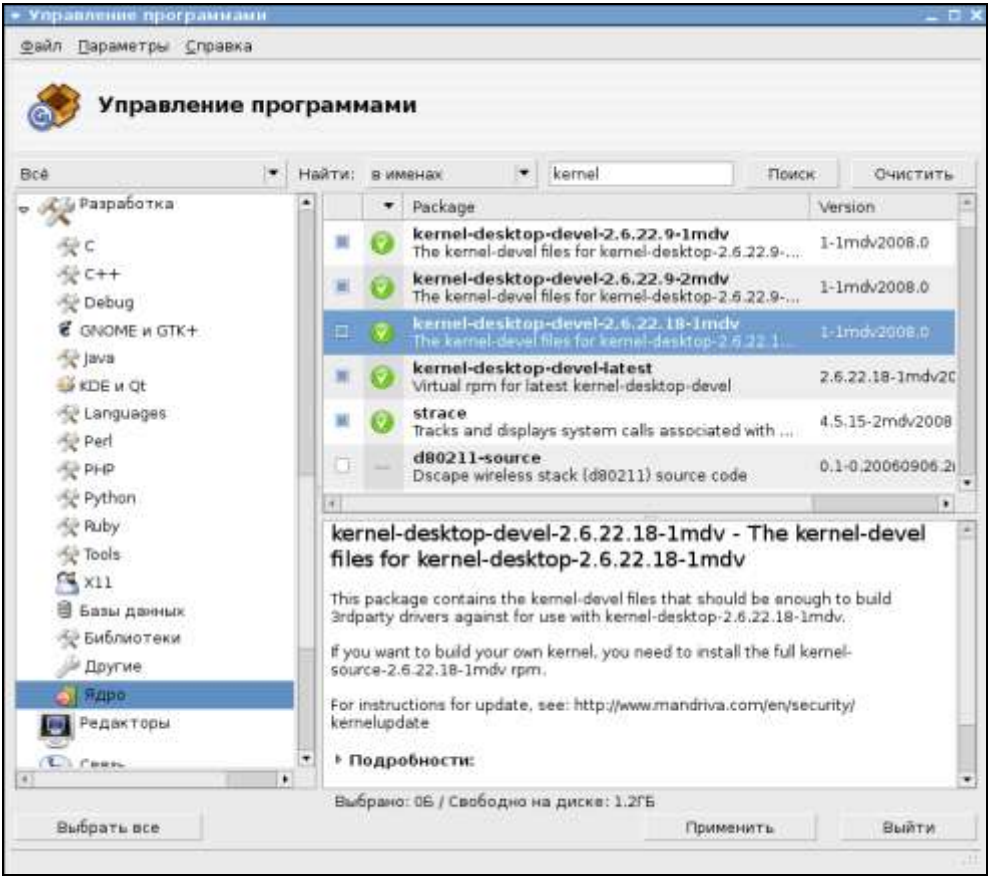


Рис. 5.9. Окно **Управление программами**. Ядро

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

Ниже приведен вывод на экран в окне терминала процесса конфигурации VMware Player.

Процесс конфигурации VMware Player

Прежде всего, получаем права администратора (пользователя root), введя команду `su` и пароль этого пользователя

```
[beard@BeardM ~]$ su
```

```
Пароль:
```

Вводим команду запуска VMware Player

```
[root@BeardM beard]# vmplayer
```

Система сообщает о необходимости конфигурирования программы

```
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.
```

Вводим предложенную системой команду

```
[root@BeardM beard]# vmware-config.pl
Making sure services for VMware Player are stopped.

Stopping VMware services:
   Virtual machine monitor                                    [  OK  ]

Configuring fallback GTK+ 2.4 libraries.

In which directory do you want to install the theme icons?
[/usr/share/icons]
```

Нажимаем <Enter>

```
What directory contains your desktop menu entry files? These files have a
.desktop file extension. [/usr/share/applications]
```

Нажимаем <Enter>

```
In which directory do you want to install the application's icon?
[/usr/share/pixmaps]
```

Нажимаем <Enter>

```
/usr/share/applications/vmware-player.desktop: error: value "vmware-
player.png" for key "Icon" in group "Desktop Entry" is an icon name with
an extension, but there should be no extension as described in the Icon
Theme Specification if the value is not an absolute path
Error on file "/root/tmp/vmware-config0/vmware-player.desktop": Failed to
validate the created desktop file
Unable to install the .desktop menu entry file. You must add it to your
menus
by hand.
```

Не обращаем внимания на описание ошибки, позднее сделаем значок запуска программы самостоятельно

```
Trying to find a suitable vmmon module for your running kernel.

None of the pre-built vmmon modules for VMware Player is suitable for
your
running kernel.  Do you want this program to try to build the vmmon mod-
ule for
your system (you need to have a C compiler installed on your system)?
[yes] y
```

Вводим "YES" или "Y" и нажимаем <Enter>

```
Using compiler "/usr/bin/gcc". Use environment variable CC to override.

What is the location of the directory of C header files that match your
running kernel?
[/lib/modules/2.6.22.18-desktop-1mdv/build/include]
```

Нажимаем <Enter>

```
Extracting the sources of the vmmon module.

Building the vmmon module.

Using 2.6.x kernel build system.
make: Entering directory `/root/tmp/vmware-config0/vmmon-only'
make -C /lib/modules/2.6.22.18-desktop-1mdv/build/include/.. SUBDIRS=$PWD
SRCROOT=$PWD/. modules
make[1]: Entering directory `/usr/src/linux-2.6.22.18-desktop-1mdv'
  CC [M]  /root/tmp/vmware-config0/vmmon-only/linux/driver.o
  CC [M]  /root/tmp/vmware-config0/vmmon-only/linux/hostif.o
  CC [M]  /root/tmp/vmware-config0/vmmon-only/common/comport.o
  CC [M]  /root/tmp/vmware-config0/vmmon-only/common/cpuid.o
  CC [M]  /root/tmp/vmware-config0/vmmon-only/common/hash.o
  CC [M]  /root/tmp/vmware-config0/vmmon-only/common/memtrack.o
  CC [M]  /root/tmp/vmware-config0/vmmon-only/common/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 <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 на рабочем столе, выбираем **Создать кнопку запуска**. В открывшемся окне вводим необходимые параметры, среди которых самый важный это **Команда**. Вписываем vmplayer. Теперь можно указать значок кнопки запуска, выбрав vmware-player.png в папке, которая была указана при конфигурации — /usr/share/pixmaps/.

Щелкнув по созданному значку, открываем окно **VMware Player** (рис. 5.10).

Кнопка **Download a Virtual Appliance** приведет нас на сайт, откуда можно загрузить уже готовые виртуальные компьютеры, а кнопкой **Open an existing Virtual Machine** можно открыть существующую виртуальную машину,

полученную из Интернета или созданную самостоятельно. VMware Server под Linux устанавливается аналогично.

Рис. 5.10. Окно **VMware Player**

Соблюдаем лицензии

Может возникнуть вопрос — не потребуется ли для виртуальных машин покупать отдельные лицензии на операционные системы? Ведь в правилах лицензирования ОС сказано: "Персональные операционные системы лицензируются по следующему принципу — одна лицензия на один компьютер. Не имеет значения, сколько физических лиц использует компьютер". Но в правилах лицензирования допускается использовать Windows XP Professional на одной физической и на одной виртуальной машине. Подробно с правилами лицензирования виртуальных машин можно ознакомиться по адресу **http://www.mslicense.ru/articles.php**.

Лицензия на Windows Server 2003 R2 Enterprise допускает одновременное использование системы не более чем на одном физическом сервере и не более чем на четырех виртуальных серверах. Это значит, что на одном физиче-

ском сервере с Windows Server 2003 R2 можно установить еще четыре виртуальных сервера с той же ОС. При этом незапущенные копии системы могут храниться в любом количестве. Ограничения есть только на одновременно работающие копии системы.

По адресу **http://download.microsoft.com/download/4/7/4/47415510-647d-4847-a554-b5bb33bd44af/Licensing_with_Microsoft_Virtual_Server_R2.doc** можно получить документ, подтверждающий ваши права на использование операционной системы на виртуальной машине.

Но в отдельных случаях вам может не хватить разрешенного числа работающих копий. В этом случае вы можете использовать другие операционные системы на виртуальных машинах. Обычно это операционные системы семейства Linux. Но как установить и настроить систему, если у вас нет опыта работы в этих системах?

И здесь есть выход. VMware предлагает на своем сайте несколько десятков готовых виртуальных машин различного назначения!

Virtual Appliances

Загляните на страницу **http://www.vmware.com/vmtn/appliances/**. На ней можно найти ссылки на готовые виртуальные машины. Virtual Appliances (Виртуальные приборы) — это уже установленные и сконфигурированные под определенные задачи системы.

Browser Appliance (Виртуальный браузер) — это виртуальная операционная система, в которой при запуске по умолчанию открывается окно браузера. Автор скачал и запустил один из таких инструментов с помощью VMware Player. Результаты просто ошеломляющие (рис. 5.11)! Без особого труда удалось подстроить систему под часовой пояс и использование русской раскладки клавиатуры. Были установлены дополнительные программы: текстовый редактор и Macromedia Flash Player. Теперь, запуская эту виртуальную машину, можно совершенно безопасно посещать самые рискованные участки всемирной паутины, при этом не опасаясь проблем на базовой машине. Подключенная флешка опозналась моментально. Любые недостающие компоненты при настройке сети или установке программ моментально скачиваются из Интернета и устанавливаются.

Есть Virtual Appliances с почтовым сервером и фильтрами спама, MySQL-сервер, Apache-сервер, маршрутизаторы, специальный Appliance для обеспечения общего подключения к Интернету, прокси-серверы, просто установленные Linux различных версий… всего не перечислишь. Это надо видеть!

Рис. 5.11. Окно **VMware Player** с запущенным Browser Appliance и открытым системным меню

К сожалению, многие инструменты имеют довольно большой объем, но современный Интернет позволяет скачивать такие объемы.

Теперь, имея достаточно мощный компьютер, вы можете установить на него несколько серверов или вспомогательных систем. Можно просто своими руками "потрогать" уже настроенные системы. И все это без нарушения лицензий, если вы имеете одну официально приобретенную ОС Windows.

Виртуальные технологии в нашей сети

Необходимые программы определили, с установкой разобрались. 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 предпола-

гается 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 несколько виртуальных.

Виртуальные компьютеры, как и обычные, могут быть включены в вашу сеть. Независимо от того, включена консоль управления сервером или нет, в сетевом окружении компьютеры могут быть обнаружены, если их операционные системы загружены.

Гостевые операционные системы на виртуальных компьютерах могут быть любыми. Правда, Windows Vista может работать в VMware Player и VMware Server версий 2 и выше. Текущая стабильная версия VMware Server 1.04 позволяет создать виртуальную машину, на которую можно установить Windows Vista, запустив эту машину в VMware Player.

Два компьютера в одном

Какую же пользу можно извлечь из виртуальных технологий в домашней сети? Начнем с самого простого. Мы уже говорили о возможности обезопасить себя от атак и вирусов из Интернета путем применения компьютера под Linux для путешествий по глобальной сети. Если у вас нет второго компьютера, вы можете создать виртуальную машину в уже существующем. При этом не придется самостоятельно устанавливать операционную систему. Имея установленный VMware Player или VMware Server, вы можете скачать уже готовый виртуальный компьютер.

Безопасный браузер

Browser Appliance — так называется виртуальный компьютер, предназначенный для посещения Интернета. Его операционная система — Ubuntu Linux — вирусным заражениям практически не 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 Browser Appliance — **http://www.vmware.com/appliances/directory/cat/0?k=Browser+Appliance**.

Перед началом скачивания архива вам будет предложено зарегистрироваться, но это не обязательно. От регистрации можно отказаться.

Скачав архив, распакуйте его в любую заранее подготовленную папку.

Теперь запустите VMware Player или VMware Server. Откройте сохраненную виртуальную машину. Система Browser Appliance настроена таким образом, что после загрузки сразу откроется окно интернет-браузера Firefox. Сеть уже настроена. Доступ в Интернет Browser Appliance получит через базовую машину с применением преобразования адресов (NAT). Никаких маршрутизаторов вам не потребуется. Все необходимые устройства созданы в виртуальной машине. Виртуальный компьютер включен в собственную подсеть, которая не имеет прямого выхода в вашу сеть. На рис. 5.12 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.

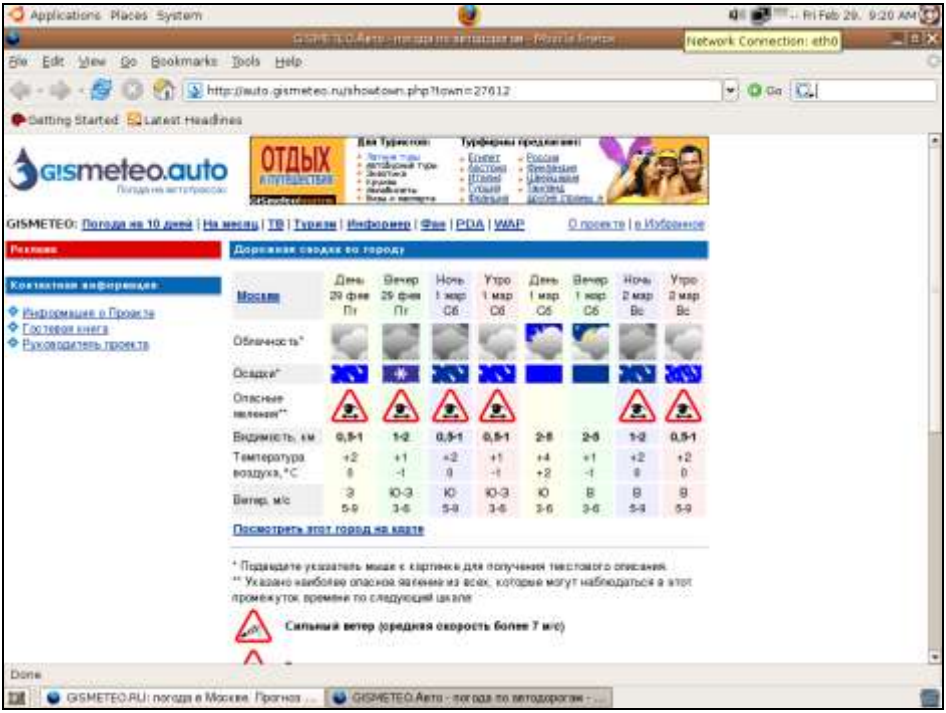


Рис. 5.12. Окно виртуальной машины Ubuntu Linux, запущенной в VMware Server, установленной на базовом компьютере Windows Vista Home Premium

Виртуальная сеть

Попробуем настроить виртуальную машину с Ubuntu Linux для работы в сети с другими нашими компьютерами. Даже если на данный момент у нас есть только один компьютер, мы можем создать маленькую сеть. Собственно, после установки VMware Server и Browser Appliance у нас уже настроено две сети… Но нас интересует собственная сеть, настройки которой мы выполним самостоятельно.

После установки VMware Server на вашей машине созданы дополнительные сетевые адаптеры. В окне **Сетевые подключения** (рис. 5.13), которое, как вы помните, может быть открыто из Центра управления сетями и общим доступом, вы можете увидеть все сетевые подключения вашего компьютера, включая и вновь созданные. В данном случае вновь созданные подключения VMware Network Adapter VMnet1 и VMware Network Adapter VMnet8. Эти адаптеры физически не существуют в вашем компьютере, а созданы программно. Программно в VMware Server созданы DHCP- и DNS-серверы. На адаптерах VMware созданы сразу две сети, а сами адаптеры принадлежат виртуальным устройствам.

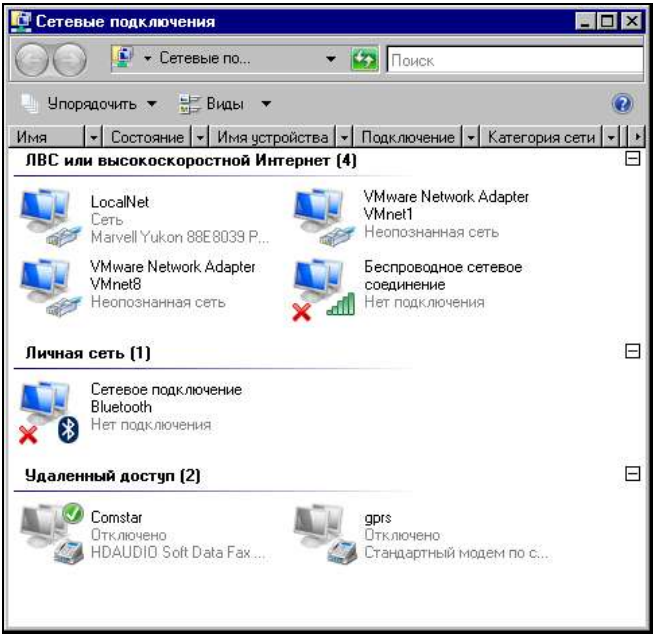


Рис. 5.13. Окно **Сетевые подключения**

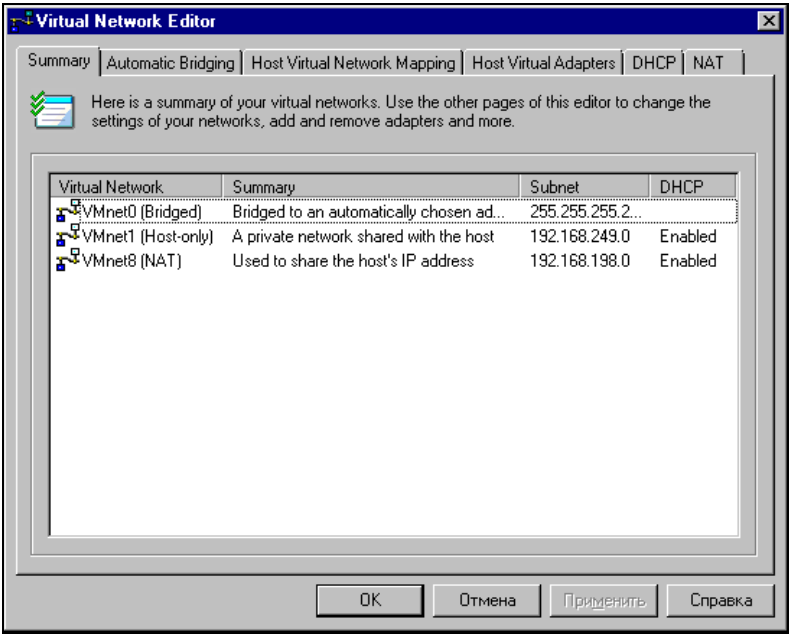


Рис. 5.14. Окно **Virtual Network Editor**, вкладка **Summary**

Откройте **Virtual Network Editor** (Менеджер виртуальных сетей): **Пуск** | **Программы** | **VMware** | **VMware Server** | **Manager Virtual Networks**. В окне **Virtual Network Editor** на вкладке **Summary** (рис. 5.14) показаны адаптеры и сервисы, которые на них работают.

VMnet0 (Bridged) — 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 внешнюю сеть, и на нем включен сервер DHCP. Сеть, связанная с этим адаптером, существует только внутри базового компьютера.

VMnet8 (NAT) — виртуальный адаптер виртуального маршрутизатора, в котором настроено преобразование сетевых адресов. Это позволяет виртуальному компьютеру получать доступ в Интернет через базовый компьютер, используя его IP-адрес вместо своего.

Наша задача — выполнить такие настройки виртуальной сети, чтобы виртуальный компьютер стал частью нашей домашней сети. IP-адреса нашим компьютерам присваивает DHCP-сервер модема-маршрутизатора, или мы их назначаем сами. Значит, дополнительные адаптеры **VMnet1** и **VMnet8** нам не нужны. Кроме того, сетевой адаптер физического компьютера должен быть мостом для виртуального адаптера виртуального компьютера. На всякий случай пролистайте вкладки окна **Virtual Network Editor** и запомните или запишите увиденные настройки. Хотя вернуть настройки по умолчанию можно, переустановив VMware Server.

Для включения виртуального компьютера в реальную сеть проделайте следующее:

1. Перейдите на вкладку **NAT**.

   Нажмите кнопки **Stop** и **Применить**. В результате вид окна должен получиться, как на рис. 5.15.

2. Перейдите на вкладку **DHCP** (рис. 5.16).

   Нажмите последовательно кнопки **Stop** и **Применить**, затем, выделяя каждую строку, нажимайте кнопку **Remove** и **Применить**. На вкладке не должно остаться ни одной строки.

3. Теперь перейдите на вкладку **Host Virtual Adapters** (рис. 5.17).

   Выделяя каждую из имеющихся в окне строк, нажимайте кнопки **Disable**, а затем **Применить**. Этим действием мы отключим не требующиеся в нашем случае адаптеры. При желании их можно удалить совсем, если вы не планируете их использование в дальнейшем. Для этого следует нажимать кнопку **Remove** вместо **Disable**.

4. На вкладке **Host Virtual Network Mapping** в выпадающем списке поля **VMnet0** (рис. 5.18) следует выбрать сетевой адаптер, через который базовый компьютер подключен к вашей сети.

5. И, наконец, на вкладке **Automatic Bridging** (рис. 5.19) ничего менять не надо. Опция **Automatically choose an available physical network adapter to bridge to VMnet0** (Автоматический выбор доступного физического сетевого адаптера для моста на VMnet0) уже снята автоматически после выбора конкретного адаптера на предыдущей вкладке.

Сеть настроена. Остается запустить VMware Server Console (рис. 5.20), подключив ее к локальному серверу VMware Server (Local host), и поправить конфигурацию виртуальной машины. Откройте окно **Virtual Machine Setting**, выбрав в левой части окна команду **Edit virtual machine setting** (Редактировать установки виртуальной машины).

В открывшемся окне (рис. 5.21) установите переключатель **Bridged: Connected directly to the physical network** (Мост: подключен к физическому сетевому адаптеру).

Все. Настроена и сеть и виртуальная машина. Теперь включите виртуальный компьютер командой **Start this virtual machine** (рис. 5.20) и настройте сетевое подключение на получение сетевых параметров через DHCP или установите эти параметры вручную, имея в виду, что присвоенный вручную IP-адрес не должен попадать в диапазон адресов, выдаваемых DHCP-сервером.

Убедиться, что виртуальный компьютер подключен к сети, можно, выполнив команду `ping <адрес_виртуального_компьютера>` с базовой машины (рис. 5.22). Если ответов на `ping` нет, то проверьте все настройки, описанные выше.

Если на виртуальном компьютере установлены все необходимые для работы в сети пакеты, через обозреватель сети можно будет увидеть доступные ресурсы (рис. 5.23). Правда, в данном конкретном случае, если у вас нет дистрибутива Ubuntu 5, вы не установите эти пакеты через Интернет, поскольку поддержка этой системы прекращена. Вы можете переустановить систему на виртуальном компьютере, воспользовавшись более свежим дистрибутивом любой версии Linux.

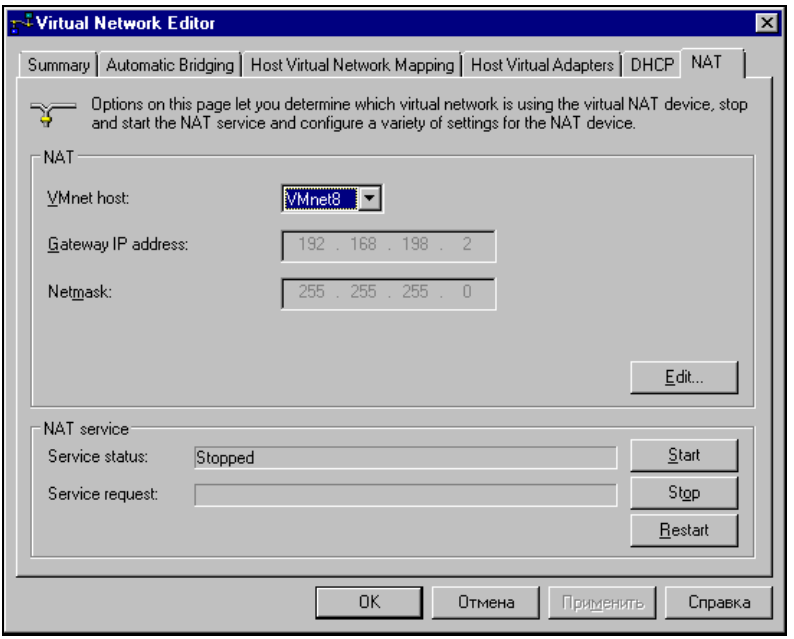


Рис. 5.15. Окно **Virtual Network Editor**, вкладка **NAT**

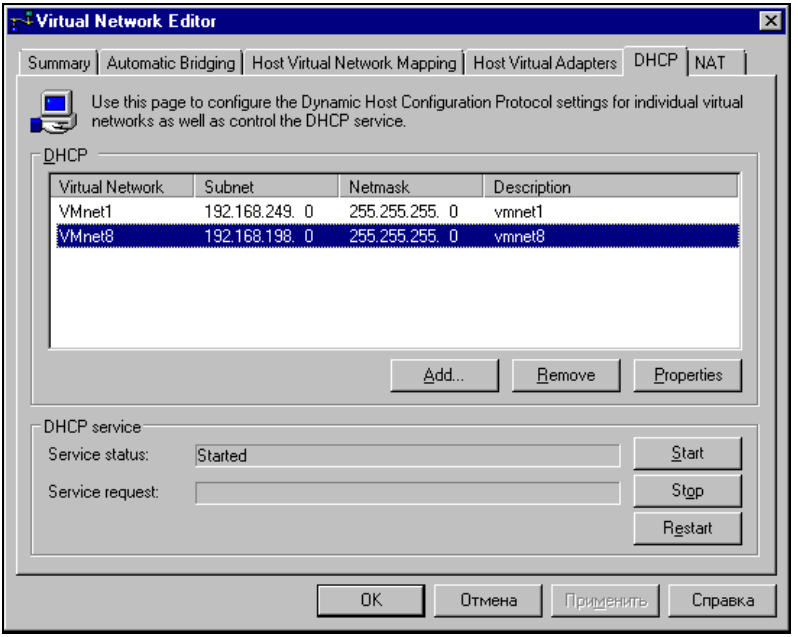


Рис. 5.16. Окно **Virtual Network Editor**, вкладка **DHCP**

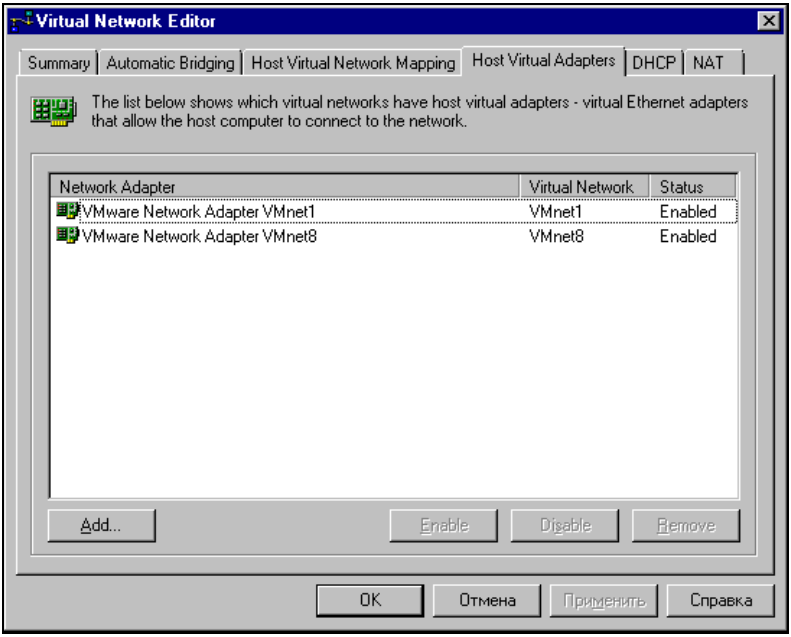


Рис. 5.17. Окно **Virtual Network Editor**, вкладка **Host Virtual Adapters**

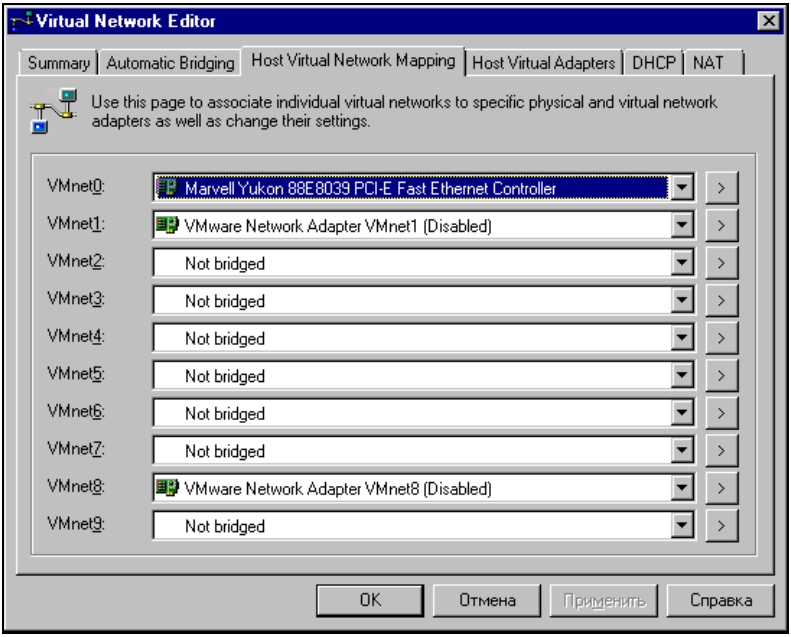


Рис. 5.18. Окно **Virtual Network Editor**, вкладка **Host Virtual Network Mapping**

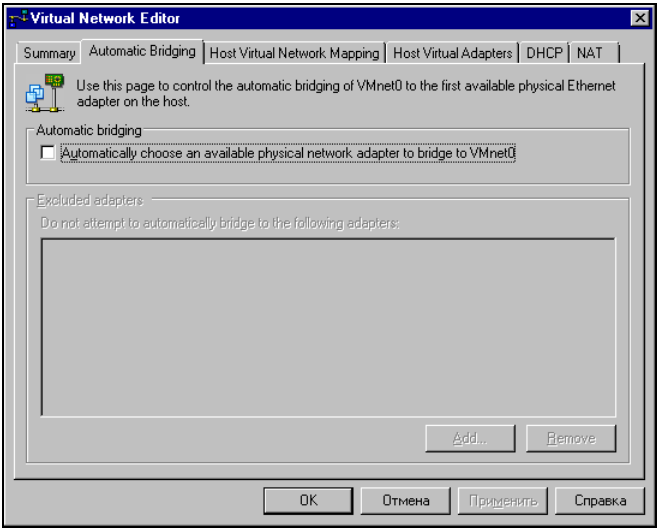


Рис. 5.19. Окно **Virtual Network Editor**, вкладка **Automatic Bridging**

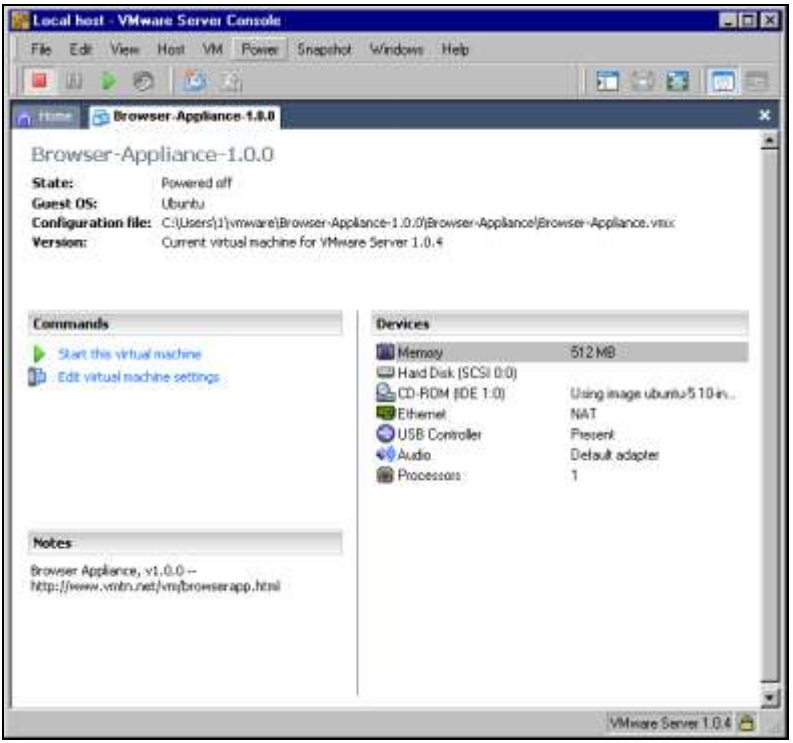


Рис. 5.20. Окно **VMware Server Console**

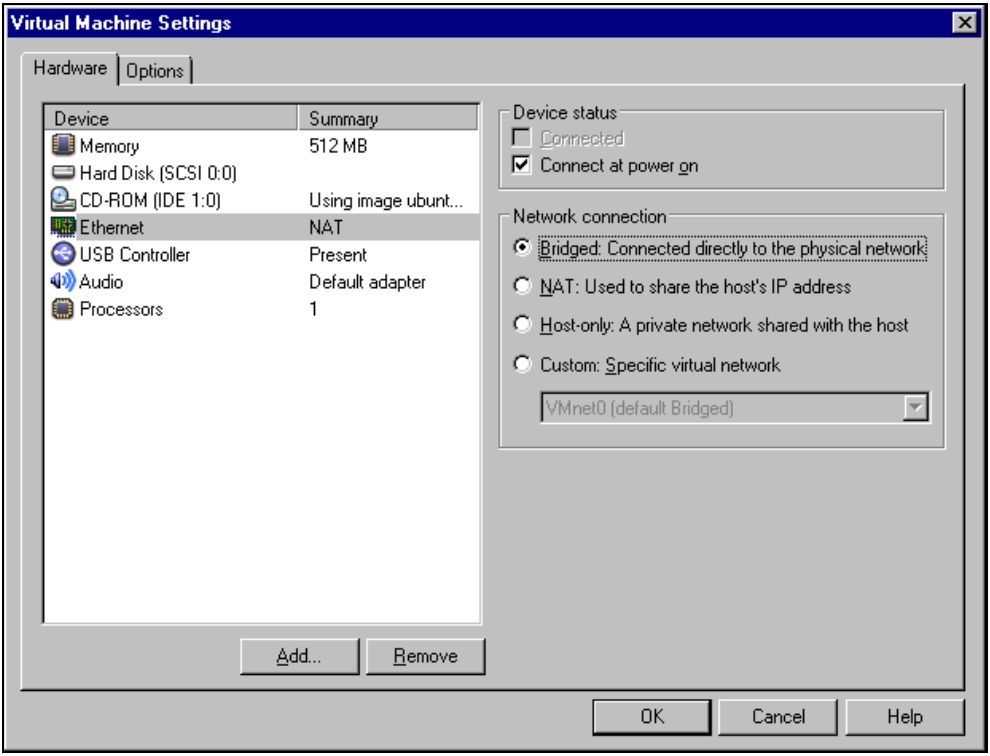


Рис. 5.21. Окно **Virtual Machine Settings**

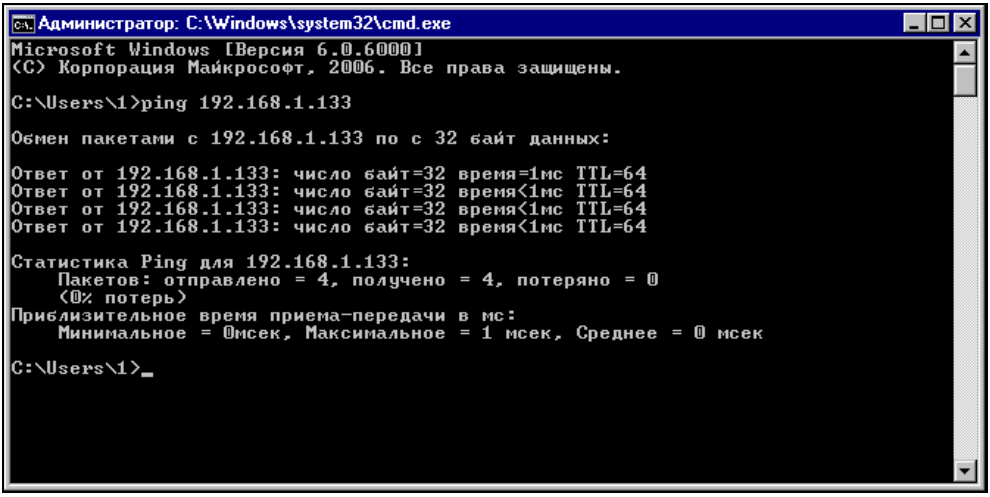


Рис. 5.22. Окно **cmd.exe**, выполнение команды `ping`

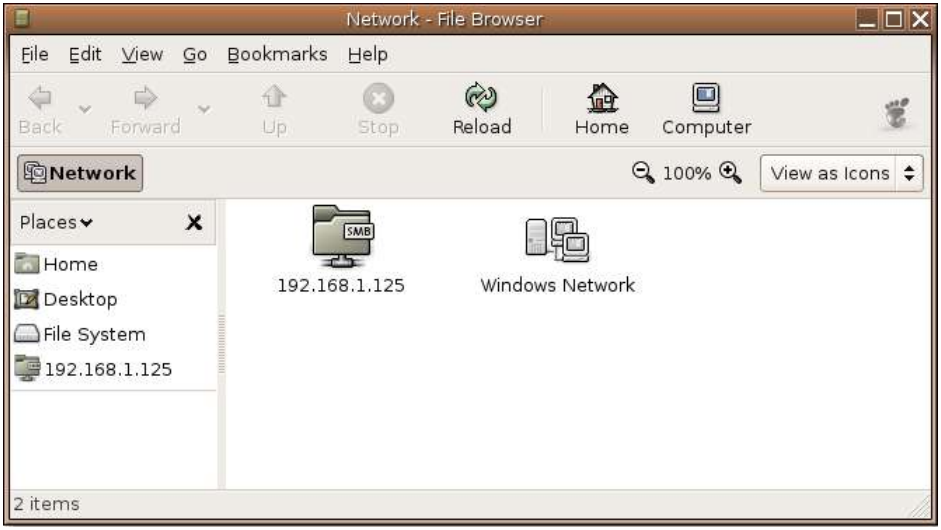


Рис. 5.23. Окно **Network – File Browser**

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. В сети автора виртуальный сервер установлен как на компьютере под управлением Windows Vista, так и на машине с ASPLinux, где в качестве виртуальной системы работает Windows XP. Виртуальный сервер, установленный на любом компьютере, работает всегда. Виртуальные компьютеры, установленные на нем, могут работать, но без запуска консоли управления виртуальным сервером их работа может быть не видна локальному пользователю. В то же время, получая доступ к виртуальному серверу по сети, вы можете управлять виртуальными компьютерами и работать на них.

Посмотрим пример такой работы в сети автора.

В данном случае консоль управления виртуальным сервером запускается на машине под Windows Vista, а виртуальная машина установлена на компьютере под ASPLinux.

При попытке подключения к удаленному компьютеру (Remote host), необходимо ввести его имя или IP-адрес, имя и пароль пользователя удаленного компьютера (рис. 5.24).

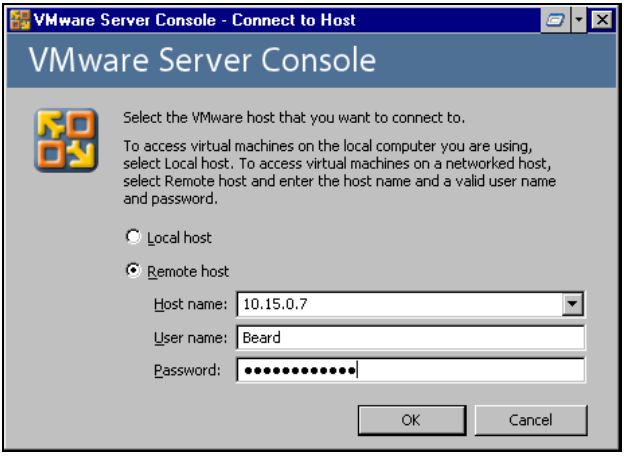


Рис. 5.24. Окно **VMware Server Console – Connect to Host**

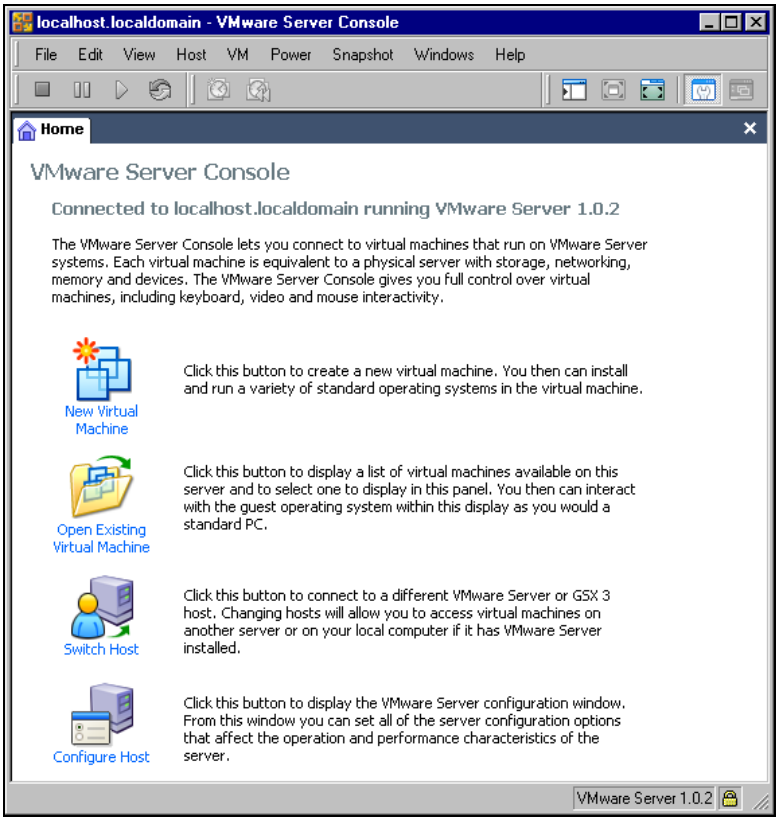


Рис. 5.25. Окно **VMware Server Console**

После ввода регистрационных данных откроется консоль управления виртуальным сервером на удаленном компьютере (рис. 5.25). Как и при работе на локальном компьютере, мы можем выполнять любые задачи по управлению виртуальным сервером, в том числе и открыть существующую виртуальную машину (**Open Existing Virtual Machine**), что нам сейчас и требуется.

В окне **Open Virtual Machine** (рис. 5.26) необходимо выбрать одну из существующих виртуальных машин. Выбираем Windows XP и нажимаем кнопку **OK**.

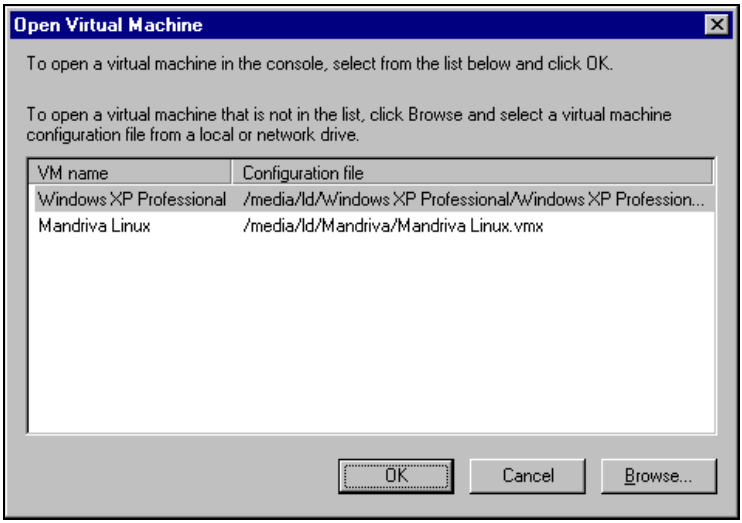


Рис. 5.26. Окно **Open Virtual Machine**

Теперь в окне (рис. 5.27) **VMware Server Console** появилась вкладка **Windows XP Professional**. Выбираем **Start this virtual machine** и через некоторое время видим экран входа в систему Windows XP (рис. 5.28).

Процедура входа в виртуальную систему ничем не отличается от процедуры входа в реальную локальную систему. Более того, на виртуальные системы распространяются все правила лицензирования, как и на реальные. Для использования операционной системы на виртуальной машине необходимо иметь обычную лицензию.

Рабочий стол виртуального компьютера может не помещаться в окне консоли управления на экране локального компьютера (рис. 5.29). С помощью полос прокрутки можно перемещать виртуальный рабочий стол в окне.

Как и любой реальный компьютер, виртуальная машина работает в сети (рис. 5.30). Для всех компьютеров сети виртуальный компьютер — просто один из узлов сети.

Рис. 5.27. Окно **VMware Server Console**, вкладка **Windows XP Professional**

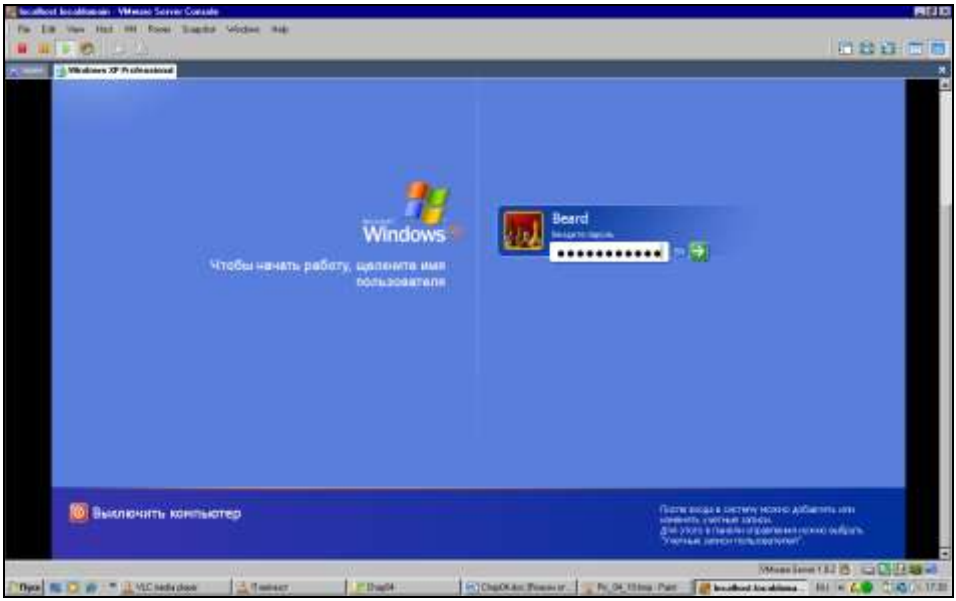


Рис. 5.28. Окно **VMware Server Console**, вкладка **Windows XP Professional**, экран входа в систему

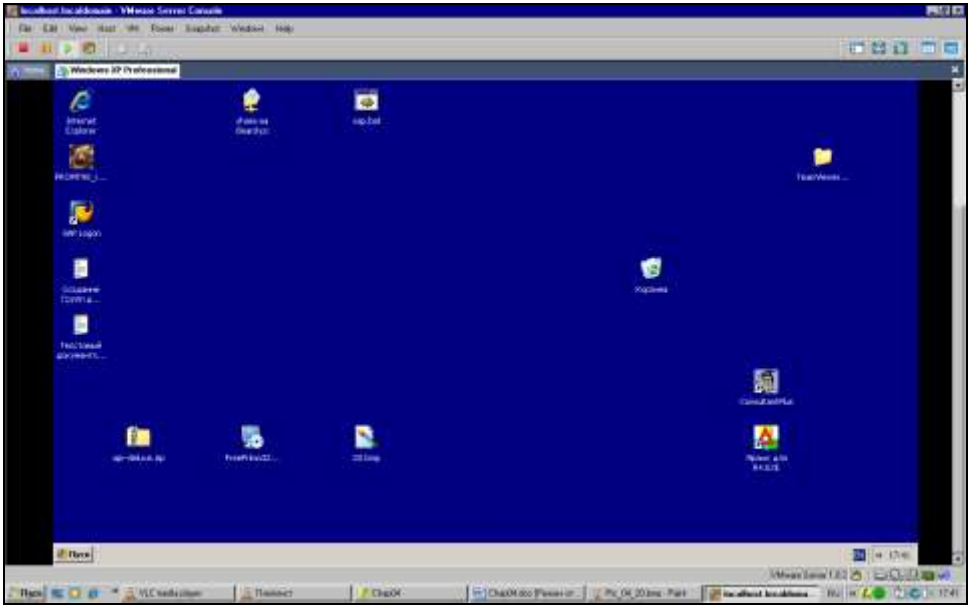


Рис. 5.29. Окно **VMware Server Console**, вкладка **Windows XP Professional**, экран загруженной системы

Рис. 5.30. Окно **VMware Server Console**, вкладка **Windows XP Professional**, экран загруженной системы. Сетевое окружение

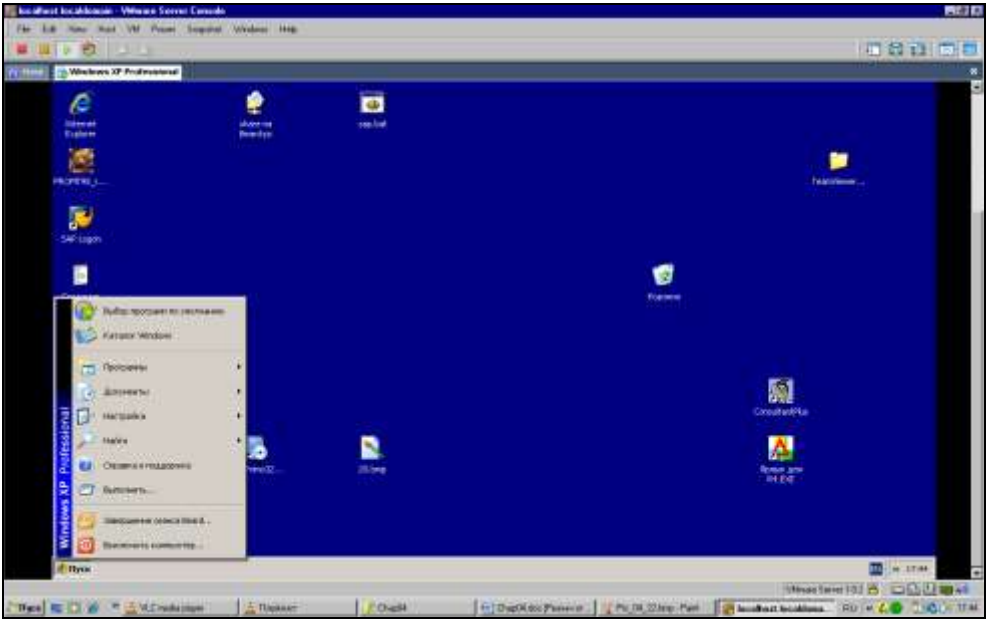


Рис. 5.31. Окно **VMware Server Console**, вкладка **Windows XP Professional**, экран загруженной системы. Выключение

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. 5.31). Если вместо выключения закрыть окно консоли управления, то виртуальный компьютер будет продолжать работать в скрытом виде. Вы сможете к нему подключиться снова как в удаленном, так и в локальном режиме.

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, например. 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 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 выше 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.

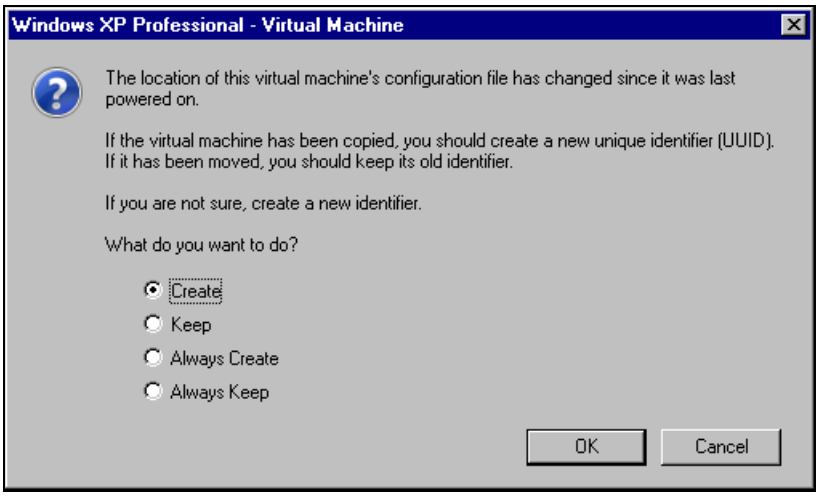


Рис. 5.32. Окно **Windows XP Professional – Virtual Machine**. Создание нового уникального идентификатора

Во время запуска ранее созданной виртуальной машины на новом месте система спросит вас о необходимости создания нового уникального идентификатора виртуального компьютера (рис. 5.32). Если это перемещенная копия системы, то можно оставить идентификатор старый (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.

Есть, конечно, определенные неудобства при работе с удаленной виртуальной машиной. Нет возможности напрямую использовать CD-привод или флеш-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. Что ж, пожалуй, теперь вы имеете достаточно информации о виртуальных машинах и виртуальных серверах. Нет необходимости приобретать еще один компьютер, когда требуется установить дополнительный сервер, выполняющий какую-либо специальную задачу. А опробовать идею, изучить настройки системы можно на виртуальной машине, предварительно сохранив ее копию.

VMware Server 2

Эта версия виртуального сервера VMware, о которой мы упомянули в начале главы, отличается ориентированностью на веб-управление. Как локально, так и удаленно подключиться к VMware Server 2 можно через браузер Internet Explorer или Firefox. Запуск виртуальных компьютеров осуществляется всегда в новом окне, а для обеспечения возможности запуска при первом подключении необходимо согласиться с установкой дополнения к браузеру. Если приходится часто обращаться к какому-либо виртуальному компьютеру, есть возможность создания ярлыка на рабочем столе Windows или значка запуска на рабочем столе Linux. Сервер может быть установлен как под Windows, так и под Linux, и гостевыми системами (виртуальными компьютерами) могут быть практически любые операционные системы.

Применение этого сервера в локальной сети может быть оправдано, когда необходимо нескольким пользователям обеспечить доступ к виртуальным компьютерам. Это может быть полезно, когда рабочее место пользователя должно быть настроено особым образом, требующим много времени у администратора. В этом случае на VMware Server 2 путем клонирования можно быстро создать несколько виртуальных компьютеров с идентичными настройками. Если эти компьютеры должны обращаться к какой-либо базе данных, то и она может быть расположена на том же физическом сервере, где и VMware Server, либо на втором сервере, который находится рядом. Это позволит исключить передачу больших объемов информации по удаленным сегментам локальной сети, чем повысить надежность работы как сети, так и приложений, работающих с базой данных.

В этом примере рассмотрим уже установленный на ОС CentOS 5.1 VMware Server 2. Описание установки для первой версии этого сервера, которое приведено уже в этой главе, вполне подходит и в данном случае. Подключение к серверу в примере выполняется с компьютера с Windows Vista. Для подключения в адресной строке браузера необходимо ввести **https://<IP-адрес_сервера>:8333**.

После процедуры авторизации откроется страница VMware Infrastructure Web Access (рис. 5.33).

С этой страницы можно выполнять все действия по администрированию виртуальных машин и самого сервера. Есть возможность установить права доступа не только к серверу, но и к каждой виртуальной машине. Все учетные записи должны быть предварительно внесены в список учетных записей пользователей базовой машины. Если пользователь, подключаясь к серверу, авторизуется с именем, которому открыт доступ только к одному виртуальному компьютеру, то другие виртуальные компьютеры будут ему недоступны.

Он их просто не увидит. Для своего виртуального компьютера пользователь может создать ярлык. Для этого следует выбрать в разделе **Commands** пункт меню **Create Virtual Machine Shortcut**. Ярлык будет создан на рабочем столе, и при щелчке мышью по нему виртуальный компьютер будет открываться в отдельном окне, а если он был до этого выключен, то включится. Все включенные компьютеры помечены зеленой стрелкой (рис. 5.33).

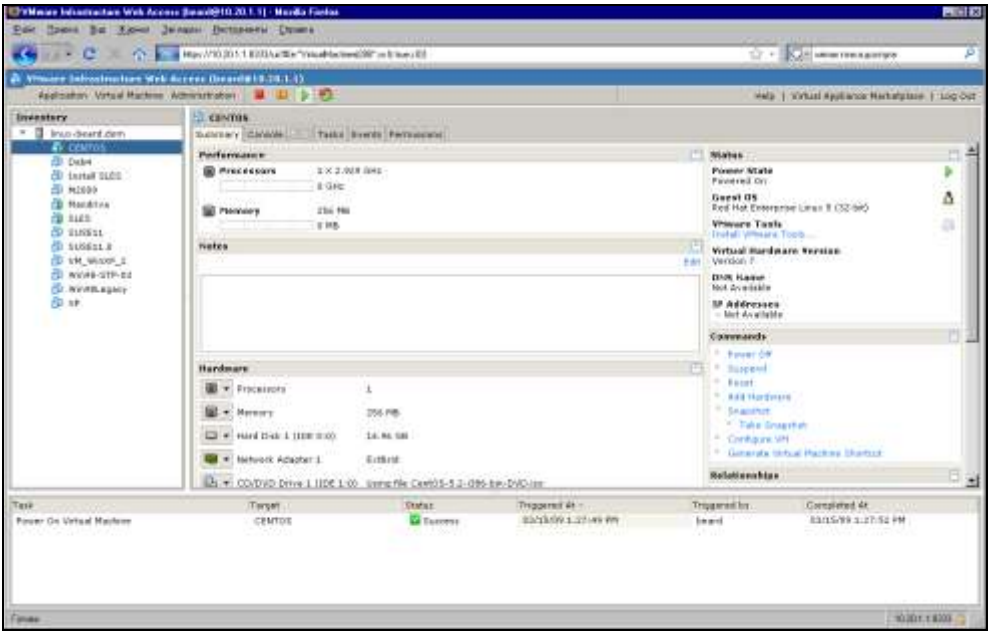


Рис. 5.33. Окно браузера **VMware Infrastructure Web Access**

Создавая виртуальные компьютеры, можно подключать к ним образы CD/DVD-дисков. Если это образы дисков с дистрибутивом, то установку системы можно производить удаленно. Следует только иметь в виду, что для обеспечения нормального быстродействия число одновременно запущенных виртуальных компьютеров не должно превышать число ядер всех процессоров базовой машины, умноженное на четыре.

Рассмотрим пример работы с виртуальной машиной, на которую устанавливается ОС CentOS. Для запуска и открытия виртуального компьютера достаточно, перейдя на вкладку **Console** (рис. 5.34), щелкнуть по надписи **Open the console in new window** (Открыть консоль в новом окне) или по заранее созданному ярлыку.

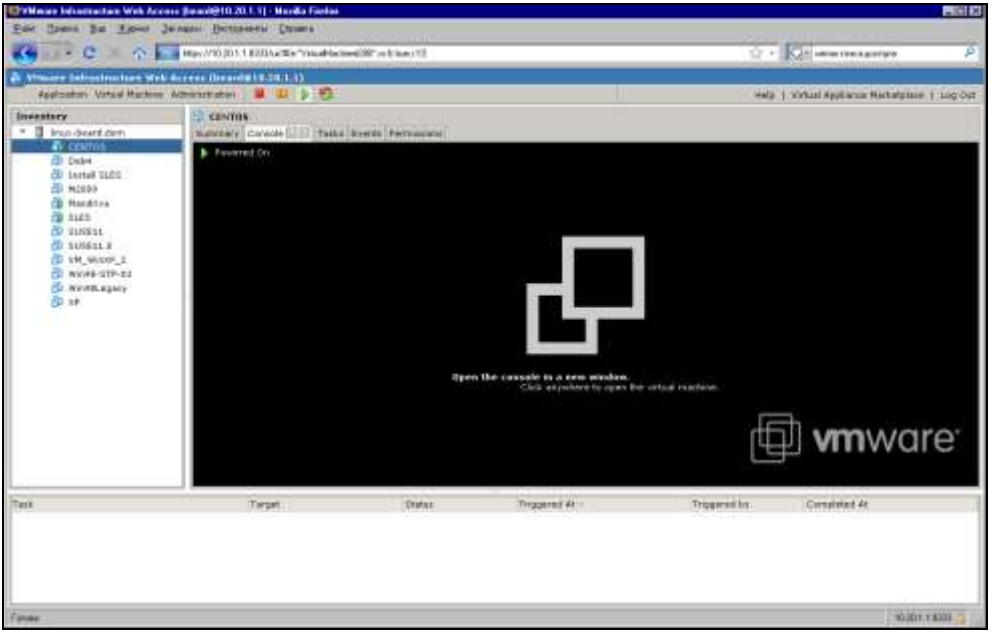


Рис. 5.34. Окно браузера **VMware Infrastructure Web Access Console**

Рис. 5.35. Окно **VMware CentOS Remote Console**

При этом откроется окно (рис. 5.35) с изображением рабочего стола виртуального компьютера или того экрана, который открыт на виртуальном компьютере. Закрытие окна виртуального компьютера не останавливает его работу, поэтому пользователи могут не выключать свои виртуальные машины и подключаться каждый раз, продолжая прерванную работу. В данном случае мы видим экран установки системы.

Вы можете воспользоваться этой виртуальной системой для экспериментов с настройкой сервера. Нет необходимости переустанавливать и перенастраивать базовую машину, если вы еще не уверены в результате. Отработав все настройки на виртуальной машине, вы можете их использовать и на реальной.

OpenVPN

Это одна из часто встречающихся задач при создании соединения между удаленными компьютерами через Интернет. Есть много описаний решения такой задачи, но одно из самых полных и понятных найдено на сайте **http://www.sys-adm.org.ua**. Его автор — Доморадов Алексей из Украины. В данном случае задача решается на базе ОС CentOS 5.2, которую мы можем применить на сервере. Чтобы не изобретать велосипед, приведем это описание с незначительными сокращениями. Описания встречающихся команд можно посмотреть в *приложении*. Внимательно воспроизводя приведенные в статье рекомендации, вам необходимо только заменять фактические имена, адреса, названия страны и города на свои.

Создание туннеля point to point

Передо мной была поставлена задача — обеспечить безопасную работу пользователей, которые работают на удаленном сервере терминалов с помощью стандартного клиента RDP — "Подключение к удаленному рабочему столу". Под безопасностью будем понимать шифрование передаваемых данных между сервером и клиентом. Также неплохо было бы сжимать данные для экономии трафика и разгрузки канала. Для лучшего понимания задачи далее прилагается ее схема (рис. 5.36).

Нам надо обеспечить подключение клиентов из харьковского филиала к серверу терминалов, расположенному в киевском офисе. Сервер терминалов имеет статический адрес 192.168.1.2/24. На системах Linux, пожалуй, самым распространенным ПО для реализации таких задач является OpenVPN. Это полноценный SSL VPN, который реализует сетевые расширения безопасности OSI уровня 2 и 3, используя индустриальный стандарт — протокол SSL/TLS. Поддерживает множество методов аутентификации клиентов, основанных на сертификатах, смарт-картах, логине/пароле.

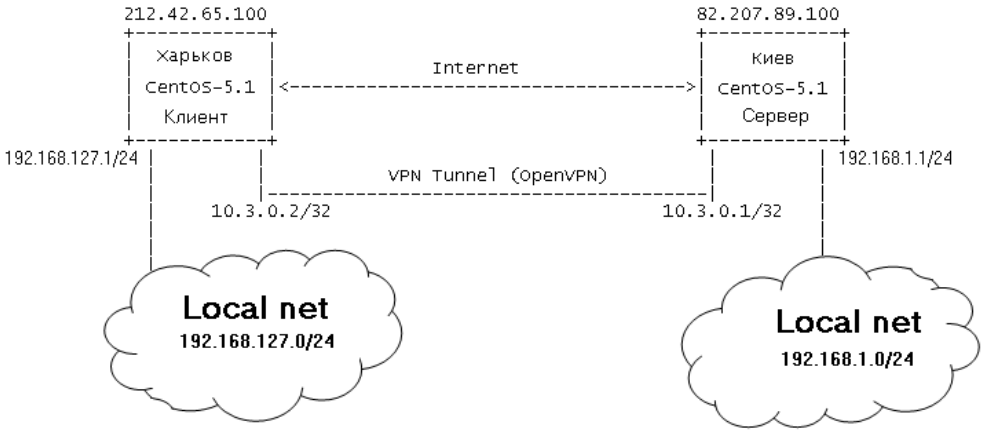


Рис. 5.36. Схема задачи

OpenVPN — мощный и очень гибкий VPN-демон. Он поддерживает безопасность SSL/TLS, Ethernet bridging, туннельный транспорт TCP или UDP через прокси или NAT, поддерживает динамические IP-адреса и DHCP, масштабируемость до сотни или тысяч пользователей, портирован на все основные платформы и ОС. Ниже приведен список поддерживаемых платформ.

- Linux 2.2 и более поздние версии
- Solaris
- OpenBSD 3.0 и более поздние версии
- Mac OS X Darwin
- FreeBSD
- NetBSD
- Windows 2000 и более поздние версии

Итак, у нас имеются следующие системы (команды в окне терминала):

```
# uname -r
2.6.18-53.1.4.el5


# cat /etc/redhat-release
CentOS release 5 (Final)
```

На обоих серверах, как в Киеве, так и в Харькове, установлены одинаковые ОС — CentOS-5.1. В принципе, ОС не имеет особого значения, но крайне желательно, чтобы на концах туннеля использовались одинаковые версии OpenVPN.

Установка OpenVPN

К сожалению, данный пакет отсутствует в официальном репозитории RHEL/CentOS. Так что вам придется либо устанавливать с других репозиториев, либо собрать RPM-пакеты из src.rpm. Если вы хотите использовать сжатие данных, то перед началом сборки OpenVPN надо будет собрать и установить пакет LZO.

```
# rpm -ivh http://www.sys-adm.org.ua/srpms/lzo-2.02-2.src.rpm
# cd /usr/src/redhat/SPECS
# rpmbuild -ba --target=i686 lzo.spec
Building target platforms: i686
Building for target i686
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.9651
+ umask 022
...
...
...
Wrote: /usr/src/redhat/SRPMS/lzo-2.02-2.src.rpm
Wrote: /usr/src/redhat/RPMS/i686/lzo-2.02-2.i686.rpm
Wrote: /usr/src/redhat/RPMS/i686/lzo-devel-2.02-2.i686.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.61481
+ umask 022
+ cd /usr/src/redhat/BUILD
+ cd lzo-2.02
+ rm -rf /var/tmp/lzo-2.02-2-root-root
+ exit 0
```

После успешной сборки устанавливаем пакет

```
# cd /usr/src/redhat/RPMS/i686/
# rpm -ivh lzo-2.02-2.i686.rpm lzo-devel-2.02-2.i686.rpm
Preparing...########################################### [100%]
   1:lzo####################################### [ 50%]
   2:lzo-devel################################# [100%]
```

Теперь у нас все готово и мы можем собирать сам OpenVPN.

```
# rpm -ivh http://www.sys-adm.org.ua/srpms/openvpn-2.0.9-1.src.rpm
# cd /usr/src/redhat/SPECS
# rpmbuild -ba --target=i686 openvpn.spec
Building target platforms: i686
Building for target i686
```

```
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.95164
+ umask 022
...
...
...
Wrote: /usr/src/redhat/SRPMS/openvpn-2.0.9-1.src.rpm
Wrote: /usr/src/redhat/RPMS/i686/openvpn-2.0.9-1.i686.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.2390
+ umask 022
+ cd /usr/src/redhat/BUILD
+ cd openvpn-2.0.9
+ '[' /var/tmp/openvpn-root '!=' / ']'
+ rm -rf /var/tmp/openvpn-root
+ exit 0
```

После успешной сборки устанавливаем пакет

```
# cd /usr/src/redhat/RPMS/i686/
# rpm -ivh openvpn-2.0.9-1.i686.rpm
Preparing...########################################### [100%]
 1:openvpn########################################### [100%]
```

На этом установку необходимого ПО можно считать завершенной, теперь переходим непосредственно к настройке.

Создание и инициализация PKI

Так как для шифрования туннеля мы будем использовать TLS (SSL/TLS плюс сертификаты для аутентификации и обмена ключей) и pre-shared static key, то сначала создадим все необходимые нам ключи и сертификаты. Как это сделать, вы можете прочитать в статье "SSL Howto" (http://sys-**adm.org.ua/security/ssl-howto.php**. Также в составе самого OpenVPN идет набор скриптов существенно облегчающих создание всех необходимых ключей и сертификатов. Вот именно этими скриптами мы и воспользуемся.

Прежде всего, инициализируем PKI (public key infrastructure)

```
# cd /usr/share/doc/openvpn-2.0.9/
# cp -R easy-rsa/ /etc/openvpn/
```

В документации к OpenVPN рекомендуют делать именно полную копию папки easy-rsa в другое место, например /etc/openvpn. И производить все изменения в этой локальной копии, чтобы при обновлении версии OpenVPN ваши изменения не пропали. Перед началом работы определим значение некоторых переменных, облегчающих процесс создания сертификатов.

Для этого правим файл /etc/openvpn/easy-rsa/vars. В нем хранятся значения по умолчанию.

```
# /etc/openvpn/easy-rsa/vars | grep -v ^# | grep -v ^$
export D=`pwd`
export KEY_CONFIG=$D/openssl.cnf
export KEY_DIR=$D/keys
echo NOTE: when you run ./clean-all, I will be doing a rm -rf on $KEY_DIR
export KEY_SIZE=2048
export KEY_COUNTRY=UA
export KEY_PROVINCE=Ukraine
export KEY_CITY=Kharkov
export KEY_ORG="SysAdm"
export KEY_EMAIL="hostmaster@sys-adm.org.ua"
```

После этого инициализируем наши переменные

```
# cd /etc/openvpn/easy-rsa/
# . ./vars
# ./clean-all
```

После того как мы произвели первоначальную подготовку, переходим непосредственно к созданию самих сертификатов. Вначале нам надо создать корневой CA (root CA), с помощью которого мы будем подписывать все наши сертификаты.

```
# ./build-ca
Generating a 2048 bit RSA private key
.........++++++
......++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UA]:
State or Province Name (full name) [Ukraine]:
Locality Name (eg, city) [Kharkov]:
```

```
Organization Name (eg, company) [SysAdm]:
Organizational Unit Name (eg, section) []:SysAdm Security Center
Common Name (eg, your name or your server's hostname) []:Root CA
Email Address [hostmaster@sys-adm.org.ua]:
```

После того как мы создали root CA, теперь генерируем ключ и сертификат для сервера.

```
# ./build-key-server gw1-kv.sys-adm.org.ua
Generating a 2048 bit RSA private key
.......................++++++
.....................++++++
writing new private key to 'gw1-kv.sys-adm.org.ua.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UA]:
State or Province Name (full name) [Ukraine]:
Locality Name (eg, city) [Kharkov]:Kiev
Organization Name (eg, company) [SysAdm]:
Organizational Unit Name (eg, section) []:Kiev VPN Server
Common Name (eg, your name or your server's hostname) []:gw1-kv.sys-
adm.org.ua
Email Address [hostmaster@sys-adm.org.ua]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234567
An optional company name []:www.sys-adm.org.ua
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'UA'
stateOrProvinceName :PRINTABLE:'Ukraine'
```

```
localityName:PRINTABLE:'Kiev'
organizationName:PRINTABLE:'SysAdm'
organizationalUnitName:PRINTABLE:'Kiev VPN Server'
commonName:PRINTABLE:'gw1-kv.sys-adm.org.ua'
emailAddress:IA5STRING:'hostmaster@sys-adm.org.ua'
Certificate is to be certified until Mar5 20:04:49 2018 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Теперь генерируем ключ и сертификат для второй точки нашего туннеля.

```
# ./build-key gw1-kh.sys-adm.org.ua
Generating a 2048 bit RSA private key
.....................++++++
......++++++
writing new private key to 'gw1-kh.sys-adm.org.ua.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UA]:
State or Province Name (full name) [Ukraine]:
Locality Name (eg, city) [Kharkov]:
Organization Name (eg, company) [SysAdm]:
Organizational Unit Name (eg, section) []:Kharkov VPN Server
Common Name (eg, your name or your server's hostname) []:gw1-kh.sys-
adm.org.ua
Email Address [hostmaster@sys-adm.org.ua]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234567
An optional company name []:www.sys-adm.org.ua
```

```
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'UA'
stateOrProvinceName :PRINTABLE:'Ukraine'
localityName:PRINTABLE:'Kharkov'
organizationName:PRINTABLE:'SysAdm'
organizationalUnitName:PRINTABLE:'Kharkov VPN Server'
commonName:PRINTABLE:'gw1-kh.sys-adm.org.ua'
emailAddress:IA5STRING:'hostmaster@sys-adm.org.ua'
Certificate is to be certified until Mar5 20:08:15 2018 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Примечание

Отличие скриптов `build-key <name>` и `build-key-server <name>` заключается в том, что при генерации сертификата с помощью срипта build-key-server мы указываем дополнительную секцию в openssl.cnf — `[server]`. В данной секции мы добавляем в наш будущий сертификат поле `nsCertType=server`. Данный метод позволяет бороться с т. н. "Man-in-the-Middle"-атаками.

Если вы создавали сертификаты, используя статью "SSL Howto", то перед созданием сертификата для сервера вам необходимо будет отредактировать ваш openssl.cnf и добавить в самый конец следующие строки.

```
[ server ]
basicConstraints=CA:FALSE
nsCertType = server
nsComment = "Kiev VPN Server Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```

А при генерации самого сертификата использовать следующую команду:

```
# openssl ca -out gw1-kv.sys-adm.org.ua.crt -config ./openssl.cnf \
-infiles gw1-kv.sys-adm.org.ua.csr -extensions server
```

Теперь генерируем так называемые параметры Диффи — Хеллмана, которые будут использоваться только на стороне сервера.

```
# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
```

```
This is going to take a long time
...
...
...
```

И последнее, что нам осталось сделать — это сгенерировать static pre-shared key.

```
# openvpn --genkey --secret secret.key
```

В табл. 5.1 указано, где используются ключи и сертификаты, которые мы создали.

Таблица 5.1. *Использование ключей и сертификатов*

Имя файла	Кем используется	Назначение	Защита
ca.crt	сервер и клиент	Root CA certificate	Нет
ca.key	только на машине, производящей подпись сертификатов	Root CA key	Да
dh1024.pem	только сервер	Параметры Diffie Hellman'a	Нет
secret.key	сервер и клиент	Shared secret key	Нет
gw1-kv.sys-adm.org.ua.crt	только сервер	Server Certificate	Нет
gw1-kv.sys-adm.org.ua.key	только сервер	Server Key	Да
gw1-kh.sys-adm.org.ua.crt	только клиент	Client Certificate	Нет
gw1-kh.sys-adm.org.ua.key	только клиент	Client Key	Да

Настройка OpenVPN

При запуске демона OpenVPN он считывает файлы с расширением conf из папки /etc/openvpn. Имя файла не имеет значения. Поэтому мы создаем собственный конфигурационный файл со следующим содержимым на стороне сервера:

```
# cat /etc/openvpn/kiev-kharkov.conf | grep -v ^$
dev tun
local 82.207.89.100
ifconfig 10.3.0.1 10.3.0.2
```

```
port 1194
proto udp
user nobody
group nobody
comp-lzo
ping 15
ping-restart 45
persist-key
persist-tun
log /var/log/openvpn.log
status /var/log/openvpn-status.log
verb 3
tls-server
ca ca.crt
cert gw1-kv.sys-adm.org.ua.crt
key gw1-kv.sys-adm.org.ua.key
dh dh1024.pem
tls-auth secret.key 0
```

Также копируем следующие файлы в папку /etc/openvpn и выставляем необходимые права.

```
ca.crt,
secret.key,
dh1024.pem,
gw1-kv.sys-adm.org.ua.crt,
gw1-kv.sys-adm.org.ua.key
# cd /etc/openvpn/
# chmod 600 ca.crt secret.key dh1024.pem
# chmod 600 gw1-kv.sys-adm.org.ua.crt
# chmod 600 gw1-kv.sys-adm.org.ua.key
```

Производим аналогичную процедуру и на стороне клиента. Создаем собственный конфигурационный файл со следующим содержимым:

```
# cat /etc/openvpn/kharkov-kiev.conf | grep -v ^$
dev tun
remote 82.207.89.100
ifconfig 10.3.0.2 10.3.0.1
port 1194
proto udp
user nobody
group nobody
```

```
comp-lzo
ping 15
ping-restart 45
persist-tun
persist-key
log /var/log/openvpn.log
status /var/log/openvpn-status.log
verb 3
tls-client
ca ca.crt
cert gw1-kh.sys-adm.org.ua.crt
key gw1-kh.sys-adm.org.ua.key
tls-auth secret.key 1
ns-cert-type server
```

Копируем следующие файлы в папку /etc/openvpn и выставляем необходимые права.

```
ca.crt,
secret.key,
gw1-kh.sys-adm.org.ua.crt,
gw1-kh.sys-adm.org.ua.key
# cd /etc/openvpn/
# chmod 600 ca.crt secret.key
# chmod 600 gw1-kh.sys-adm.org.ua.crt
# chmod 600 gw1-kh.sys-adm.org.ua.key
```

На этом настройку OpenVPN можно считать завершенной. Осталось только запустить сам демон на обоих серверах и настроить автоматический запуск при старте системы.

Выполняем следующие команды на стороне сервера

```
[root@gw1-kv openvpn]# chkconfig --level 35 openvpn on
[root@gw1-kv openvpn]# service openvpn start
Starting openvpn:[OK]
```

И на стороне клиента

```
[root@gw1-kh openvpn]# chkconfig --level 35 openvpn on
[root@gw1-kh openvpn]# service openvpn start
Starting openvpn:[OK]
```

При этом в системе должен был появиться новый интерфейс — tun0

```
# ifconfig tun0
tun0Link encap:UNSPECHWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
```

```
inet addr:10.3.0.2P-t-P:10.3.0.1Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICASTMTU:1500Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b)TX bytes:0 (0.0 b)
```

На данный момент сервер и клиент должны "видеть" друг друга. Для проверки воспользуемся командой ping

```
[root@gw1-kh log]# ping -c 4 10.3.0.1
PING 10.3.0.1 (10.3.0.1) 56(84) bytes of data.
64 bytes from 10.3.0.1: icmp_seq=1 ttl=64 time=1.86 ms
64 bytes from 10.3.0.1: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 10.3.0.1: icmp_seq=3 ttl=64 time=2.07 ms
64 bytes from 10.3.0.1: icmp_seq=4 ttl=64 time=2.85 ms

--- 10.3.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 1.062/1.964/2.854/0.639 ms
[root@gw1-kv log]# ping -c4 10.3.0.2
PING 10.3.0.2 (10.3.0.2) 56(84) bytes of data.
64 bytes from 10.3.0.2: icmp_seq=1 ttl=64 time=4.18 ms
64 bytes from 10.3.0.2: icmp_seq=2 ttl=64 time=1.12 ms
64 bytes from 10.3.0.2: icmp_seq=3 ttl=64 time=2.09 ms
64 bytes from 10.3.0.2: icmp_seq=4 ttl=64 time=2.11 ms

--- 10.3.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 1.128/2.378/4.184/1.116 ms
```

Для того чтобы работал доступ к серверу терминалов, необходимо внести некоторые изменения в firewall. Далее я приведу лишь минимальный набор команд, необходимый для проверки работы нашего туннеля. Будем считать, что форвардинг включен на обоих серверах и политика по умолчанию во всех цепочках — ACCEPT.

На стороне клиента выполняем следующую команду:

```
# iptables -t nat -A POSTROUTING -s 192.168.127.0/255.255.255.0 -o
tun0 -j SNAT --to-source 10.3.0.2
```

А на стороне сервера выполняем следующую команду:

```
# iptables -t nat -A PREROUTING -p tcp -i tun0 -d 10.3.0.1 --dport
3389 -j DNAT --to-destination 192.168.1.2:3389
```

Теперь запускаем клиента подключения к удаленному рабочему столу на любой машине в харьковском офисе и в строке адреса набираем 10.3.0.1. Если вы все правильно настроили, то вы должны соединиться с сервером терминалов.

Мы можем сделать так, что подсети 192.168.1.0/24 и 192.168.127.0/24 будут видеть друг друга "напрямую". Для этого достаточно на каждом из шлюзов прописать маршрут в соответствующую подсеть.

Прописываем маршрут в подсеть 192.168.127.0/24 на стороне сервера

```
[root@gw1-kv log]# route add -net 192.168.127.0/24 gw 10.3.0.2
[root@gw1-kv log]# route -n | grep tun0
10.3.0.20.0.0.0 255.255.255.255 UH000 tun0
192.168.127.0 10.3.0.2255.255.255.0 UG000 tun0
```

А на стороне клиента прописываем маршрут в подсеть 192.168.1.0/24

```
[root@gw1-kh log]# route add -net 192.168.1.0/24 gw 10.3.0.1
[root@gw1-kh log]# route -n | grep tun0
10.3.0.10.0.0.0 255.255.255.255 UH000 tun0
192.168.1.0 10.3.0.1255.255.255.0 UG000 tun0
```

Теперь производим проверку "видимости" подсети 192.168.127.0/24 с помощью команды ping. Для этого на стороне сервера выполняем следующую команду:

```
[root@gw1-kv log]# ping -c 4 192.168.127.2
PING 192.168.127.2 (192.168.127.2) 56(84) bytes of data.
64 bytes from 192.168.127.2: icmp_seq=1 ttl=127 time=2.43 ms
64 bytes from 192.168.127.2: icmp_seq=2 ttl=127 time=2.06 ms
64 bytes from 192.168.127.2: icmp_seq=3 ttl=127 time=1.81 ms
64 bytes from 192.168.127.2: icmp_seq=4 ttl=127 time=2.65 ms

--- 192.168.127.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.810/2.240/2.653/0.326 ms
```

Ну и для чистоты совести производим проверку "видимости" подсети 192.168.1.0/24 с помощью команды ping. Для этого на стороне клиента выполняем следующую команду:

```
[root@gw1-kh log]# ping -c 4 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=127 time=4.70 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=127 time=1.93 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=127 time=1.75 ms
```

```
64 bytes from 192.168.1.2: icmp_seq=4 ttl=127 time=2.65 ms

--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 1.752/2.761/4.705/1.173 ms
```

Теперь любой клиент из подсети 192.168.127.0/24 сможет попасть на сервер терминалов, находящийся в подсети 192.168.1.0/24, просто указав в строке адреса 192.168.1.2. К сожалению, при такой настройке в сетевом окружении клиентов Windows вы не сможете использовать NetBIOS имена компьютеров, а только их IP-адреса. Если вам необходим данный функционал, то на одной из сторон можно поднять WINS-сервер. Или настроить VPN в режиме моста.

На этом настройку нашей системы можно считать завершенной.

О чем не сказано…

Мы не рассматривали в этой главе сервер LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам).

Вероятно, для описания Linux-сервера, содержащего все необходимые в сети службы, потребовалась бы целая книга. Во всяком случае, даже описание настройки почтового сервера в различных вариантах установки может занять большую главу. А если требуется сервер, который заменит Windows AD, придется согласовывать работу LDAP, Samba, Postfix, возможно, и других серверов. Можно почитать о настройке такого сервера в незавершенной, по всей видимости, статье по адресу **http://freesource.info/wiki/AltLinux/Dokumentacija/OpenLDAP?v=19no&**. Материалов по настройке такого сервера в Интернете появляется все больше, а разработчики пытаются создавать графические интерфейсы для него, позволяющие эффективно им управлять. Одна из последних разработок — Mandriva DS. Но пока, при отсутствии достаточного опыта в настройке серверных служб, трудно найти доступные для понимания начинающего материалы, чтобы самостоятельно настроить сервер, который заменит контроллер домена Windows. Тем не менее, если вы решились применить в вашей небольшой сети Linux-сервер, начните с малого. Настройте самые необходимые в вашей сети службы и… приступайте к экспериментам, которые лучше проводить на отдельном компьютере. Пока сеть небольшая, можно обойтись без централизованного хранилища параметров доступа к ресурсам сети. Но кто знает, что нас ждет впереди?

Глава 6

Средства администратора малой сети

Задачи администрирования часто выполняются в консольном режиме. Но есть и графические утилиты, с помощью которых также можно выполнить значительное число операций, связанных с администрированием рабочих станций, серверов и сети. Пока еще состав графических средств администрирования Linux и их вид может отличаться от дистрибутива к дистрибутиву. Отличительной особенностью консольных команд является возможность их запуска в конвейерном режиме, когда результат работы одной программы передается другой программе для дальнейшей обработки. Это позволяет выполнять достаточно сложные команды, которые в Windows могут быть выполнены только с помощью специально написанных программ. В то же время, графические средства позволяют получить данные в наглядном виде и не требуют запоминания консольных команд. Рассмотрим несколько полезных для администратора утилит как для консольного режима, так и с графическим интерфейсом.

Утилиты для контроля состояния рабочих станций и серверов

Эти утилиты применяются для обслуживания рабочих станций и серверов. Несмотря на то что Linux изначально создавалась для работы в сети, есть параметры, которые следует настраивать независимо от того, работает компьютер в локальной сети или он подключен к Интернету, или вообще не подключен ни к какой сети. Последний вариант встречается в наше время довольно редко. Рабочая станция, имеющая модемное подключение к Интернету, большую часть времени работает без сети. Есть компьютеры, которые выполняют специфические задачи, при выполнении которых необходимо обеспечить максимальный уровень защиты информации. В этом случае машину вообще не подключают к Интернету и к сети. В практике работы автора

такие рабочие места встречались. Обмен информацией с другими машинами был возможен только через съемные носители информации, подлежавшие строгому учету. Но администрирование таких рабочих станций все равно необходимо. Пользователь должен получить соответствующее его задачам рабочее окружение, а состояние системы должно контролироваться, чтобы исключить возможность случайной потери данных и обеспечить актуальность версий программ пользователя.

Конечно, Linux очень стабильная система. Практика показывает, что при грамотном обслуживании Linux значительно стабильнее Windows. Если серверы Windows в последние годы начали работать достаточно стабильно, то рабочая станция Windows обычно не выдерживает непрерывной работы в течение нескольких дней без потери производительности. Операционные системы семейства Linux могут работать на рабочей станции месяцами без перезагрузок. Если в домашних условиях такая работа компьютера не так уж необходима (если только на вашем компьютере не работает какой-нибудь веб-сервер для вашей сети), то в условиях предприятий возможны ситуации, когда рабочая станция не выключается практически никогда. Рабочие места диспетчеров, управляющих производственными процессами или движением транспортных средств, предполагают непрерывную работу в течение длительного времени. Пользователи передают друг другу смену, а на экране компьютера продолжается отображение текущей ситуации, которая требует постоянного внимания оператора. На таких рабочих местах Linux позволит увеличить время непрерывной работы, уменьшить время, необходимое для обслуживания рабочей станции. Тем не менее, как уже было отмечено, требуется грамотное администрирование системы.

Представляет интерес тот факт, что Linux всегда может быть доступен для администратора по сети. Современные Windows-системы для рабочих станций тоже могут обслуживаться удаленно, но в небольших простых сетях часто удобнее проводить процедуры обслуживания через графический интерфейс пользователя. При этом рабочие станции Windows без применения специальных программ не позволяют одновременную работу удаленного и локального пользователя — а Linux позволяет это делать. Локальный пользователь может и не знать, что к его компьютеру подключился администратор.

Способы удаленного управления и администрирования

Для удаленного администрирования Linux есть несколько способов. Это и применение различных вариантов сервера VNC на рабочей станции, и использование подключения SSH, которое позволяет удаленно запускать даже программы с графическим интерфейсом, XDMCP и др.

XDMCP

XDMCP (X Display Manager Control Protocol) позволяет подключаться к удаленному компьютеру не только для администрирования, но и просто для работы на нем, как на сервере терминалов. Следует только учесть, что защищенность такого подключения не высока, и его можно применять лишь в вашей локальной сети. Подключения через Интернет по протоколу XDMCP небезопасны. Тем не менее, в локальной сети, которая защищена от несанкционированного доступа извне, такое подключение может быть использовано с успехом.

Чтобы обеспечить возможность такого подключения, во всех версиях Linux есть графический интерфейс. Так, например, в CentOS 5.3, пройдя по пути **Параметры | Администрирование | Экран входа в систему**, вы откроете окно **Параметры окна входа в систему** (рис. 6.1), в котором на вкладке **Удаленный вход** достаточно выбрать режим удаленного входа в поле со списком **Стиль**. По умолчанию удаленный вход запрещен. Если вы хотите ограничить число одновременных удаленных входов, достаточно нажать кнопку **Настроить XDMCP** и указать в соответствующем поле открывшейся формы требуемое число. В CentOS по умолчанию разрешено 16 подключений.

Как и в Windows, не следует пытаться точно запоминать описанные операции. Важнее понять их смысл. От дистрибутива к дистрибутиву наименования пунктов меню и содержание форм могут несколько отличаться. Пройдите по другим вкладкам этого окна и посмотрите, какие параметры вас могут заинтересовать. Возможно, вы захотите разрешить удаленный вход для администратора системы, это можно сделать на вкладке **Безопасность.**

Во всех версиях Linux, используя для удаленного входа учетную запись, отличающуюся от учетной записи локального пользователя, вы подключитесь к рабочему столу, которого локальный пользователь видеть не будет.

Подключиться удаленно к системе по протоколу XDMCP проще всего, используя стандартную для всех современных версий Linux программу Клиент Терминального сервера (рис. 6.2).

Этот клиент поддерживает возможность подключения к удаленной системе по нескольким распространенным протоколам: RDP, RDPv5, VNC, XDMCP, ICA, и можете всегда им воспользоваться. В частности, настройка подключения к терминалу Windows выполняется привычным для пользователей Windows способом.

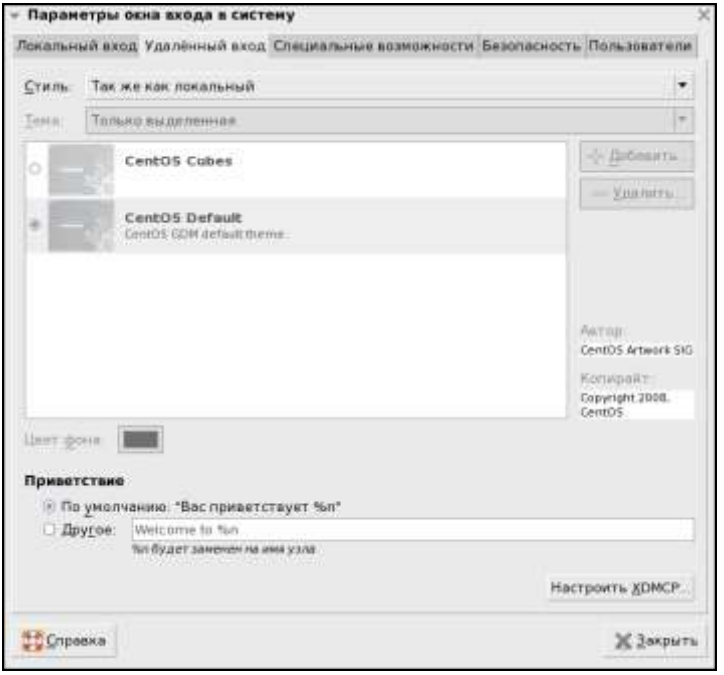


Рис. 6.1. Окно **Параметры окна входа в систему**

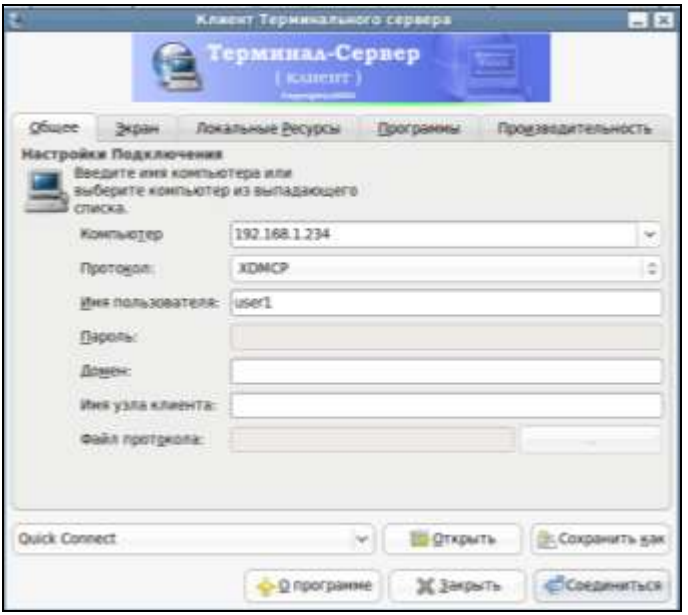


Рис. 6.2. Окно **Клиент Терминального сервера**

VNC

В некоторых случаях администратору может потребоваться подключение к рабочему столу пользователя. В этом случае достаточно использовать стандартный для всех Linux способ подключения посредством VNC (Virtual Network Computing). По умолчанию во все дистрибутивы включен сервер и клиент VNC.

Пройдя по пути **Параметры | Удаленный рабочий стол**, вы откроете форму **Параметры удаленного рабочего стола** (рис. 6.3).

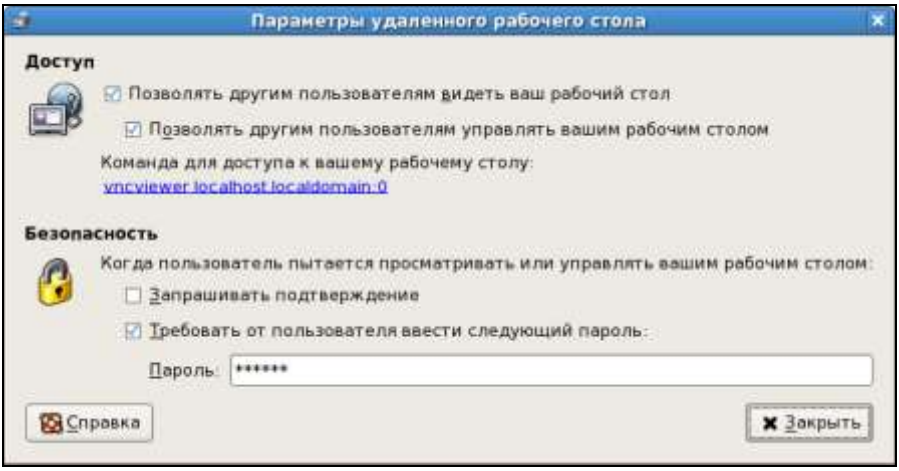


Рис. 6.3. Окно **Параметры удаленного рабочего стола**

Все параметры доступа, которые можно выбрать в этом окне, понятны без лишних объяснений. Подключиться к удаленной системе можно посредством Клиента Терминального сервера, рассмотренного ранее, или из командной строки, введя команду `vncviewer <IP-адрес_удаленного_компьютера>`.

SSH

Это стандартный для Linux способ удаленного запуска программ. Администрируя удаленную систему, вы можете выполнить необходимые команды как в консольном режиме, так и в графическом. Этот способ удаленного доступа требует более углубленного знания системы. Настройка его не всегда проста. По ссылке **http://freesource.info/wiki/AltLinux/Dokumentacija/NastrojjkaSSH?v=9xm&** вы можете прочитать о настройках сервера и клиента. Если терпения у вас хватит, то вы получите очень хороший инструмент как для администрирования, так и просто для организации удаленного доступа к системам Linux. Причем

для Windows есть два приложения, которые позволяют Windows-клиентам использовать SSH для подключения к удаленным компьютерам Linux. Поищите в Интернете информацию о работе с программами PuTTY и Xming. Уверен, что они вам понравятся.

При первоначальном знакомстве с SSH для обеспечения возможности запуска графических приложений в удаленном режиме следует соблюсти некоторые условия.

Управление процессами

На рабочих станциях и серверах нередко возникает необходимость выяснить, какие процессы запущены, какие файлы с ними связаны, остановить процесс, работающий не корректно. В Windows для выполнения подобных задач есть Диспетчер задач, имеющий весьма ограниченные возможности, и утилиты сторонних разработчиков. В Linux все средства для управления процессами есть в каждом дистрибутиве.

Управлять процессами пользователь может в соответствии со своими правами в системе. Суперпользователь имеет неограниченные права, а рядовой пользователь может управлять процессами, которыми он владеет. Для просмотра и управления процессами есть несколько команд, из которых чаще всего применяются `top` и `ps`. Команда `top` выводит на экран (рис. 6.4) список запущенных процессов в реальном времени, обновляя картину каждые три секунды.

В этом окне мы можем увидеть информацию о времени работы компьютера (в заголовке), числе пользователей, работающих в системе, числе запущенных процессов, загруженности процессора и памяти. Под заголовком — перечень процессов, который можно сортировать по различным признакам:

- <Shift>+<N> — сортировка по PID;
- <Shift>+<A> — сортировать процессы по возрасту;
- <Shift>+<P> — сортировать процессы по использованию ЦПУ;
- <Shift>+<M> — сортировать процессы по использованию памяти;
- <Shift>+<T> — сортировка по времени выполнения.

На рис. 6.5 показано окно терминала GNOME, запущенное пользователем user1. Идентификатор этого процесса (PID) 15494. Также можно увидеть процессы, запущенные другими пользователями. Например, пользователь beard использует firefox (PID 4298). Более подробно о команде можно прочитать в справке по команде и в Интернете, например по ссылке **http://www.linuxcenter.ru/lib/books/kostromin/gl_08_04.phtml**.

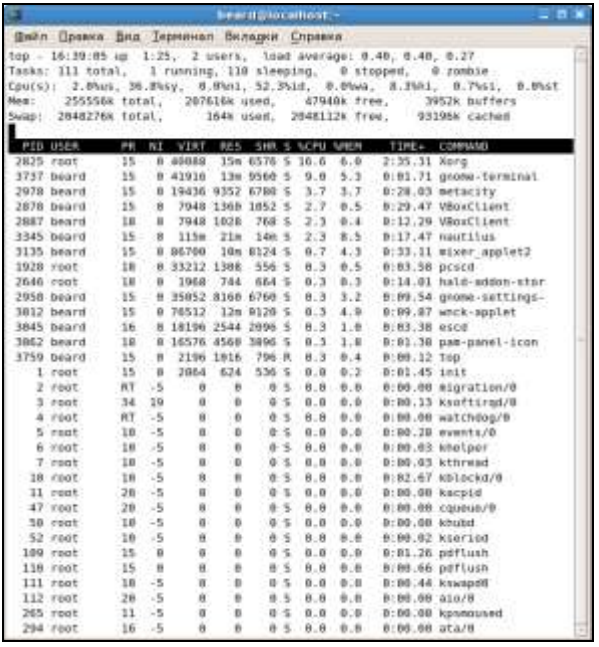


Рис. 6.4. Окно терминала со списком запущенных процессов, выведенных командой `top`

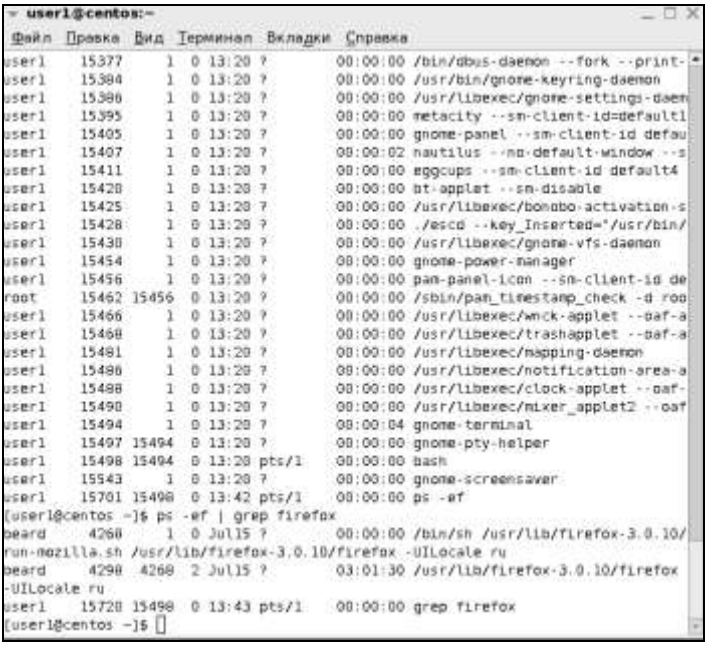


Рис. 6.5. Окно терминала со списком запущенных процессов, выведенных командой `ps`

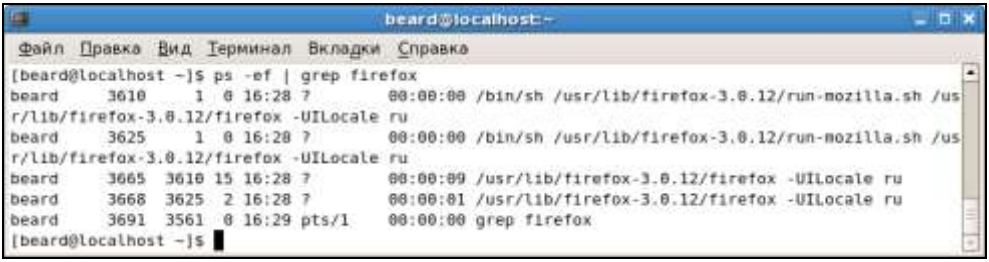


Рис. 6.6. Окно терминала со списком запущенных процессов, выведенных командой `ps -ef | grep firefox`

Команда `ps` с аргументами `-ef` (рис. 6.5) выводит весь перечень процессов в системе. На рисунке конец списка занимает всю площадь окна терминала. Для того чтобы вывести на экран информацию только об интересующих процессах, можно применять другие опции, о которых можно узнать из справки по команде, или дополнительные команды. На рис. 6.6 команда `ps -ef` была выполнена совместно с командой `grep firefox`, которая из всего потока вывода команды `ps` выбирает строки со словом `firefox`. Теперь в списке только пять строк. В последней строке информация о только что запущенной команде, а в предыдущих — информация о процессе firefox, который выполняется от имени пользователя beard. Первая строка показывает основной процесс с PID 3610, а вторая — дочерний процесс (возможно, вкладка в окне браузера) с PID 3625. При необходимости можно остановить какой-либо процесс с помощью команды `kill`. Но остановить можно только процесс, владельцем которого вы являетесь, либо от имени суперпользователя. Для получения прав управления всеми процессами можно получить права пользователя root, введя команду `su -` и пароль суперпользователя по запросу системы. После этого вы можете остановить требуемый процесс, введя команду `kill` и PID процесса, который хотите остановить. Понятно, что останавливая процесс, вы должны хорошо представлять себе последствия этого действия. На странице **http://www.linuxcenter.ru/lib/books/kostromin/gl_08_04.phtml** вы можете найти еще много полезных сведений об уже рассмотренных командах и некоторых других, которые могут вам пригодиться при управлении процессами в Linux.

Управление учетными записями

Как и в системах Windows, операционные системы Linux требуют, чтобы каждый пользователь имел необходимые для работы в системе права. Но эти права должны быть ограничены определенными рамками, чтобы пользова-

тель не мог навредить системе, а вредоносные программы не могли получить достаточных полномочий для достижения своих деструктивных целей.

В современных дистрибутивах Linux всегда есть графические средства для управления учетными записями пользователей. Но и в окне терминала можно выполнить практически все связанные с этой задачей действия. Для этого есть несколько легко запоминающихся команд, которые приведены в табл. 6.1.

Таблица 6.1. *Команды управления учетными записями пользователей*

Команда	**Описание**
`groupadd group_name`	создание новой группы
`groupdel group_name`	удаление группы
`groupmod -n new_group_name old_group_name`	переименование группы
`useradd -c "Name Surname " -g admin -d /home/user1 -s /bin/bash user1`	создание нового пользователя, принадлежащего группе "admin"
`useradd user1`	создание нового пользователя
`userdel -r user1`	удаление пользователя ('-r', удаляет домашний каталог)
`usermod -c "User FTP" -g system -d /ftp/user1 -s /bin/nologin user1`	изменить пользовательские атрибуты
`passwd`	сменить пароль
`passwd user1`	изменить пользовательский пароль (доступно только администратору)
`chage -E 2005-12-31 user1`	установить дату окончания действия учетной записи пользователя user1
`pwck`	проверка синтаксиса и формата файла '/etc/passwd', существования пользователей и их каталогов
`grpck`	проверка синтаксиса и формата файла '/etc/group', существования групп
`newgrp group_name`	вход в новую группу, чтобы изменить группу по умолчанию для вновь создаваемых файлов

Графический интерфейс управления учетными записями доступен пользователю root. В CentOS это окно можно вызвать, набрав в командной строке `system-config-users` от имени пользователя root. Графический интерфейс

управления пользователями интуитивно понятен и нагляден. На рис. 6.7 приведен интерфейс **Менеджер пользователей** для управления учетными записями пользователей из CentOS 5.3.

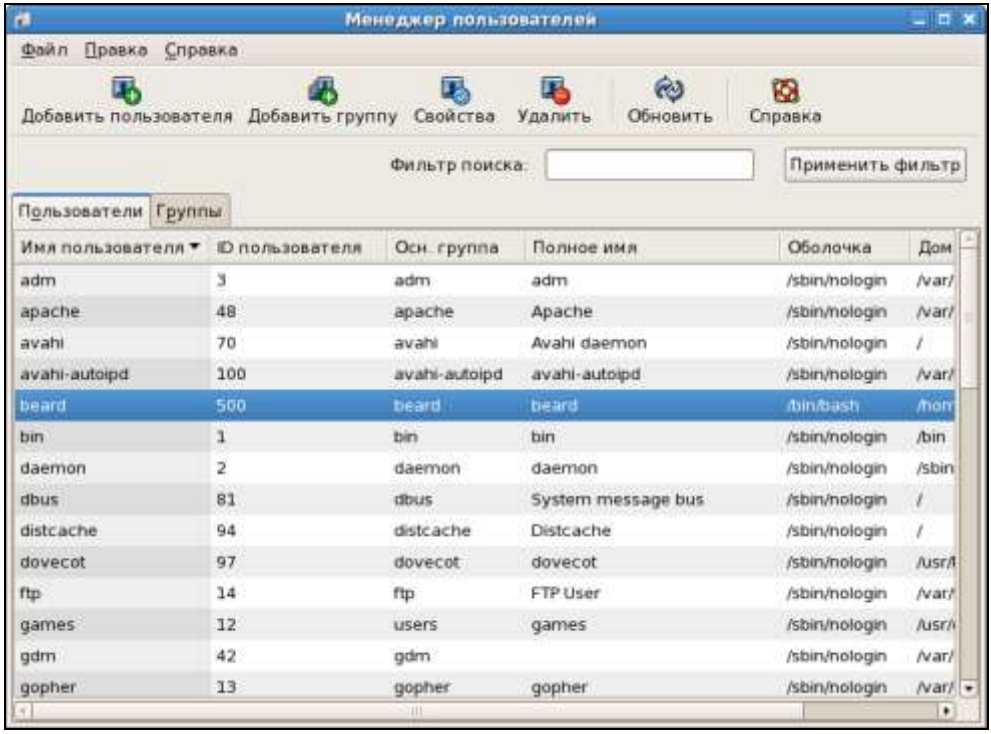


Рис. 6.7. Окно **Менеджер пользователей**

Кнопка **Применить фильтр** позволяет выбирать пользователей, имена которых включают определенные символы, если их ввести в поле **Фильтр поиска**. Воспользовавшись пунктом оконного меню **Правка** | **Параметры**, можно включить отображение системных пользователей (на рисунке включено).

Управление службами

Эта задача в Windows решается посредством специальных оснасток. В Linux управление службами имеет некоторые отличия в связи с существованием нескольких режимов работы системы. Среди этих режимов основными можно считать обычный консольный режим и графический режим. Службы, которые должны обеспечивать работу программ в графическом режиме, не должны запускаться в консольном режиме, а службы, поддерживающие про-

граммы, не связанные с графикой (например звуковая подсистема), вполне могут быть запущены в консольном режиме. Для управления уровнем запуска служб и управления ими можно воспользоваться командой **Система | Администрирование | Настройка сервероа | Службы** или терминальной командой от имени пользователя root `system-config-services`. В обоих случаях вы увидите на экране окно **Настройка служб** (рис. 6.8).

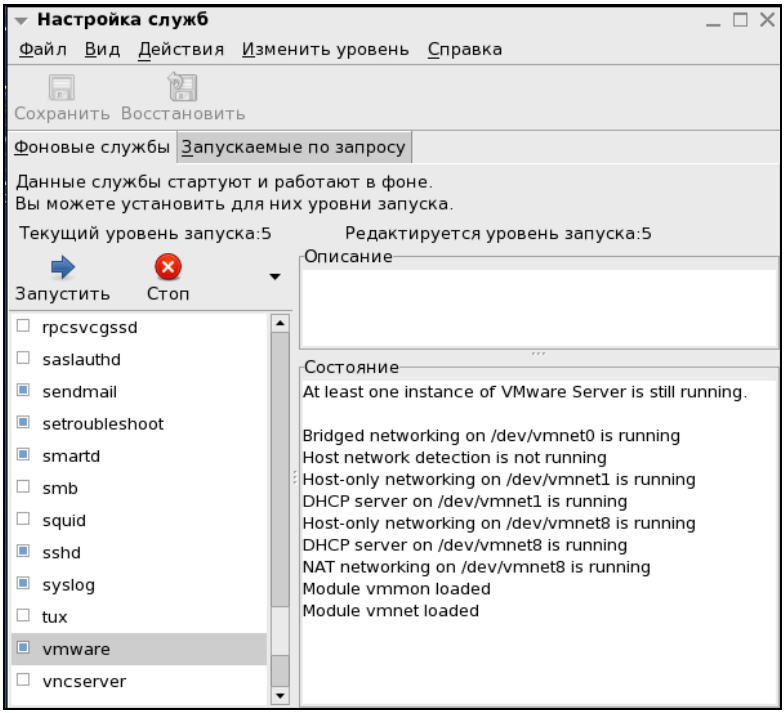


Рис. 6.8. Окно **Настройка служб**

Пользуясь оконным меню и кнопками **Запустить** и **Стоп**, вы можете управлять уровнем запуска служб, останавливать и запускать их.

Работа с дисковой подсистемой

При анализе состояния системы может быть необходимо проверить состояние дисковой подсистемы, наличие свободного места на дисках, создать или удалить разделы, отформатировать логические диски. Частой задачей может быть монтирование дисков, подключенных к компьютеру. Хотя в современных дистрибутивах эта операция часто выполняется автоматически, полезно знать и соответствующие команды.

Наиболее часто используются, пожалуй, две простые утилиты: – `df` и `mount`. Первая показывает все примонтированные диски и разделы, их размер и свободное место на них. Вторая всегда выполняется с параметрами и позволяет подключить к системе диски, разделы или внешние сменные носители. Например, командой `mount /mnt/disk ext3 /dev/sda4` можно примонтировать, сделав доступным для системы, раздел sda4, отформатированный в файловой системе ext3. При этом каталог /mnt/disk должен уже существовать. Для размонтирования раздела применяется команда `umount /mnt/disk`.

Системный монитор

Во многих дистрибутивах Linux присутствует эта очень удобная графическая утилита. На рис. 6.9 приведен вид этой программы, открытой на вкладке **Ресурсы**. Здесь можно увидеть степень загруженности процессора, виртуальной памяти и сети. Эта информация бывает очень полезной при отладке приложений или для контроля работы сервера.

Рис. 6.9. Окно **Системный монитор**, вкладка **Ресурсы**

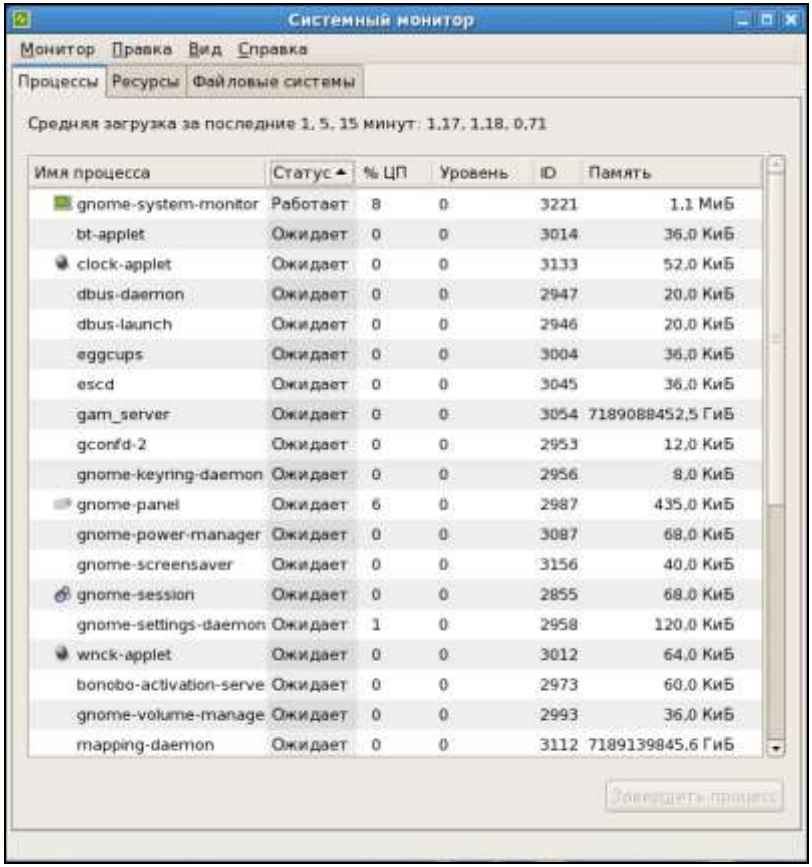


Рис. 6.10. Окно **Системный монитор**, вкладка **Процессы**

Открыв вкладку **Процессы** (рис. 6.10), можно увидеть информацию, уже знакомую нам по выводу команды `ps`. Настроить вывод информации можно с помощью пункта меню **Правка**. Как и любую другую графическую утилиту, Системный монитор можно вызвать из окна терминала. Для этого достаточно набрать команду `gnome-system-monitor`.

Утилиты для контроля состояния сети

Чаще всего бывает необходимо проверить доступность узлов в сети, определить маршрут до узла, посмотреть настройки сетевых адаптеров, настроить маршрутизацию или преобразование адресов (NAT). Само собой, требуется элементарная настройка сетевых интерфейсов и периодический контроль их состояния.

Для выполнения этих задач есть как графические, так и консольные утилиты. Графические могут иметь отличающиеся от дистрибутива к дистрибутиву интерфейсы. В версиях Linux на основе Linux Red Hat, например CentOS, графические утилиты позволяют выполнить достаточно полную настройку сетевых интерфейсов. На рис. 6.11 приведено окно **Настройка сети** в CentOS 5.3. Его можно открыть, пройдя по пути **Система** | **Администрирование** | **Сеть**.

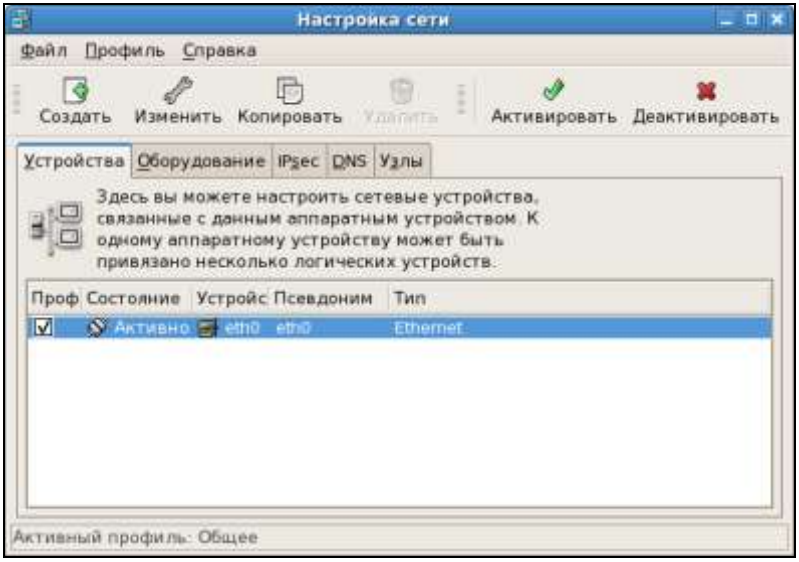


Рис. 6.11. Окно **Настройка сети**

Выделив в окне настраиваемое устройство (в данном случае eth0), нажмите кнопку **Изменить**. Откроется окно **Устройство Ethernet** (рис. 6.12), в котором можно указать все необходимые параметры для настройки сети. Если вы уже настраивали параметры сети на компьютерах Windows, то все параметры вам понятны и настройка не составит труда.

Осваивая различные версии Linux, вы можете встретить более или менее удобные графические утилиты для настройки сети. Но в любой версии Linux совершенно одинаково работают консольные утилиты, которые можно применять всегда.

Примечание

Важно помнить, что настройка модулей операционной системы должна выполняться только одним способом. Иначе настройки, выполненные из консоли, можно потерять, запустив графическую утилиту, предназначенную для той же цели.

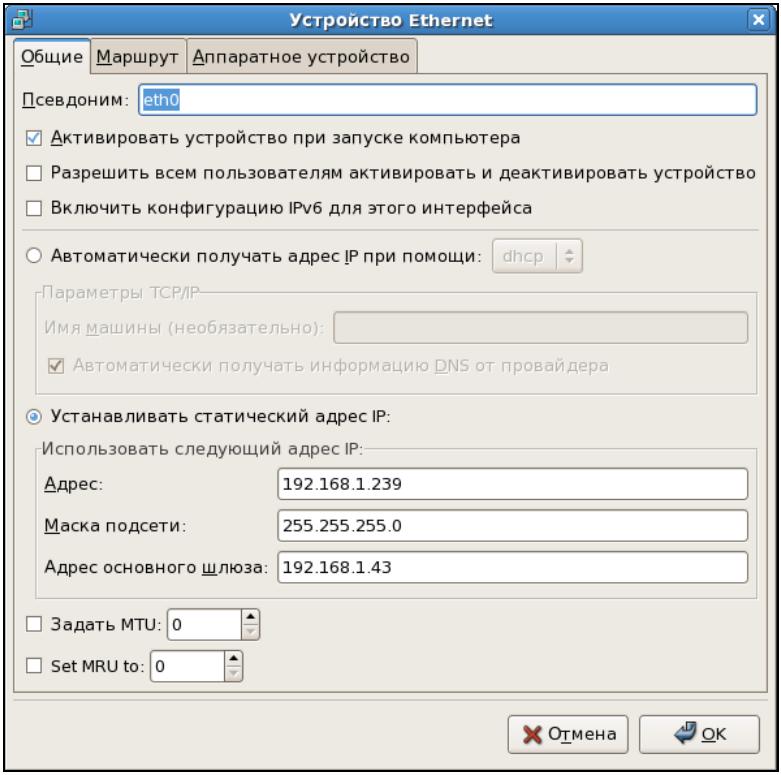


Рис. 6.12. Окно **Устройство Ethernet**

Для повторения однотипных настроек все команды можно записать и сохранить в исполняемых файлах. Это позволит существенно сократить затраты времени на проведение настроек и не искать графические утилиты в незнакомой версии Linux.

Настройка NAT

Одна из часто возникающих задач при настройке сети — включить преобразование адресов (NAT — Network Address Translate) для подключения пользователей к Интернету через один компьютер. В Linux для этого есть простая команда `iptables`. Сложность здесь только в том, что следует указать параметры команды, которые необходимы именно в вашем случае. Команда для выполнения решаемой задачи выглядит так:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Возможно, что ваш сетевой интерфейс, через который будет осуществляться доступ в Интернет, имеет другое имя — eth1 или eth2, замените им

имя eth0, указанное в команде. Больше никаких параметров изменять не потребуется.

Конечно, более тонкие настройки потребуют обращения к справке по `iptables`.

Контроль и изменение параметров сети

Графическую утилиту "Настройка сети" мы уже рассмотрели. Но есть консольные утилиты, которые позволяют быстро решить вопросы настройки сети в любой версии Linux.

`Ifconfig` — одна из таких утилит. Если выполнить команду `ifconfig` без параметров в окне терминала от имени суперпользователя root, то на экран будет выведен перечень всех существующих в системе интерфейсов и их текущие настройки. Вывод команды `ifconfig` на компьютере автора показан ниже:

```
[beard@brd-cent ~]$ su -
Пароль:
[root@brd-cent ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:22:15:2F:41:E0
          inet addr:192.168.1.102  Bcast:192.168.1.255
Mask:255.255.255.0
          inet6 addr: fe80::222:15ff:fe2f:41e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:396301 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356645 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52770339 (50.3 MiB)  TX bytes:65413219 (62.3 MiB)
          Interrupt:177


lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:71530 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:57396905 (54.7 MiB)  TX bytes:57396905 (54.7 MiB)



vmnet1    Link encap:Ethernet  HWaddr 00:50:56:C0:00:01
          inet addr:172.16.81.1  Bcast:172.16.81.255
Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fec0:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

vmnet8    Link encap:Ethernet  HWaddr 00:50:56:C0:00:08
          inet addr:172.16.247.1  Bcast:172.16.247.255
Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fec0:8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@brd-cent ~]#
```

Как видим, кроме собственно настроек, показана информация о принятых и отправленных пакетах, о пакетах с ошибками, коллизиях и другая полезная информация. Нет информации о шлюзе по умолчанию, через который компьютер имеет доступ в Интернет. О шлюзе поговорим чуть позднее.

Та же самая утилита применяется для установки параметров сетевых интерфейсов.

Команда `ifconfig eth0 192.168.1.1 netmask 255.255.255.0` установит для интерфейса eth0 IP-адрес 192.168.1.1 и маску подсети 255.255.255.0.

После изменения параметров интерфейса его следует "перезагрузить", выполнив две команды:

```
ifconfig eth0 down
ifconfig eth0 up
```

Первая команда деактивирует интерфейс, а вторая снова активирует.

У утилиты `ifconfig` есть "родственница" `iwconfig`, которая предназначена для работы с беспроводными интерфейсами. Работает она аналогично `ifconfig`. Командой `iwconfig eth1 mtu 1400` можно установить значение MTU для беспроводного интерфейса eth1 равное 1400. Это может быть полезно для работы с интерфейсами WiMAX или WiFi, когда через них осуществляется общее подключение.

Для настройки шлюза по умолчанию придется применить еще одну утилиту. `Ifconfig` не позволила нам посмотреть и установить значение этого параметра. Для установки шлюза по умолчанию служит команда `route`. Достаточно выполнить ее, указав параметры, как в примере:

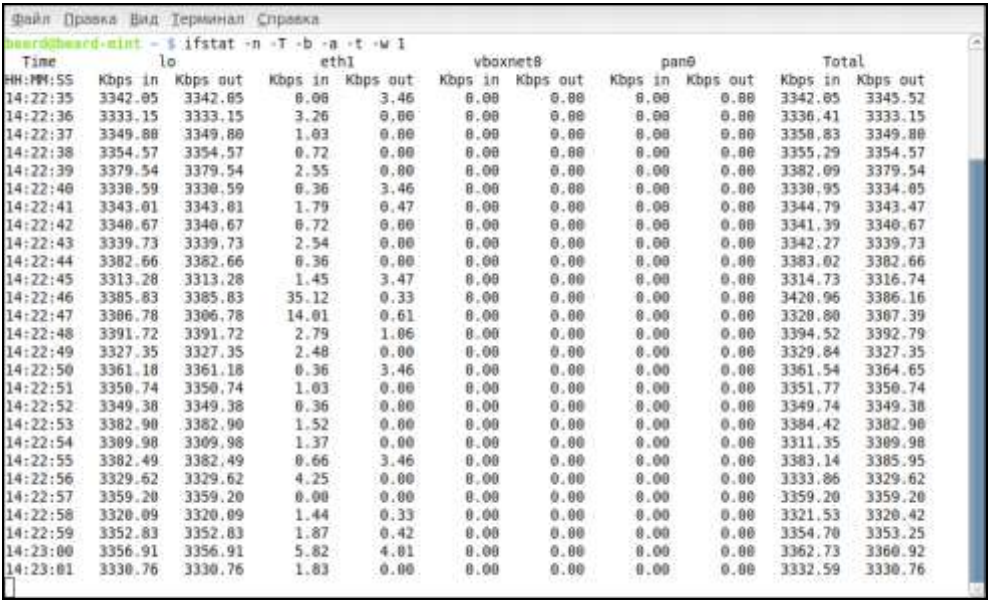
```
route add -net 0/0 gw 192.168.1.109.
```

IP-адрес следует изменить на необходимый.

Контроль сетевой активности и соединений

Настроив сетевые подключения, мы начинаем ими пользоваться. Конечно, нам интересно посмотреть, как активно работает подключение, сколько информации передается и принимается, нет ли лишних подключений, которые могут привести к перерасходу трафика. Существует много средств для выполнения таких задач, но наиболее просто они решаются с помощью консольных утилит `ifstat` и `netstat`.

На рис. 6.13 приведено окно терминала с выводом команды `ifstat -n -T -b -a -t -w 1`. Команда с указанными параметрами позволяет посмотреть активность всех сетевых интерфейсов, включая модемы и беспроводные адаптеры. Каждую секунду выводится новая строка с данными за прошедшую секунду.



Файл Правка Вид Терминал Справка

```
beard@beard-mint ~ $ ifstat -n -T -b -a -t -w 1
   Time            lo                eth1            vboxnet0            pan0              Total
HH:MM:SS   Kbps in  Kbps out   Kbps in  Kbps out   Kbps in  Kbps out   Kbps in  Kbps out   Kbps in  Kbps out
14:22:35   3342.05   3342.05      0.00      3.46      0.00      0.00      0.00      0.00   3342.05   3345.52
14:22:36   3333.15   3333.15      3.26      0.00      0.00      0.00      0.00      0.00   3336.41   3333.15
14:22:37   3349.80   3349.80      1.03      0.00      0.00      0.00      0.00      0.00   3350.83   3349.80
14:22:38   3354.57   3354.57      0.72      0.00      0.00      0.00      0.00      0.00   3355.29   3354.57
14:22:39   3379.54   3379.54      2.55      0.00      0.00      0.00      0.00      0.00   3382.09   3379.54
14:22:40   3330.59   3330.59      0.36      3.46      0.00      0.00      0.00      0.00   3330.95   3334.05
14:22:41   3343.01   3343.01      1.79      0.47      0.00      0.00      0.00      0.00   3344.79   3343.47
14:22:42   3340.67   3340.67      0.72      0.00      0.00      0.00      0.00      0.00   3341.39   3340.67
14:22:43   3339.73   3339.73      2.54      0.00      0.00      0.00      0.00      0.00   3342.27   3339.73
14:22:44   3382.66   3382.66      0.36      0.00      0.00      0.00      0.00      0.00   3383.02   3382.66
14:22:45   3313.28   3313.28      1.45      3.47      0.00      0.00      0.00      0.00   3314.73   3316.74
14:22:46   3385.83   3385.83     35.12      0.33      0.00      0.00      0.00      0.00   3420.96   3386.16
14:22:47   3386.78   3306.78     14.01      0.61      0.00      0.00      0.00      0.00   3320.80   3307.39
14:22:48   3391.72   3391.72      2.79      1.06      0.00      0.00      0.00      0.00   3394.52   3392.79
14:22:49   3327.35   3327.35      2.48      0.00      0.00      0.00      0.00      0.00   3329.84   3327.35
14:22:50   3361.18   3361.18      0.36      3.46      0.00      0.00      0.00      0.00   3361.54   3364.65
14:22:51   3350.74   3350.74      1.03      0.00      0.00      0.00      0.00      0.00   3351.77   3350.74
14:22:52   3349.38   3349.38      0.36      0.00      0.00      0.00      0.00      0.00   3349.74   3349.38
14:22:53   3382.90   3382.90      1.52      0.00      0.00      0.00      0.00      0.00   3384.42   3382.90
14:22:54   3309.98   3309.98      1.37      0.00      0.00      0.00      0.00      0.00   3311.35   3309.98
14:22:55   3382.49   3382.49      0.66      3.46      0.00      0.00      0.00      0.00   3383.14   3385.95
14:22:56   3329.62   3329.62      4.25      0.00      0.00      0.00      0.00      0.00   3333.86   3329.62
14:22:57   3359.20   3359.20      0.00      0.00      0.00      0.00      0.00      0.00   3359.20   3359.20
14:22:58   3320.09   3320.09      1.44      0.33      0.00      0.00      0.00      0.00   3321.53   3320.42
14:22:59   3352.83   3352.83      1.87      0.42      0.00      0.00      0.00      0.00   3354.70   3353.25
14:23:00   3356.91   3356.91      5.82      4.01      0.00      0.00      0.00      0.00   3362.73   3360.92
14:23:01   3330.76   3330.76      1.83      0.00      0.00      0.00      0.00      0.00   3332.59   3330.76
```

Рис. 6.13. Окно терминала с выводом команды `ifstat -n -T -b -a -t -w 1`

Команда `netstat -tup` отображает все установленные сетевые соединения по протоколам TCP и UDP без разрешения имен в IP-адреса, идентификаторы и имена процессов, обеспечивающих эти соединения. Если совместно с `netstat` использовать утилиты `watch` и `grep`, то можно получить очень полезный инструмент для контроля за сетевыми соединениями.

Вывод команды `watch --interval 1 netstat -a -n -t` приведен на рис. 6.14. Информация в окне терминала обновляется каждую секунду.

Добавив к этой команде "довесок" с конвейерным перенаправлением к утилите `grep`, выбирающей из всего потока данных участки с указанным фрагментом текста, можно отслеживать только интересующие нас события. Так команда `watch --interval 1 netstat -a -n -t | grep 192` выводит информацию о соединениях, в IP-адресах которых есть сочетание 192 (рис. 6.15).

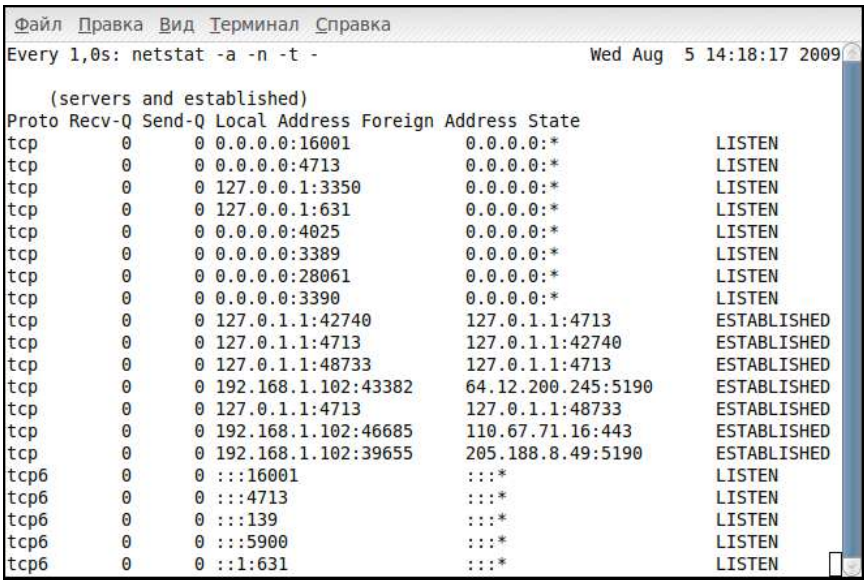


Рис. 6.14. Вывод команды `watch --interval 1 netstat -a -n -t`

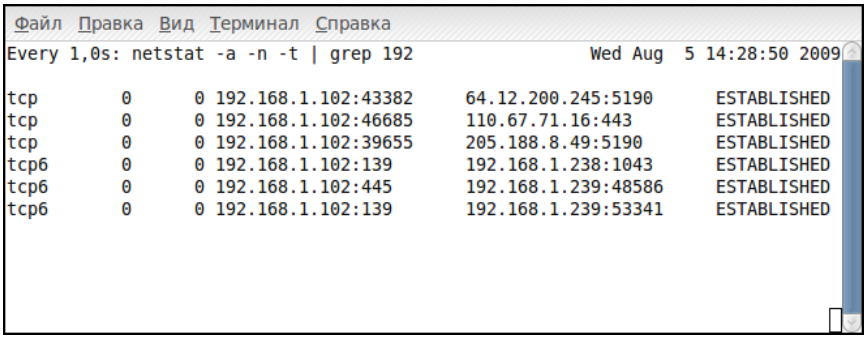


Рис. 6.15. Вывод команды `watch --interval 1 netstat -a -n -t | grep 192`

Заключение

Операционная система Linux развивается очень быстро. Появляются новые версии, которые постепенно становятся все более удобными, имеют в своих дистрибутивах множество полезных программ. Например, Linux Mint 7 (**http://www.linuxmint.com/**) содержит наиболее новые версии приложений, которые обычно требуются пользователю домашнего компьютера. Серверные версии Linux также не стоят на месте. Тысячи серверов в России работают под управлением Linux CentOS 5.3 (**http://www.centos.org/**), которая на сегодняшний день может быть отмечена как одна из самых стабильных версий. Многие пользователи Linux, для которых стабильность и надежность системы важны, используют CentOS на своих компьютерах.

В книге приведены примеры работы лишь с некоторыми версиями Linux. Но для начинающего пользователя, желающего использовать эту красивую и обычно бесплатную систему, этих сведений достаточно, чтобы начать осваивать Linux, применив в своей небольшой сети.

Отсутствие вирусов, надежность, наличие в дистрибутивах практически всех программ, которые могут понадобиться пользователю ПК, наличие бесплатных аналогов программ для Windows, возможность найти в Интернете информацию о работе с большинством версий Linux на русском языке делает Linux все более привлекательной.

Автор надеется, что вы, установив на своих компьютерах Linux, не захотите отказываться от него. А то, чего Linux еще не может, можно выполнить на виртуальной машине Windows, работающей в среде Linux и VMware Server. К счастью, ресурсов современных компьютеров достаточно, чтобы одновременно запускать две и более операционных систем.

Удачи вам!

Приложение

Здесь приведены наиболее употребительные команды Linux в виде примеров их выполнения с пояснениями к примерам. Таблица П1 может быть справочным руководством по командам, которые распределены по нескольким разделам. Дополнительную информацию о командах можно получить, введя команду без параметров или с параметром `-h`.

Таблица П1

Наиболее употребительные команды Linux		
Системная информация		
№	**Команда**	**Описание**
1	`arch`	Показать архитектуру машины (1)
2	`uname -m`	Показать архитектуру машины (2)
3	`uname -r`	Показать версию используемого ядра
4	`dmidecode -q`	Показать аппаратные компоненты системы (SMBIOS/DMI)
5	`hdparm -i /dev/hda`	Отобразить характеристики жесткого диска
6	`hdparm -tT /dev/sda`	Выполнить тест чтения жесткого диска
7	`cat /proc/cpuinfo`	Показать информацию о процессоре
8	`cat /proc/interrupts`	Показать прерывания
9	`cat /proc/meminfo`	Проверить использование памяти
10	`cat /proc/swaps`	Показать swap-файл(ы)
11	`cat /proc/version`	Показать версию ядра
12	`cat /proc/net/dev`	Показать сетевые адаптеры и статистику
13	`cat /proc/mounts`	Показать смонтированные файловые системы

Таблица П1 *(продолжение)*

Наиболее употребительные команды Linux		
Системная информация		
№	**Команда**	**Описание**
14	`lspci -tv`	Отобразить устройства PCI
15	`lsusb -tv`	Показать устройства USB
16	`date`	Показать системную дату
17	`cal 2008`	Показать календарь на 2008 год
18	`date 081219302008.15`	Установить дату и время — МесяцДеньЧасМинутыГод.Секунды
19	`clock -w`	Сохранить изменения даты в BIOS
Завершение работы, перезагрузка, завершение сеанса		
№	**Команда**	**Описание**
20	`shutdown -h now`	Завершить работу системы (1)
21	`shutdown -h hours:minutes &`	Запланировать завершение работы системы (выключение компьютера)
22	`shutdown -c`	Отменить запланированное завершение работы системы
23	`shutdown -r now`	Перезагрузить (1)
23	`reboot`	Перезагрузить (2)
25	`logout`	Завершение сеанса
Файлы и директории		
№	**Команда**	**Описание**
26	`cd /home`	Перейти в каталог /home
27	`cd ..`	Перейти в каталог на один уровень выше
28	`cd ../..`	Перейти в каталог на два уровня выше
29	`cd`	Перейти в домашний каталог
30	`cd ~user1`	Перейти в домашний каталог
31	`cd -`	Перейти в предыдущий каталог
32	`pwd`	Показать путь к рабочему каталогу
33	`ls`	Просмотр списка файлов в каталоге

Таблица П1 *(продолжение)*

Файлы и директории		
№	**Команда**	**Описание**
34	`ls -F`	Просмотр списка файлов в каталоге
35	`ls -l`	Показать детализированную информацию о файлах и каталогах (права доступа, время создания, владелец, размер)
36	`ls -a`	Показать скрытые файлы
37	`ls *[0-9]*`	Показать файлы и каталоги, имена которых содержат числа
38	`mkdir dir1`	Создать каталог с именем dir1
39	`mkdir dir1 dir2`	Создать два каталога одновременно
40	`mkdir -p /tmp/dir1/dir2`	Создать вложенные каталоги
41	`rm -f file1`	Удалить файл с именем file1
42	`rmdir dir1`	Удалить каталог с именем dir1
43	`rm -rf dir1`	Рекурсивно удалить каталог dir1 и его содержимое
44	`rm -rf dir1 dir2`	Рекурсивно удалить два каталога dir1 и dir2 и их содержимое
45	`mv dir1 new_dir`	Переименовать/переместить файл или каталог
46	`cp file1 file2`	Копировать файл
47	`cp dir/* .`	Копировать все файлы каталога в рабочий каталог
48	`cp -a /tmp/dir1 .`	Копировать каталог в рабочий каталог
49	`cp -a dir1 dir2`	Копировать каталог
50	`ln -s file1 lnk1`	Создать символьную ссылку на каталог или файл
51	`ln file1 lnk1`	Создать физическую ссылку на каталог или файл
52	`touch -t 0712250000 file1`	Изменить штамп времени файла или каталога (`YYMMDDhhmm`)
53	`file file1`	Выводить в виде текста информацию о типе файла
54	`iconv -l`	Выводить список известных кодировок

Таблица П1 *(продолжение)*

Файлы и директории		
№	**Команда**	**Описание**
55	`iconv -f fromEncoding -t toEncoding inputFile > outputFile`	Перекодирует файл `inputFile` из кодировки `fromEncoding` в кодировку `toEncoding`, создавая новый файл `outputFile`
56	`find . -maxdepth 1 -name *.jpg -print -exec convert "{}" -resize 80x60 "thumbs/{}" \;`	Пакет команд изменяет размеры графических файлов из текущего каталога и создает измененные копии (эскизы) в каталоге thumbs (требует наличия конвертора из Imagemagick)
Поиск файлов		
№	**Команда**	**Описание**
57	`find / -name file1`	Поиск файла или каталога в файловой системе, начиная с корневого каталога
58	`find / -user user1`	Поиск файлов или каталогов, принадлежащих пользователю user1
59	`find /home/user1 -name \*.bin`	Поиск файлов с расширением bin в каталоге /home/user1
60	`find /usr/bin -type f -atime +100`	Поиск бинарных файлов, не использовавшихся за прошедшие 100 дней
61	`find /usr/bin -type f -mtime -10`	Поиск файлов или каталогов, измененных за прошедшие 10 дней
62	`find / -name \*.rpm -exec chmod 755 '{}' \;`	Поиск файлов с расширением rpm и изменение прав доступа к ним
63	`find / -xdev -name \*.rpm`	Поиск файлов с расширением rpm только на жестких дисках. Сменные носители игнорируются
64	`locate \*.ps`	Поиск файлов с расширением ps (предварительно необходимо выполнить команду `updatedb`)
65	`whereis halt`	Показать местоположение бинарного исполняемого файла, содержащего руководства, относящиеся к файлу halt
66	`which halt`	Отображает полный путь к файлу halt

Таблица П1 *(продолжение)*

Монтирование файловых систем		
№	**Команда**	**Описание**
67	`mount /dev/hda2 /mnt/hda2`	Монтировать диск с именем hda2 с проверкой существования каталога /mnt/hda2
68	`umount /dev/hda2`	Монтировать диск с именем hda2. Необходим выход из точки монтирования mnt/hda2
69	`fuser -km /mnt/hda2`	Быстрое монтирование, когда устройство занято
70	`umount -n /mnt/hda2`	Выполнение `umount` без записи в файл /etc/mtab. Полезно, когда файл только для чтения или жесткий диск переполнен
71	`mount /dev/fd0 /mnt/floppy`	Монтировать гибкий диск
72	`mount /dev/cdrom /mnt/cdrom`	Монтировать CD или DVD
73	`mount /dev/hdc /mnt/cdrecorder`	Монтировать CD-R/CD-RW или DVD-R/DVD-RW(+-)
74	`mount -o loop file.iso /mnt/cdrom`	Монтировать файл ISO-образа диска
75	`mount -t vfat /dev/hda5 /mnt/hda5`	Монтировать файловую систему FAT32
76	`mount /dev/sda1 /mnt/usbdisk`	Монтировать USB флэш-диск
77	`mount -t smbfs -o username=user,password=pass //WinClient/share /mnt/share`	Монтировать ресурс сети Windows
78	`mount -o bind /home/user/prg /var/ftp/user`	Монтирует директорию в директорию (binding). Доступна с версии ядра 2.4.0. Полезна, например, для предоставления содержимого пользовательской директории через ftp. Выполнение данной команды сделает копию содержимого /home/user/prg в /var/ftp/user
Дисковое пространство		
№	**Команда**	**Описание**
79	`df -h`	Показать список примонтированных разделов
80	`ls -lSr | more`	Показать размер файлов и каталогов, упорядоченных по размеру
81	`du -sh dir1`	Оценить место, используемое каталогом dir1

Таблица П1 *(продолжение)*

Дисковое пространство		
№	**Команда**	**Описание**
82	`du -sk * | sort -rn`	Показать размер файлов и каталогов, отсортированных по размеру
83	`rpm -q -a --qf '%10{SIZE}t%{NAME}n' | sort -k1,1n`	Показать размер дискового пространства, используемого RPM-пакетами, с сортировкой по размеру (в системах Fedora, Red Hat и на их основе)
84	`dpkg-query -W -f='${Installed-Size;10}t${Package}n' | sort -k1,1n`	Показать место, используемое DEB-пакетами, установив сортировку по размеру (в системах Ubuntu, Debian и на их основе)
Пользователи и группы		
№	**Команда**	**Описание**
85	`groupadd group_name`	Создание новой группы
86	`groupdel group_name`	Удаление группы
87	`groupmod -n new_group_name old_group_name`	Переименование группы
88	`useradd -c "Name Surname " -g admin -d /home/user1 -s /bin/bash user1`	Создание нового пользователя, принадлежащего группе admin
89	`useradd user1`	Создание нового пользователя
90	`userdel -r user1`	Удаление пользователя (`-r` удаляет домашний каталог)
91	`usermod -c "User FTP" -g system -d /ftp/user1 -s /bin/nologin user1`	Изменить пользовательские атрибуты
92	`gpasswd –a (-d)userid group-name`	Добавить (удалить) члена группы. Используется числовой идентификатор пользователя
93	`passwd`	Сменить пароль
94	`passwd user1`	Изменить пользовательский пароль (доступно только администратору)
95	`chage -E 2005-12-31 user1`	Установить дату окончания действия учетной записи пользователя user1
96	`pwck`	Проверка синтаксиса и формата файла /etc/passwd, существования пользователей и их каталогов

Таблица П1 *(продолжение)*

Пользователи и группы		
№	**Команда**	**Описание**
97	`grpck`	Проверка синтаксиса и формата файла /etc/group, существования групп
98	`newgrp group_name`	Вход в новую группу, чтобы изменить группу по умолчанию для вновь создаваемых файлов
Права доступа к файлам		
№	**Команда**	**Описание**
99	`ls -lh`	Показать права доступа
100	`ls /tmp | pr -T5 -W$COLUMNS`	Вывод списка файлов и каталогов с разделением его в терминале на пять колонок

101	`chmod ugo+rwx directory1`
	или
	`chmod 777 directory1`
		Установка разрешений доступа на чтение (`r`), запись (`w`), исполнение (`x`) для пользователей владельцев (`u`), групп (`g`) и других (`o`)

102	`chmod go-rwx directory1`	Удалить разрешения доступа на чтение (`r`), запись (`w`), исполнение (`x`) для группы пользователей (`g`) и других (`o`)
103	`chown user1 file1`	Назначить владельцем файла пользователя user1
104	`chown -R user1 directory1`	Назначить владельцем каталога и всех файлов и каталогов, содержавшихся внутри, пользователя user1
105	`chgrp group1 file1`	Изменить группу-владельца файла
106	`chown user1:group1 file1`	Изменить владельца и группу владельца файла
107	`find / -perm -u+s`	Просмотреть все файлы в системе с установленным атрибутом SUID
108	`chmod u+s /bin/file1`	Установка атрибута SUID для бинарного файла, чтобы пользователь при его исполнении получил права владельца этого файла
109	`chmod u-s /bin/file1`	Снятие атрибута SUID, для бинарного файла
110	`chmod g+s /home/public`	Установка атрибута SGID для каталога (передаются права группы владельца)
111	`chmod g-s /home/public`	Снятие атрибута SGID для каталога

Таблица П1 *(продолжение)*

Права доступа к файлам		
№	**Команда**	**Описание**
112	`chmod o+t /home/public`	Установка атрибута STIKY для каталога — позволяет удаление файлов только законным владельцам
113	`chmod o-t /home/public`	Снятие атрибута STIKY для каталога
Специальные атрибуты файлов		
№	**Команда**	**Описание**
114	`chattr +a file1`	Разрешает запись в файл только в режиме добавления
115	`chattr +c file1`	Разрешает сжатие и распаковку файла автоматически ядром
116	`chattr +d file1`	Указывает утилите dump игнорировать данный файл во время выполнения резервного копирования
117	`chattr +i file1`	Этот атрибут делает невозможным удаление, изменение, переименование или связывание (создание ссылки)
118	`chattr +S file1`	Указывает, что при сохранении изменений будет произведена синхронизация, как при выполнении команды `sync`
119	`chattr +s file1`	Разрешает безопасное удаление файла, место, занимаемое файлом на диске, заполняется нулями, что предотвращает возможность восстановления данных
120	`chattr +u file1`	Позволяет восстанавливать содержание файла, даже если файл будет удален
121	`lsattr`	Показать специальные атрибуты
Архивирование и сжатие файлов		
№	**Команда**	**Описание**
122	`bunzip2 file1.bz2`	Распаковать файл file1.bz2
123	`bzip2 file1`	Сжать файл file1
124	`gunzip file1.gz`	Распаковать файл file1.gz
125	`gzip file1`	Сжать файл file1

Таблица П1 *(продолжение)*

Архивирование и сжатие файлов		
№	**Команда**	**Описание**
126	`gzip -9 file1`	Архивирование с максимальным сжатием
127	`rar a file1.rar test_file`	Создать rar-архив file1.rar
128	`rar a file1.rar file1 file2 dir1`	Сжать file1, file2 и dir1 одновременно
129	`rar x file1.rar`	Создать архив rar
130	`unrar x file1.rar`	Распаковать архив rar
131	`tar -cvf archive.tar file1`	Создать несжатый tarball
132	`tar -cvf archive.tar file1 file2 dir1`	Создать архив, содержащий file1, file2 и dir1
133	`tar -tf archive.tar`	Показать содержание архива
134	`tar -xvf archive.tar`	Извлечение tarball
135	`tar -xvf archive.tar -C /tmp`	Извлечение tarball в /tmp
136	`tar -cvfj archive.tar.bz2 dir1`	Создать tarball, сжатый в bzip2
137	`tar -xvfj archive.tar.bz2`	Распаковать архив tar, сжатый в bzip2
138	`tar -cvfz archive.tar.gz dir1`	Создать tarball, сжатый в gzip
139	`tar -xvfz archive.tar.gz`	Декомпрессируйте сжатый архив tar в gzip
140	`zip file1.zip file1`	Создать архив, сжатый в zip
141	`zip -r file1.zip file1 file2 dir1`	Сжатие в zip одновременно нескольких файлов
142	`unzip file1.zip`	Распаковать архив zip
RPM-пакеты (установка и удаление программ)		
№	**Команда**	**Описание**
143	`rpm -ivh package.rpm`	Установить пакет rpm
144	`rpm -ivh --nodeeps package.rpm`	Установить пакет rpm, но игнорировать зависимости
145	`rpm -U package.rpm`	Обновить пакет rpm, не изменяя файлы конфигурации

Таблица П1 *(продолжение)*

RPM-пакеты (установка и удаление программ)		
№	**Команда**	**Описание**
146	`rpm -F package.rpm`	Обновить пакет rpm, если он уже установлен
147	`rpm -e package_name.rpm`	Удалить пакет rpm
148	`rpm -qa`	Показать все пакеты rpm, установленные в системе
149	`rpm -qa | grep httpd`	Показать все пакеты rpm с именем httpd
150	`rpm -qi package_name`	Получить информацию об установленном пакете
151	`rpm -qg "System Environment/Daemons"`	Показать пакеты rpm определенной группы приложений
152	`rpm -ql package_name`	Показать список файлов, созданных установленным пакетом rpm
153	`rpm -qc package_name`	Показать список файлов конфигурации, созданных установленным пакетом rpm
154	`rpm -q package_name --whatrequires`	Показать список зависимостей, требуемых для пакета rpm
155	`rpm -q package_name --whatprovides`	Показать совместимость пакета rpm
156	`rpm -q package_name --scripts`	Показать сценарии, запущенные при инсталляции/удалении пакета
157	`rpm -q package_name --changelog`	История просмотров пакета
158	`rpm -qf /etc/httpd/conf/httpd.conf`	Проверить, какой пакет rpm принадлежит данному файлу
159	`rpm -qp package.rpm -l`	Показать список файлов, создаваемых пакетом rpm, если он еще не установлен
160	`rpm --import /media/cdrom/RPM-GPG-KEY`	Импортировать публичный ключ цифровой подписи
161	`rpm --checksig package.rpm`	Проверить целостность пакета rpm
162	`rpm -qa gpg-pubkey`	Проверить целостность всех установленных пакетов rpm
163	`rpm -V package_name`	Проверить размер файла, разрешения, тип, владельца, группу, контрольную сумму MD5 и последнюю модификацию

Таблица П1 *(продолжение)*

RPM-пакеты (установка и удаление программ)		
№	**Команда**	**Описание**
164	`rpm -Va`	Проверить все пакеты rpm, установленные в системе. Использовать с предостережением
165	`rpm -Vp package.rpm`	Проверить пакет rpm, еще не установленный
166	`rpm2cpio package.rpm | cpio --extract --make-directories *bin*`	Извлечь исполняемый файл из пакета rpm
167	`rpm -ivh /usr/src/redhat/RPMS/ `arch`/package.rpm`	Установить пакет, построенный из исходника rpm
168	`Rpmbuild --rebuild package_name.src.rpm`	Создать пакет rpm из исходника rpm
YUM-пакеты (установка и удаление программ)		
№	**Команда**	**Описание**
169	`yum install package_name`	Загрузить и установить пакет
170	`yum localinstall package_name.rpm`	Установка пакета с попыткой разрешения зависимостей
171	`yum update package_name.rpm`	Обновить все пакеты, установленные в системе
172	`yum update package_name`	Обновить пакет
173	`yum remove package_name`	Удалить пакет
174	`yum list`	Показать список всех пакетов, установленных в системе
175	`yum search package_name`	Найти пакет rpm в репозитории
176	`yum clean packages`	Очистить кэш удаления загруженных пакетов rpm
177	`yum clean headers`	Удалить все заголовочные файлы, которые система использовала для разрешения зависимостей
178	`yum clean all`	Удалить из кэша информацию о пакетах и заголовочных файлах

Таблица П1 *(продолжение)*

Deb-пакеты (установка и удаление программ)		
№	**Команда**	**Описание**
179	`dpkg -i package.deb`	Установка/обновление deb-пакетов
180	`dpkg -r package_name`	Удаление deb-пакетов
181	`dpkg -l`	Показать все deb-пакеты, установленные в системе
182	`dpkg -l | grep httpd`	Показать все deb-пакеты, установленные в системе с именем "httpd"
183	`dpkg -s package_name`	Получить информацию относительно определенного пакета, установленного в системе
184	`dpkg -L package_name`	Показать список файлов, принадлежащих пакету, установленных в системе
185	`dpkg --contents package.deb`	Показать список файлов, принадлежащих установленному пакету
186	`dpkg -S /bin/ping`	Проверить, какой пакет принадлежит данному файлу
187	`apt-get install package_name`	Установить / обновить пакет
188	`apt-cdrom install package_name`	Установить / обновить пакет с CD-ROM
189	`apt-get update`	Обновить список пакетов
190	`apt-get upgrade`	Обновить все установленные пакеты
191	`apt-get remove package_name`	Удалить пакет из системы
192	`apt-get check`	Проверить зависимости
193	`apt-get clean`	Очистить кэш от загруженных пакетов
194	`apt-cache search searched-package`	Получить список пакетов, содержащих строку "searched-packages"
Работа с текстом		
№	**Команда**	**Описание**
195	`cat file1`	Показать содержимое текстового файла (на стандартном устройстве вывода)
196	`tac file1`	Показать содержимое текстового файла в обратном порядке (на стандартном устройстве вывода)

Таблица П1 *(продолжение)*

Работа с текстом		
№	**Команда**	**Описание**
197	`cat file1 | command( sed, grep, awk, grep, etc...) > result.txt`	Работа с текстом в файле и запись результата в новый файл
198	`cat file1 | command( sed, grep, awk, grep, etc...) >> result.txt`	Работа с текстом в файле, результат добавляется в существующий файл
199	`more file1`	Постраничный вывод содержимого файла file1 на стандартное устройство вывода
200	`less file1`	Постраничный вывод содержимого файла file1 на стандартное устройство вывода, но с возможностью пролистывания в обе стороны (вверх-вниз), поиска по содержимому и т. п.
201	`head -2 file1`	Вывести первые две строки файла file1 на стандартное устройство вывода. По умолчанию выводится десять строк
202	`tail -2 file1`	Вывести последние две строки файла file1 на стандартное устройство вывода. По умолчанию выводится десять строк
203	`tail -f /var/log/messages`	Выводить содержимое файла /var/log/messages на стандартное устройство вывода по мере появления в нем текста
204	`grep Aug /var/log/messages`	Поиск слова "Aug" в файле /var/log/messages
205	`grep ^Aug /var/log/messages`	Поиск слов, которые начинаются с "Aug", в файле /var/log/messages
206	`grep [0-9] /var/log/messages`	Выбрать из файла /var/log/messages все строки, которые содержат числа
207	`grep Aug -R /var/log/*`	Искать строку "Aug" в файлах каталога /var/log и вложенных каталогах
208	`sed 's/stringa1/ stringa2/g' example.txt`	Заменить строку "string1" на "string2" в файле example.txt
209	`sed '/^$/d' example.txt`	Удалить все пустые строки из файла example.txt
210	`sed '/ *#/d; /^$/d' example.txt`	Удалить комментарии и пустые строки в файле example.txt
211	`echo 'esempio' | tr '[:lower:]' '[:upper:]'`	Конвертировать текст из строчных букв в прописные

Таблица П1 *(продолжение)*

Работа с текстом		
№	**Команда**	**Описание**
212	`sed -e '1d' example.txt`	Удалить первую строку из файла example.txt
213	`sed -n '/string1/p'`	Просмотр строк, которые содержат слово "string1"
214	`sed -e 's/ *$//' example.txt`	Удалить пустые символы в конце каждой строки
215	`sed -e 's/stringa1//g' example.txt`	Удалить из текста слово "string1", оставив остальной текст неизменным
216	`sed -n '1,5p;5q' example.txt`	Просмотр от первой до пятой строки
217	`sed -n '5p;5q' example.txt`	Просмотр пятой строки
218	`sed -e 's/00*/0/g' example.txt`	Заменить несколько нолей единственным нолем
219	`cat -n file1`	Пронумеровать строки при выводе содержимого файла
220	`cat example.txt | awk 'NR%2==1'`	При выводе содержимого файла, не выводить четные строки файла
221	`echo a b c | awk '{print $1}'`	Вывести первую колонку. Разделение по умолчанию, по пробелу/пробелам или символу/символам табуляции
222	`echo a b c | awk '{print $1,$3}'`	Вывести первую и третью колонки. Разделение по умолчанию, по пробелу/пробелам или символу/символам табуляции
223	`paste file1 file2`	Объединить содержимое file1 и file2 в виде таблицы: строка 1 из file1 = строка 1 колонка (1 – n), строка 1 из file2 = строка 1 колонка (n+1 – m)
224	`paste -d '+' file1 file2`	Объединить содержимое file1 и file2 в виде таблицы с разделителем "+"
225	`sort file1 file2`	Отсортировать содержимое двух файлов
226	`sort file1 file2 | uniq`	Отсортировать содержимое двух файлов, не отображая повторов
227	`sort file1 file2 | uniq -u`	Отсортировать содержимое двух файлов, отображая только уникальные строки (строки, встречающиеся в обоих файлах, не выводятся на стандартное устройство вывода)

Таблица П1 *(продолжение)*

Работа с текстом		
№	**Команда**	**Описание**
228	`sort file1 file2 | uniq -d`	Отсортировать содержимое двух файлов, отображая только повторяющиеся строки
229	`comm -1 file1 file2`	Сравнить содержимое двух файлов, не отображая строки, принадлежащие файлу file1
230	`comm -2 file1 file2`	Сравнить содержимое двух файлов, не отображая строки, принадлежащие файлу file2
231	`comm -3 file1 file2`	Сравнить содержимое двух файлов, удаляя строки, встречающиеся в обоих файлах
Преобразование кодировок и форматов файлов		
№	**Команда**	**Описание**
232	`dos2unix filedos.txt fileunix.txt`	Конвертировать файл текстового формата MS-DOS в UNIX (отличие в символах возврата каретки)
233	`unix2dos fileunix.txt filedos.txt`	Конвертировать файл текстового формата из UNIX в MS-DOS (отличие в символах возврата каретки)
234	`recode ..HTML < page.txt > page.html`	Конвертировать содержимое текстового файла page.txt в HTML-файл page.html
235	`recode -l | more` *или* `iconv -l | more`	Вывести список доступных форматов
Сеть (LAN и WiFi)		
№	**Команда**	**Описание**
236	`ifconfig eth0`	Показать конфигурацию сетевого интерфейса eth0
237	`ifup eth0`	Активировать (поднять) интерфейс eth0
238	`ifdown eth0`	Деактивировать (опустить) интерфейс eth0
239	`ifconfig eth0 192.168.1.1 netmask 255.255.255.0`	Выставить интерфейсу eth0 IP-адрес и маску подсети
240	`ifconfig eth0 promisc`	Перевести интерфейс eth0 в promiscuous-режим для "отлова" пакетов (sniffing)
241	`ifconfig eth0 -promisc`	Отключить promiscuous-режим на интерфейсе eth0

Таблица П1 *(продолжение)*

Сеть (LAN и WiFi)		
№	**Команда**	**Описание**
242	`dhclient eth0`	Активировать интерфейс eth0 в DHCP-режиме
243	`route -n`	Вывести локальную таблицу маршрутизации
244	`netstat -rn`	Вывести локальную таблицу маршрутизации
245	`route add -net 0/0 gw IP_Gateway`	Задать IP-адрес шлюза по умолчанию (default gateway)
246	`route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1`	Добавить статический маршрут в сеть 192.168.0.0/16 через шлюз с IP-адресом 192.168.1.1
247	`route del 0/0 gw IP_gateway`	Удалить IP-адрес шлюза по умолчанию (default gateway)
248	`echo "1" > /proc/sys/net/ipv4/ip_forward`	Разрешить пересылку пакетов (forwarding)
249	`hostname`	Отобразить имя компьютера
250	`host www.example.com`	Разрешить имя хоста в IP-адрес и наоборот (1)
251	`nslookup www.example.com`	Разрешить имя хоста в IP-адрес и наоборот (2)
252	`ip link show`	Отобразить состояние всех интерфейсов
253	`mii-tool eth0`	Отобразить статус и тип соединения для интерфейса eth0
254	`ethtool eth0`	Отображает статистику интерфейса eth0 с выводом такой информации, как поддерживаемые и текущие режимы соединения
255	`netstat -tup`	Отображает все установленные сетевые соединения по протоколам TCP и UDP без разрешения имен в IP-адреса и PID и имена процессов, обеспечивающих эти соединения
256	`netstat -tupl`	Отображает все сетевые соединения по протоколам TCP и UDP без разрешения имен в IP-адреса и PID и имена процессов, слушающих порты
257	`tcpdump tcp port 80`	Отобразить весь трафик на TCP-порт 80 (обычно HTTP)
258	`iwlist scan`	Просканировать эфир на предмет доступности беспроводных точек доступа

Таблица П1 *(продолжение)*

Сеть (LAN и WiFi)		
№	**Команда**	**Описание**
259	`iwconfig eth1`	Показать конфигурацию беспроводного сетевого интерфейса eth1
260	`whois www.example.com`	Поиск в базе данных системы Whois
Сеть Microsoft (Samba)		
№	**Команда**	**Описание**
261	`nbtscan ip_addr`	Разрешить IP-адрес в NetBIOS-имя
262	`nmblookup -A ip_addr`	Разрешить IP-адрес в NetBIOS-имя
263	`smbclient -L ip_addr/hostname`	Показать удаленный ресурс Windows-машины
264	`smbget -Rr smb://ip_addr/share`	Загрузка файлов с удаленной Windows-машины через smb
265	`mount -t smbfs (cifs) -o username=user,password=pass //WinClient/share /mnt/share`	Монтировать удаленный ресурс сети Windows
iptables (firewall)		
№	**Команда**	**Описание**
266	`iptables -t filter -L`	Отобразить все цепочки правил в filter-таблице
267	`iptables -t nat -L`	Отобразить все цепочки правил в NAT-таблице
268	`iptables -t filter -F`	Очистить все цепочки правил в filter-таблице
269	`iptables -t nat -F`	Очистить все цепочки правил в NAT-таблице
270	`iptables -t filter -X`	Удалить любые цепочки, созданные пользователем
271	`iptables -t filter -A INPUT -p tcp --dport telnet -j ACCEPT`	Разрешить входящее подключение Telnet
272	`iptables -t filter -A OUTPUT -p tcp --dport http -j DROP`	Блокировать исходящие HTTP-соединения
273	`iptables -t filter -A FORWARD -p tcp --dport pop3 -j ACCEPT`	Позволить "прокидывать" (forward) POP3-соединения

Таблица П1 *(продолжение)*

iptables (firewall)		
№	**Команда**	**Описание**
274	`iptables -t filter -A INPUT -j LOG --log-prefix "DROP INPUT"`	Включить журналирование ядром пакетов, проходящих через цепочку INPUT, и добавлением к сообщению префикса "DROP INPUT"
275	`iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`	Включить NAT (Network Address Translate) исходящих пакетов на интерфейс eth0. Допустимо при использовании с динамически выделяемыми IP-адресами
276	`iptables -t nat -A PREROUTING -d 192.168.0.1 -p tcp -m tcp --dport 22 -j DNAT --to-destination 10.0.0.2:22`	Переадресовать пакеты, адресованные хостом другому хосту
277	`# modprobe iptable_nat # iptables -t nat -A POSTROUTING -o eth2 -j MASQUARADE # /proc/sys/net/ipv4/ip_forward`	Включить NAT (Network Address Translate) исходящих пакетов на интерфейс eth2. И разрешить пересылку пакетов (CentOS)
Сеть Novell Netware		
№	**Команда**	**Описание**
278	`# ipx_configure --auto_interface=on — auto_primary=on # ipx_interface add -p eth0 802.2I 777`	Настройка IPX (можно указать в файле etc/init.d/rc (SUSE11))
Анализ файловых систем		
№	**Команда**	**Описание**
279	`badblocks -v /dev/hda1`	Проверить раздел hda1 на наличие bad-блоков
280	`fsck /dev/hda1`	Проверить/восстановить целостность файловой системы Linux раздела hda1
281	`fsck.ext2 /dev/hda1`	Проверить/восстановить целостность файловой системы ext2 раздела hda1
282	`e2fsck /dev/hda1`	Проверить/восстановить целостность файловой системы ext3 раздела hda1

Таблица П1 *(продолжение)*

Анализ файловых систем		
№	**Команда**	**Описание**
283	`e2fsck -j /dev/hda1`	Проверить/восстановить целостность файловой системы ext3 раздела hda1 с указанием, что журнал расположен там же
284	`fsck.ext3 /dev/hda1`	Проверить/восстановить целостность файловой системы ext3 раздела hda1
285	`fsck.vfat /dev/hda1`	Проверить/восстановить целостность файловой системы FAT раздела hda1
286	`fsck.msdos /dev/hda1`	Проверить/восстановить целостность файловой системы FAT раздела hda1
287	`dosfsck /dev/hda1`	Проверить/восстановить целостность файловой системы FAT раздела hda1
Форматирование файловых систем		
№	**Команда**	**Описание**
288	`mkfs /dev/hda1`	Создать файловую систему Linux на разделе hda1
289	`mke2fs /dev/hda1`	Создать файловую систему ext2 на разделе hda1
290	`mke2fs -j /dev/hda1`	Создать журналирующую файловую систему ext3 на разделе hda1
291	`mkfs -t vfat 32 -F /dev/hda1`	Создать файловую систему FAT32 на разделе hda1
292	`fdformat -n /dev/fd0`	Форматирование флоппи-диска без проверки
293	`mkswap /dev/hda3`	Создание swap-пространства на разделе hda3
294	`swapon /dev/hda3`	Активировать swap-пространство, расположенное на разделе hda3
295	`swapon /dev/hda2 /dev/hdb3`	Активировать swap-пространства, расположенные на разделах hda2 и hdb3
Резервное копирование		
№	**Команда**	**Описание**
296	`dump -0aj -f /tmp/home0.bak /home`	Создать полную резервную копию каталога /home в файл /tmp/home0.bak
297	`dump -1aj -f /tmp/home0.bak /home`	Создать инкрементальную резервную копию каталога /home в файл /tmp/home0.bak

Таблица П1 *(продолжение)*

Резервное копирование		
№	**Команда**	**Описание**
298	`restore -if /tmp/home0.bak`	Восстановить из резервной копии /tmp/home0.bak в интерактивном режиме
299	`rsync -rogpav --delete /home /tmp`	Синхронизация между каталогами /home и /tmp
300	`rsync -rogpav -e ssh --delete /home ip_address:/tmp`	Синхронизировать через SSH-туннель
301	`rsync -az -e ssh --delete ip_addr:/home/public /home/local`	Синхронизировать локальный каталог с отдаленным каталогом через SSH со сжатием
302	`rsync -az -e ssh --delete /home/local ip_addr:/home/public`	Синхронизировать отдаленный каталог с локальным каталогом через SSH со сжатием
303	`dd bs=1M if=/dev/hda | gzip | ssh user@ip_addr 'dd of=hda.gz'`	Создать резервную копию локального жесткого диска на удаленном компьютере через SSH
304	`dd if=/dev/sda of=/tmp/file1`	Резервная копия содержания жесткого диска в файл
305	`tar -Puf backup.tar /home/user`	Создать инкрементальную резервную копию каталога /home/user в файл backup.tar с сохранением полномочий
306	`( cd /tmp/local/ && tar c . ) | ssh -C user@ip_addr 'cd /home/share/ && tar x -p'`	Копирование содержимого /tmp/local на удаленный компьютер через SSH-туннель в /home/share/
307	`( tar c /home ) | ssh -C user@ip_addr 'cd /home/backup-home && tar x -p'`	Копирование содержимого /home на удаленный компьютер через SSH-туннель в /home/backup-home
308	`tar cf - . | (cd /tmp/backup ; tar xf - )`	Копирование одного каталога в другой с сохранением полномочий и ссылок
309	`find /home/user1 -name '*.txt' | xargs cp -av --target-directory=/home/backup/ --parents`	Поиск в /home/user1 всех файлов с расширением txt и копирование их в другой каталог

Таблица П1 *(продолжение)*

Резервное копирование		
№	**Команда**	**Описание**
310	`find /var/log -name '*.log' | tar cv --files-from=- | bzip2 > log.tar.bz2`	Поиск в /var/log всех файлов с расширением log и создание bzip-архива из них
311	`dd if=/dev/hda of=/dev/fd0 bs=512 count=1`	Создать копию MBR (Master Boot Record) с /dev/hda на дискету
312	`dd if=/dev/fd0 of=/dev/hda bs=512 count=1`	Восстановить MBR из резервной копии, сохраненной на дискету
CD-ROM, DVD-ROM		
№	**Команда**	**Описание**
313	`cdrecord -v gracetime=2 dev=/dev/cdrom -eject blank=fast -force`	Очистить перезаписываемый CD-ROM
314	`mkisofs /dev/cdrom > cd.iso`	Создать ISO-образ диска в файле cd.iso
315	`mkisofs /dev/cdrom | gzip > cd_iso.gz`	Создать сжатый ISO-образ диска в файле cd_iso.gz
316	`mkisofs -J -allow-leading-dots -R -V "Label CD" -iso-level 4 -o ./cd.iso data_cd`	Создать ISO-образ каталога
317	`cdrecord -v dev=/dev/cdrom cd.iso`	Записать ISO-образ на диск
318	`gzip -dc cd_iso.gz | cdrecord dev=/dev/cdrom -`	Записать сжатый ISO-образ на диск
319	`mount -o loop cd.iso /mnt/iso`	Монтировать ISO-образ
320	`cd-paranoia -B`	Записать треки аудиодиска в WAV-файлы
321	`cd-paranoia -- "-3"`	Записать первые три трека аудиодиска в WAV-файлы
322	`cdrecord --scanbus`	Просканировать CD-рекордер на наличие канала SCSI
323	`dd if=/dev/hdc | md5sum`	Выполнить md5sum для диска

Таблица П1 *(продолжение)*

Мониторинг и отладка		
№	**Команда**	**Описание**
324	`top`	Отобразить запущенные процессы, используемые ими ресурсы и другую полезную информацию (с автоматическим обновлением данных)
325	`ps -eafw`	Отобразить запущенные процессы, используемые ими ресурсы и другую полезную информацию (единожды)
326	`ps -e -o pid,args --forest`	Вывести PID и процессы в виде дерева
327	`Pstree`	Отобразить дерево процессов
328	`kill -9 98989`	Остановить процесс с PID 98989 без соблюдения целостности данных
329	`kill -KILL 98989`	Остановить процесс с PID 98989 без соблюдения целостности данных
330	`kill -TERM 98989`	Корректно завершить процесс с PID 98989
331	`kill -1 98989`	Заставить процесс с PID 98989 перечитать файл конфигурации
332	`kill -HUP 98989`	Заставить процесс с PID 98989 перечитать файл конфигурации
333	`pstree`	Отобразить дерево процессов
334	`lsof -p $$`	Отобразить список файлов, открытых процессами
335	`lsof /home/user1`	Отобразить список открытых файлов из каталога/home/user1
336	`strace -c ls >/dev/null`	Вывести список системных вызовов, созданных и полученных процессом ls
337	`strace -f -e open ls >/dev/null`	Вывести вызовы библиотек
338	`watch -n1 'cat /proc/interrupts'`	Отобразить прерывания в режиме реального времени
339	`last reboot`	Отобразить историю перезагрузок системы
340	`last user1`	Отобразить историю регистрации пользователя user1 в системе и время его нахождения в ней
341	`lsmod`	Вывести загруженные модули ядра

Таблица П1 *(продолжение)*

Мониторинг и отладка		
№	**Команда**	**Описание**
342	`free -m`	Показать состояние оперативной памяти в мегабайтах
343	`smartctl -A /dev/hda`	Контроль состояния жесткого диска /dev/hda через SMART
344	`smartctl -i /dev/hda`	Проверить доступность SMART на жестком диске /dev/hda
345	`tail /var/log/dmesg`	Вывести десять последних записей из журнала загрузки ядра
346	`tail /var/log/messages`	Вывести десять последних записей из системного журнала
347	`apropos ...keyword`	Выводит список команд, которые так или иначе относятся к ключевым словам. Полезно, когда вы знаете, что делает программа, но не помните команду
348	`man ping`	Вызов руководства по работе с программой, в данном случае — `ping`
349	`whatis ...keyword`	Отображает описание действий указанной программы
350	`mkbootdisk --device /dev/fd0 'uname -r'`	Создает загрузочный флоппи-диск
351	`gpg -c file1`	Шифрует файл file1 с помощью GNU Privacy Guard
352	`gpg file1.gpg`	Дешифрует файл file1 с помощью GNU Privacy Guard
353	`wget -r www.example.com`	Загружает рекурсивно содержимое сайта www.example.com
354	`wget -c www.example.com/file.iso`	Загрузите файл с возможностью остановить загрузку и возобновить позже
355	`echo 'wget -c www.example.com/files.iso' | at 09:00`	Начать загрузку в указанное данное время
356	`ldd /usr/bin/ssh`	Вывести список библиотек, необходимых для работы SSH
357	`alias hh='history'`	Назначить алиас (псевдоним) hh-команде `history`

Таблица П1 *(продолжение)*

Мониторинг и отладка		
№	**Команда**	**Описание**
358	`chsh`	Изменить командную оболочку (сменить shell)
359	`chsh --list-shells`	Показать удаленные подключения
360	`who -a`	Просмотр информации о текущем пользователе, времени последней загрузки системы и др.
361	`startx`	Запуск видеосистемы (xserver)
362	`Pidof <имя_программы>`	Определить идентификатор (PID) по имени программы
Команды через сочетания клавиш		
№	**Команда**	**Описание**
363	<Ctrl>+<a>	Переход к началу строки
364	<Ctrl>+<b>	Аналог стрелки влево (например, если она не работает)
365	<Ctrl>+<c>	Отменить редактирование команды или прекратить работу (если запущена)
366	<Ctrl>+<d>	Аналог <Delete>. Если строка пустая — выход из текущего терминала
367	<Ctrl>+<e>	Переход к концу строки
368	<Ctrl>+<f>	Аналог стрелки вправо
369	<Ctrl>+<g>	Выход из режима дополнения
370	<Ctrl>+<h>	Аналог <BackSpace>
371	<Ctrl>+<i>	Аналог <Tab>
372	<Ctrl>+<k>	Удалить все до конца строки
373	<Ctrl>+<l>	Очистить экран (набранная строка и даже позиция курсора остается)
374	<Ctrl>+<r>	Поиск по истории набранных команд назад
375	<Ctrl>+<s>	Остановка вывода на терминал
376	<Ctrl>+<t>	Поменять местами текущий символ с предыдущим
377	<Ctrl>+<u>	Удалить все до начала строки
378	<Ctrl>+<v>	Преобразует следующую клавишу в ее символьное отображение (<Enter> — "^M", <Esc> — "^[" и т. д.)

Таблица П1 *(продолжение)*

Команды через сочетания клавиш		
№	**Команда**	**Описание**
379	<Ctrl>+<w>	Удалить от курсора до начала слова
380	<Ctrl>+<x> дважды	Скачок между началом строки и текущей позицией курсора
381	<Ctrl>+<x>	Выход из консольных текстовых редакторов
382	<Ctrl>+<y>	Вставить из буфера
383	<Ctrl>+<z>	Притормозить/остановить выполнение команды в фон
384	<Ctrl>+<_>	Отмена последнего изменения
385	<Alt>+< **<** >	К первой команде в истории (вообще к самой первой в .bash_history)
386	<Alt>+< **>** >	К последней команде в истории
387	<Alt>+<?>	Показать весь список вариантов дополнения (аналог 2T, см. ниже)
388	<Alt>+<*>	Вставить все возможные варианты дополнения
389	<Alt>+</>	Попытаться дополнить имя файла (из имеющихся в текущем каталоге)
390	<Alt>+<.>	Вставить последний аргумент из предыдущей команды
391	<Alt>+<b>	Влево на слово
392	<Alt>+<c>	Сделать первую букву слова заглавной (и перейти к следующему слову)
393	<Alt>+<d>	Удалить от текущей позиции до конца слова
394	<Alt>+<f>	Вправо на слово
395	<Alt>+<l>	Сделать первую букву слова строчной (и перейти к следующему слову)
396	<Alt>+<n>	Искать по истории (но не сразу, а после полного ввода и нажатия <Enter>)
397	<Alt>+<p>	Искать по истории назад
398	<Alt>+<r>	Очистить всю строку
399	<Alt>+<t>	Поменять слова местами
400	<Alt>+<u>	Сделать все буквы заглавными от текущей позиции до конца слова

Таблица П1 *(окончание)*

Команды через сочетания клавиш		
№	**Команда**	**Описание**
401	<Alt>+<BackSpace>	Удалить от текущей позиции до начала слова
402	<Esc>+<d>	Удалить от курсора до конца слова
403	<Esc>+<f>	Вправо на слово
404	<Esc>+<b>	Влево на слово
405	<Esc>+<t>	Поменять местами слова
406	2T	2T обозначает дважды нажатый <Tab>
407	2T	Все доступные команды
408	(string)2T	Все доступные команды, начинающиеся на string
409	/2T	Все каталоги, включая скрытые. Для текущего надо набрать ./2T
410	*2T	Каталоги, кроме скрытых
411	~2T	Все пользователи, присутствующие в /etc/passwd
412	~f2T	Все пользователи, присутствующие в /etc/passwd, начинающиеся на f
413	$2T	Все системные переменные
414	@2T	Все записи в /etc/hosts
415	=2T	Вывод наподобие ls или dir
416	!!	Выполнить последнюю команду в истории
417	!abc	Выполнить последнюю команду в истории, начинающуюся на abc
418	!a:p	Напечатать последнюю команду в истории, начинающуюся на a
419	!n	Выполнить *n*-ную команду в истории
420	!$	Последний аргумент последней команды
421	!^	Первый аргумент последней команды
422	^abc^xyz	Заменить abc на xyz в последней команде и выполнить результат

Предметный указатель