

Д. КОЛИСНИЧЕНКО

# САМОУЧИТЕЛЬ системного администратора Linux

Дистрибутивы Fedora 13, Mandriva  
2010.1 Spring, openSUSE 11.3,  
Ubuntu 10

Установка и настройка  
операционной системы

Подробное рассмотрение файловой  
системы Linux

Настройка сети и маршрутизации  
без конфигураторов

Брандмауэры iptables и ebtables,  
chroot-окружение

Настройка серверов: Web, FTP, DNS,  
DHCP, почтового и сервера баз данных

Прокси-серверы Squid и SquidGuard

Linux-сервер в Windows-сети: свой  
среди чужих

Виртуальные частные сети (VPN)

Создание LiveCD

Сетевой сканер nmap

Система управления доступом Tomsy

Защита и оптимизация Linux-сервера

Автоматизация задач с помощью bash

Программные RAID-массивы

СИСТЕМНЫЙ  
АДМИНИСТРАТОР

УДК 681.3.06  
ББК 32.973.26-018.2  
К60

**Колисниченко Д. Н.**

К60 Самоучитель системного администратора Linux. — СПб.: БХВ-Петербург, 2011. — 544 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0639-7

Описаны основы сетевого взаимодействия, планирование и монтаж сети (Ethernet и Wi-Fi), настройка сети и маршрутизации без конфигураторов. Даны примеры настройки различных типов серверов: Web, FTP, DNS, DHCP, почтового сервера, сервера баз данных. Рассмотрены дистрибутивы Fedora 13, Mandriva 2010.1 Spring, openSUSE 11.3, Ubuntu 10, файловая система Linux, установка и базовая настройка Linux, а также связки Apache + MySQL + PHP. Особое внимание уделено защите сетевых сервисов и оптимизации работы сервера: использованию брандмауэров iptables и ebtables, прокси-серверов Squid и SquidGuard, созданию chroot-окружения, управлению доступом с помощью системы Tomoyo, настройке VPN-сервера, аудиту сети при помощи сетевого сканера nmap. Приведены практические рекомендации по стратегии администрирования и уходу за аппаратными средствами, работе Linux-сервера в Windows-сети, созданию LiveCD, автоматизации задач с помощью bash, использованию программных RAID-массивов.

*Для администраторов Linux*

УДК 681.3.06  
ББК 32.973.26-018.2

#### **Группа подготовки издания:**

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Григорий Добин</i>
Компьютерная верстка	<i>Натальи Караваевой</i>
Корректор	<i>Виктория Пиотровская</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 03.11.10.

Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 43,86.

Тираж 1800 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 978-5-9775-0639-7

© Колисниченко Д. Н., 2010  
© Оформление, издательство "БХВ-Петербург", 2010

# Оглавление

- Введение..... 1**
- ЧАСТЬ I. ОСНОВЫ АДМИНИСТРИРОВАНИЯ..... 3**
- Глава 1. Становимся администратором..... 5**
  - 1.1. Краткая история Linux..... 5
  - 1.2. Почему именно Linux? ..... 7
  - 1.3. Основные задачи системного администратора..... 7
- Глава 2. Классификация сетей..... 9**
  - 2.1. Краткая история сетей..... 9
    - 2.1.1. 1941–1975 годы..... 9
    - 2.1.2. 1976–1982 годы..... 10
    - 2.1.3. 1983–1989 годы..... 11
    - 2.1.4. 1990–1995 годы..... 12
    - 2.1.5. 1996–1999 годы..... 13
    - 2.1.6. 2000 — наше время ..... 14
  - 2.2. Классификация сетей..... 14
    - 2.2.1. По занимаемой территории ..... 14
    - 2.2.2. По топологии ..... 15
    - 2.2.3. По ведомственной принадлежности..... 17
    - 2.2.4. По скорости передачи данных ..... 17
    - 2.2.5. По типу среды передачи данных ..... 17
    - 2.2.6. По способу организации взаимодействия компьютеров..... 17
  - 2.3. Способы передачи данных в сетях..... 17
  - 2.4. Модель OSI..... 19
  - 2.5. Что такое протокол? ..... 21
  - 2.6. Адресация компьютеров ..... 22
  - 2.7. Система DNS ..... 25

<b>Глава 3. Основные сетевые устройства .....</b>	<b>26</b>
3.1. Активное и пассивное сетевое оборудование .....	26
3.2. Оборудование, необходимое для построения Ethernet-сети .....	26
3.3. Оборудование, необходимое для построения сети Wi-Fi .....	30
3.4. Дополнительные сетевые устройства .....	31
<b>Глава 4. Планирование сети .....</b>	<b>34</b>
4.1. Важность планирования .....	34
4.1.1. Планирование как основа безопасности .....	35
4.1.2. Построение транспортной системы корпоративной сети .....	36
4.2. Обеспечение безопасности сети .....	38
4.2.1. Защита данных, передаваемых по публичным каналам связи .....	38
4.2.2. Выдача IP-адресов по рабочим местам .....	39
4.2.3. Привязка IP-адресов к MAC-адресам .....	39
4.2.4. Антивирусные серверные решения .....	39
4.2.5. Антивирусные клиентские решения .....	40
4.2.6. Необходим ли дежурный администратор? .....	40
4.3. Человеческий фактор .....	40
4.3.1. Ограничение доступа .....	40
4.3.2. Как быть с обиженными или уволенными сотрудниками? .....	40
4.3.3. Принцип "правая рука не знает, что делает левая" .....	41
4.3.4. Планирование безопасности серверной комнаты/этажа .....	41
4.4. Отдел системного администрирования и безопасности .....	42
4.4.1. Подбор персонала .....	42
4.4.2. Инструктаж отдела ИТ .....	42
4.4.3. Распределение задач и сфер ответственности .....	43
4.4.4. Контроль работы и иерархия .....	43
4.5. Программы для планирования сети .....	44
<b>Глава 5. Монтаж Ethernet-сети .....</b>	<b>45</b>
5.1. Развитие стандарта Ethernet .....	45
5.1.1. Модификации стандарта Ethernet .....	45
5.1.2. Стандарты Fast Ethernet (100 Мбит/с) .....	46
5.1.3. Gigabit Ethernet (1000 Мбит/с) .....	48
5.1.4. Наше будущее — 10 Gigabit Ethernet .....	48
5.2. Несколько слов о коллизиях .....	49
5.3. Монтаж сети .....	50
5.3.1. Основные компоненты Ethernet-сети .....	50
5.3.2. Подробнее о витой паре .....	51
5.3.3. Обжим витой пары .....	52
5.4. Ограничения при построении сети .....	55

<b>Глава 6. Основы беспроводной сети. Монтаж беспроводной сети.....</b>	<b>58</b>
6.1. Преимущества и недостатки беспроводной сети.....	58
6.2. Основные принципы работы беспроводной сети .....	59
6.3. Расширение спектра.....	61
6.4. Wi-Fi.....	62
6.5. Радиочастоты и каналы Wi-Fi.....	65
6.5.1. Стандарты 802.11b и 802.11g .....	65
6.5.2. Стандарт 802.11a .....	66
6.6. Режимы работы сети.....	67
6.7. Основные сетевые устройства беспроводной сети.....	68
6.8. Выбор точки доступа.....	69
6.8.1. Поддерживаемые точкой доступа стандарты .....	70
6.8.2. Область применения и радиус действия точки доступа .....	70
6.8.3. Антенна точки доступа .....	71
6.8.4. Алгоритм шифрования .....	71
6.8.5. Дополнительные функции.....	71
6.9. Настройка беспроводной сети .....	73
6.9.1. Выбор расположения точки доступа .....	73
6.9.2. Физическая установка точки доступа.....	75
6.9.3. Практическая настройка беспроводной сети.....	76
6.9.4. Настройка соединения Wi-Fi в Linux .....	81
 <b>ЧАСТЬ II. ЗНАКОМСТВО С LINUX .....</b>	<b>83</b>
 <b>Глава 7. Особенности установки Linux .....</b>	<b>85</b>
7.1. Системные требования .....	85
7.2. Параметры ядра.....	86
7.3. Проверка носителей.....	89
7.4. Изменение таблицы разделов .....	90
7.5. Выбор групп пакетов .....	95
7.6. Выбор графической среды .....	97
7.7. Установка пароля root .....	97
7.8. Создание учетных записей пользователей .....	99
7.9. Установка Linux по сети.....	100
7.9.1. Немного о загрузке и установке по сети .....	100
7.9.2. Подготовка загрузочного сервера.....	100
7.9.3. Настройка клиента .....	102
7.10. Проблемы при установке .....	102
7.10.1. Проблема с APIC .....	102
7.10.2. Ошибка: <i>kernel panic:VFS: Unable to mount root fs</i> .....	103
7.10.3. Проблемы с некоторыми LCD-мониторами .....	103
7.10.4. Сообщение <i>Probing EDD</i> и зависание системы.....	103

7.10.5. Список известных проблем в Mandriva Linux 2009 .....	103
7.10.6. Не переключается раскладка в Fedora 13.....	104
7.11. Вход в систему и завершение работы .....	104
<b>Глава 8. Командная строка Linux.....</b>	<b>106</b>
8.1. Консоль .....	106
8.2. Переход в консоль и обратно.....	106
8.3. Выход из консоли и завершение работы (команды <i>poweroff</i> , <i>halt</i> , <i>reboot</i> , <i>shutdown</i> ) .....	107
8.4. Как работать в консоли .....	108
8.5. Графические терминалы.....	109
8.6. Перенаправление ввода/вывода.....	110
8.7. Команды Linux .....	111
<b>Глава 9. Файловая система .....</b>	<b>112</b>
9.1. Файловые системы, поддерживаемые Linux.....	112
9.1.1. Выбор файловой системы.....	113
9.1.2. Linux и файловые системы Windows.....	114
9.1.3. Сменные носители.....	115
9.2. Особенности файловой системы Linux.....	115
9.2.1. Имена файлов .....	115
9.2.2. Файлы и устройства .....	115
9.2.3. Корневая файловая система и монтирование .....	116
9.2.4. Стандартные каталоги Linux .....	117
9.2.5. Ссылки: жесткие и символические.....	118
9.2.6. Задание прав доступа к файлам и каталогам .....	119
9.2.7. Специальные права доступа (SUID и SGID).....	120
9.3. Монтирование файловых систем .....	120
9.3.1. Команды <i>mount</i> и <i>umount</i> .....	120
9.3.2. Файлы устройств и монтирование.....	121
9.3.3. Опции монтирования файловых систем .....	124
9.3.4. Монтирование разделов при загрузке .....	125
9.3.5. Подробно о UUID и файле <i>/etc/fstab</i> .....	127
9.3.6. Монтирование Flash-дисков .....	129
9.4. Настройка журнала файловой системы ext3 .....	130
9.5. Файловая система ext4.....	131
9.5.1. Сравнение ext3 и ext4.....	131
9.5.2. Совместимость с ext3 .....	132
9.5.3. Переход на ext4.....	132
9.6. Псевдофайловые системы .....	133
9.6.1. Виртуальная файловая система <i>sysfs</i> .....	134
9.6.2. Виртуальная файловая система <i>proc</i> .....	134

9.7. Программы для разметки диска .....	138
9.7.1. Программа <i>fdisk</i> .....	138
9.7.2. Программа <i>parted</i> .....	140
<b>Глава 10. Команды управления пользователями .....</b>	<b>145</b>
10.1. Многопользовательская система .....	145
10.2. Пользователь <i>root</i> .....	146
10.2.1. Максимальные полномочия .....	146
10.2.2. Как работать без <i>root</i> .....	146
10.2.3. Переход к традиционной учетной записи <i>root</i> .....	150
10.3. Создание, удаление и модификация пользователей стандартными средствами .....	152
10.3.1. Команды <i>adduser</i> и <i>passwd</i> .....	152
10.3.2. Команда <i>usermod</i> .....	153
10.3.3. Команда <i>userdel</i> .....	154
10.3.4. Подробно о создании пользователей .....	154
10.4. Группы пользователей .....	155
10.5. Команды квотирования .....	155
<b>ЧАСТЬ III. НАСТРОЙКА СЕТИ В LINUX .....</b>	<b>159</b>
<b>Глава 11. Настройка локальной сети .....</b>	<b>161</b>
11.1. Несколько слов о монтаже сети .....	161
11.2. Файлы конфигурации сети в Linux .....	163
11.3. Настройка сети с помощью конфигуратора .....	165
11.3.1. Настройка сети в Linux Mandriva .....	166
11.3.2. Настройка сети в Fedora .....	173
11.3.3. Настройка сети в Debian, Ubuntu и Denix. Конфигураторы nm-connection-editor (NetworkManager) и network-admin .....	178
11.3.4. Конфигуратор <i>netconfig</i> в Slackware .....	181
11.4. Утилиты для диагностики соединения .....	181
11.5. Для фанатов, или как настроить сеть вручную .....	185
11.5.1. Конфигурационные файлы Fedora .....	186
11.5.2. Конфигурационные файлы openSUSE .....	188
11.5.3. Конфигурационные файлы Debian/Ubuntu .....	190
11.6. Команда <i>mti-tool</i> .....	190
11.7. Перед тем как перейти к следующей главе .....	191
<b>Глава 12. Настройка ADSL-доступа к Интернету .....</b>	<b>192</b>
12.1. Причина популярности DSL-соединений .....	192
12.2. Физическое подключение ADSL-модема .....	192

12.3. Настройка DSL-соединения в Fedora .....	193
12.4. Настройка DSL-соединения в openSUSE.....	195
12.5. Настройка DSL-соединения в Ubuntu .....	199
12.6. Настройка DSL-соединения в Mandriva.....	203
<b>Глава 13. Подключение к сети Wi-Fi .....</b>	<b>204</b>
13.1. О настройке Wi-Fi в Linux .....	204
13.2. Простая настройка (Ubuntu/Denix/Fedora) .....	204
13.3. "Тяжелый случай" .....	206
13.4. Возможные осложнения .....	209
<b>Глава 14. Маршрутизация .....</b>	<b>210</b>
14.1. Выбор маршрута, или краткое введение в маршрутизацию.....	210
14.2. Таблица маршрутизации ядра. Установка маршрута по умолчанию .....	211
14.3. Изменение таблицы маршрутизации. Команда <i>route</i> .....	215
14.4. Включение IPv4-переадресации, или превращение компьютера в шлюз .....	217
14.5. Протоколы маршрутизации .....	218
14.5.1. Routing Information Protocol .....	218
14.5.2. RIP-2.....	218
14.5.3. Open Shortest Path First.....	219
<b>Глава 15. Брандмауэры iptables и ebtables.....</b>	<b>220</b>
15.1. Что такое брандмауэр .....	220
15.2. Цепочки и правила .....	221
15.3. Использование брандмауэра iptables .....	223
15.4. Шлюз своими руками .....	226
15.5. Брандмауэр ebtables .....	231
<b>ЧАСТЬ IV. ОПЕРАЦИОННАЯ СИСТЕМА LINUX.....</b>	<b>233</b>
<b>Глава 16. Загрузчики Linux .....</b>	<b>235</b>
16.1. Базовые загрузчики.....	235
16.2. Конфигурационные файлы GRUB и GRUB2 .....	236
16.2.1. Конфигурационный файл GRUB .....	236
16.2.2. Конфигурационный файл GRUB2 .....	237
16.3. Команды установки загрузчиков .....	242
16.4. Установка тайм-аута выбора операционной системы. Редактирование параметров ядра Linux.....	242
16.5. Установка собственного фона загрузчика GRUB и GRUB2.....	245
16.6. Постоянные имена и GRUB .....	246
16.7. Две и более ОС Linux на одном компьютере .....	246
16.8. Загрузка с ISO-образов .....	248



<b>Глава 17. Системы инициализации Linux .....</b>	<b>249</b>
17.1. Начальная загрузка Linux .....	249
17.2. Система инициализации init .....	250
17.2.1. Файл <code>/etc/inittab</code> .....	250
17.2.2. Команда <code>init</code> .....	252
17.2.3. Команда <code>service</code> .....	252
17.2.4. Редакторы уровней запуска .....	252
17.3. Система инициализации <code>upstart</code> .....	255
17.3.1. Как работает <code>upstart</code> ? .....	255
17.3.2. Конфигурационные файлы <code>upstart</code> .....	256
17.4. Система инициализации <code>Slackware</code> .....	257
 <b>Глава 18. Пакеты и управление пакетами .....</b>	<b>259</b>
18.1. Что такое пакет? .....	259
18.2. Репозитории пакетов .....	261
18.3. Программы для управления пакетами .....	262
18.4. Программы <code>rpm</code> и <code>rpmbuild</code> (все Red Hat-совместимые дистрибутивы) .....	263
18.5. Графический менеджер пакетов <code>rpm-drake</code> ( <code>Mandriva</code> ) .....	264
18.6. Программа <code>urpmi</code> .....	266
18.6.1. Установка пакетов. Управление источниками пакетов.....	267
18.6.2. Обновление и удаление пакетов .....	271
18.6.3. Поиск пакета. Получение информации о пакете.....	271
18.7. Программа <code>yum</code> .....	272
18.7.1. Использование <code>yum</code> .....	272
18.7.2. Управление источниками пакетов .....	274
18.7.3. Установка пакетов через прокси-сервер .....	275
18.7.4. Плагины для <code>yum</code> .....	276
18.8. Графический менеджер пакетов в <code>Fedora</code> — <code>gpk-application</code> .....	276
18.9. Программы <code>dpkg</code> и <code>apt-get</code> : установка пакетов в <code>Debian/Ubuntu</code> .....	277
18.9.1. Программа <code>dpkg</code> .....	277
18.9.2. Программа <code>apt-get</code> .....	278
18.9.3. Установка <code>RPM</code> -пакетов в <code>Debian/Ubuntu</code> .....	280
18.9.4. Подключение репозитория <code>Medibuntu</code> .....	280
18.9.5. Графический менеджер <code>Synaptic</code> в <code>Debian/Ubuntu</code> .....	280
18.10. Установка пакетов в <code>Slackware</code> .....	281
18.10.1. Управление пакетами.....	283
18.10.2. Нет нужного пакета: вам поможет программа <code>rpm2tgz</code> .....	285
18.10.3. Программа <code>slackpkg</code> : установка пакетов из Интернета.....	286
18.11. Установка программ в <code>openSUSE</code> .....	287
18.11.1. Менеджер пакетов <code>zypper</code> .....	287
18.11.2. Графический менеджер ёпакетов <code>openSUSE</code> .....	290

<b>Глава 19. Процессы .....</b>	<b>294</b>
19.1. Аварийное завершение процесса.....	294
19.2. Программа <i>top</i> — кто больше всех расходует процессорное время? .....	296
19.3. Изменение приоритета процесса .....	298
19.4. Перенаправление ввода/вывода.....	299
<b>Глава 20. Протоколирование системы. Журналы .....</b>	<b>300</b>
20.1. Демоны протоколирования системы.....	300
20.2. Изучаем файлы журналов .....	302
<b>Глава 21. Резервное копирование.....</b>	<b>305</b>
21.1. Зачем нужно делать резервные копии .....	305
21.2. Выбор носителя для резервной копии .....	306
21.3. Правила хранения носителей с резервными копиями.....	307
21.4. Стратегии создания резервной копии .....	307
21.5. Программа <i>tag</i> .....	309
21.6. Сетевое резервное копирование .....	310
21.7. Запись CD/DVD из консоли.....	311
21.7.1. Команда <i>dd</i> — создание образа диска .....	311
21.7.2. Команды <i>cdrecord</i> и <i>dvdrecord</i> — запись образа на болванку .....	312
21.7.3. Команды очистки перезаписываемых дисков .....	312
21.7.4. Команда <i>mkisofs</i> — создание ISO-образа .....	313
21.7.5. Преобразование образов дисков .....	313
21.7.6. Создание и монтирование файлов с файловой системой.....	314
<b>Глава 22. Автоматизация выполнения задач.</b>	
<b>Планировщики задач <i>crond</i>, <i>anacron</i>, <i>atd</i> .....</b>	<b>315</b>
22.1. Планировщик задач — зачем он нужен? .....	315
22.2. Планировщик <i>crond</i> .....	315
22.3. Планировщик <i>anacron</i> .....	317
22.4. Разовое выполнение команд — демон <i>atd</i> .....	317
<b>ЧАСТЬ V. ЛОКАЛЬНАЯ БЕЗОПАСНОСТЬ LINUX-СЕРВЕРА.....</b>	<b>319</b>
<b>Глава 23. Основные уязвимости .....</b>	<b>321</b>
23.1. От кого будем защищать сервер? Мотивация взлома .....	321
23.2. Ваша система взломана .....	322
23.3. Основные уязвимости Linux-сервера .....	324

<b>Глава 24. Обеспечение безопасности сервера.....</b>	<b>326</b>
24.1. Защита от "восстановления пароля root" .....	326
24.2. Защита от перезагрузки .....	327
24.3. Отключение учетной записи root — нестандартный метод .....	328
24.4. Отключение учетной записи root средствами KDM.....	331
24.5. Система управления доступом .....	331
<b>Глава 25. Параметры загрузчика Linux .....</b>	<b>332</b>
25.1. Установка пароля .....	332
25.1.1. Загрузчик GRUB2.....	332
25.1.2. Загрузчик GRUB.....	333
25.2. Восстановление загрузчика GRUB/GRUB2 .....	334
<b>Глава 26. RAID-массивы .....</b>	<b>336</b>
26.1. Что такое RAID?.....	336
26.2. Программные RAID-массивы .....	338
26.3. Создание программных массивов .....	338
<b>ЧАСТЬ VI. НАСТРОЙКА СЕТЕВЫХ СЛУЖБ.....</b>	<b>341</b>
<b>Глава 27. DNS-сервер .....</b>	<b>343</b>
27.1. Еще раз о том, что такое DNS.....	343
27.2. Кэширующий сервер DNS.....	344
27.3. Полноценный DNS-сервер .....	349
27.4. Вторичный DNS-сервер.....	353
27.5. Обновление базы данных корневых серверов .....	354
<b>Глава 28. DHCP-сервер.....</b>	<b>357</b>
28.1. Протокол динамической конфигурации узла.....	357
28.2. Конфигурационный файл DHCP-сервера .....	357
28.3. База данных аренды .....	359
28.4. Полный листинг конфигурационного файла .....	359
28.5. Управление сервером DHCP.....	360
28.6. Настройка клиентов .....	360
<b>Глава 29. Web-сервер. Связка Apache + PHP + MySQL.....</b>	<b>361</b>
29.1. Самый популярный Web-сервер.....	361
29.2. Установка Web-сервера и интерпретатора PHP. Выбор версии.....	361
29.3. Тестирование настроек.....	363

29.4. Файл конфигурации Web-сервера .....	365
29.4.1. Базовая настройка.....	365
29.4.2. Самые полезные директивы файла конфигурации .....	365
29.4.3. Директивы <i>Directory</i> , <i>Limit</i> , <i>Location</i> , <i>Files</i> .....	367
29.5. Управление запуском сервера Apache .....	369
29.6. Пользовательские каталоги.....	370
29.7. Установка сервера баз данных MySQL .....	370
29.7.1. Установка сервера .....	370
29.7.2. Изменение пароля root и добавление пользователей.....	371
29.7.3. Запуск и останов сервера .....	372
29.7.4. Программа MySQL Administrator .....	372
<b>Глава 30. FTP-сервер.....</b>	<b>374</b>
30.1. Зачем нужен FTP.....	374
30.2. Установка FTP-сервера.....	374
30.3. Конфигурационный файл.....	375
30.4. Настройка реального сервера .....	379
30.5. Программы ftpwho и ftpcount.....	380
30.6. Конфигуратор gproftpd .....	381
30.7. Альтернативные FTP-серверы .....	382
<b>Глава 31. Почтовый сервер.....</b>	<b>383</b>
31.1. Что такое Qmail? .....	383
31.2. Подготовка к установке Qmail.....	383
31.3. Установка Qmail и необходимых дополнений.....	385
31.3.1. Загрузка и установка Qmail .....	385
31.3.2. Установка ucspi-tcp и daemontools.....	386
31.3.3. Установка EZmlm — средства для создания рассылки .....	386
31.3.4. Установка Autoresponder — автоответчика .....	386
31.3.5. Установка MailDrop — фильтра для сообщений .....	386
31.3.6. Установка QmailAdmin — Web-интерфейса для настройки Qmail.....	387
31.4. Настройка после установки и запуск Qmail .....	387
31.5. Настройка почтовых клиентов .....	389
31.6. Дополнительная информация .....	390
<b>Глава 32. Сервис Samba.....</b>	<b>391</b>
32.1. Установка Samba.....	391
32.2. Базовая настройка Samba .....	391
32.3. Настройка общих ресурсов .....	392
32.4. Просмотр ресурсов Windows-сети .....	394

<b>Глава 33. Настройка SSH-сервера .....</b>	<b>395</b>
33.1. Протокол SSH и SSH-клиент .....	395
33.2. ssh-сервер .....	397
<b>Глава 34. Сервер времени .....</b>	<b>401</b>
34.1. Проблема синхронизации времени .....	401
34.2. Настройка сервера и Linux-клиентов .....	401
34.3. Настройка Windows-клиентов .....	402
<b>Глава 35. Сетевая файловая система NFS .....</b>	<b>405</b>
35.1. Установка сервера и клиента .....	405
35.2. Настройка сервера .....	405
35.3. Монтирование удаленных файловых систем .....	407
<b>ЧАСТЬ VII. БЕЗОПАСНОСТЬ В СЕТИ.....</b>	<b>409</b>
<b>Глава 36. Аудит сети с помощью nmap .....</b>	<b>411</b>
36.1. Что такое nmap? .....	411
36.2. Где мне взять nmap?.....	412
36.3. Основы использования nmap .....	412
<b>Глава 37. Защита сетевых сервисов .....</b>	<b>414</b>
37.1. Защита Web-сервера .....	414
37.2. Защита FTP .....	414
37.3. Защита DNS .....	415
37.4. Защита Samba .....	416
37.5. DHCP — привязка к MAC-адресу .....	416
37.6. Защита от спама: Greylisting и Qmail .....	419
<b>Глава 38. Оптимизация сервера .....</b>	<b>421</b>
38.1. Общая оптимизация Linux .....	421
38.1.1. Оптимизация подкачки .....	421
38.1.2. Изменение планировщика ввода/вывода .....	422
38.2. Оптимизация сетевых сервисов .....	423
38.2.1. Секреты оптимизации Samba .....	424
38.2.2. Оптимизация ProFTPD.....	424
38.2.3. Оптимизация Apache.....	426
38.2.4. Оптимизация SSH.....	428

<b>Глава 39. Chroot-окружение .....</b>	<b>429</b>
39.1. Песочница .....	429
39.2. Пример создания chroot-окружения .....	429
<b>Глава 40. Управление доступом.....</b>	<b>432</b>
40.1. Что такое Томоуо?.....	432
40.2. Установка Томоуо. Готовые LiveCD .....	432
40.3. Инициализация системы .....	433
<b>Глава 41. Виртуальные частные сети.....</b>	<b>437</b>
41.1. Для чего нужна виртуальная частная сеть?.....	437
41.2. Необходимое программное обеспечение.....	438
41.3. Канал для передачи данных VPN .....	438
41.3.1. Соединение сеть-сеть .....	438
41.3.2. Соединение клиент-сеть .....	439
41.4. Настройка соединения сеть-сеть .....	439
41.4.1. Установка OpenS/WAN.....	439
41.4.2. Немного терминологии.....	439
41.4.3. Генерирование ключей .....	440
41.4.4. Конфигурационный файл .....	440
41.4.5. Установка VPN-соединения .....	443
41.4.6. Настройка брандмауэра iptables.....	443
41.5. Настройка соединения клиент-сеть.....	444
41.5.1. Редактирование конфигурационных файлов.....	444
41.5.2. Настройка Linux-клиента.....	447
41.5.3. Настройка Windows-клиента.....	449
<b>Глава 42. Прокси-сервер Squid и антивирус ClamAV .....</b>	<b>454</b>
42.1. Зачем нужен прокси-сервер в локальной сети? .....	454
42.1.1 Базовая настройка Squid .....	454
42.1.2. Практические примеры настройки Squid.....	456
42.1.3. Управление прокси-сервером.....	457
42.1.4. Настройка клиентов .....	457
42.1.5. Прозрачный прокси-сервер .....	458
42.1.6. Расширение squidGuard .....	459
42.2. Антивирусная защита .....	462
42.2.1. Зачем нужен антивирус в Linux .....	462
42.2.2. Установка ClamAV .....	463
42.2.3. Проверка файловой системы.....	463
42.2.4. Прозрачная проверка почты .....	463
42.2.5. Проверка Web-трафика.....	464

<b>ЧАСТЬ VIII. ТЕОРИЯ И ПРАКТИКА СИСТЕМНОГО АДМИНИСТРАТОРА.....</b>	<b>469</b>
<b>Глава 43. Стратегия администрирования .....</b>	<b>471</b>
43.1. О чем эта глава? .....	471
43.2. И руководство, и пользователи довольны. Миф или реальность? .....	472
43.3. Роль главного администратора .....	474
<b>Глава 44. Уход за "железом" .....</b>	<b>478</b>
44.1. Обязанности администратора .....	478
44.2. "Про запас", или обменный фонд .....	479
44.3. Чистка компьютеров. Профилактика системы охлаждения .....	480
44.4. Охлаждение компьютеров .....	481
44.5. Стойки для оборудования .....	482
44.6. Влажность .....	483
44.7. Инструмент системного администратора .....	484
<b>Заключение .....</b>	<b>487</b>
<b>ПРИЛОЖЕНИЯ .....</b>	<b>489</b>
<b>Приложение 1. Параметры ядра .....</b>	<b>491</b>
<b>Приложение 2. Суперсервер xinetd .....</b>	<b>494</b>
П2.1. Сетевые сервисы и суперсервер .....	494
П2.2. Конфигурационный файл суперсервера .....	494
<b>Приложение 3. Команды Linux .....</b>	<b>496</b>
П3.1. Общие команды .....	496
П3.1.1. Команда <i>arch</i> — вывод архитектуры компьютера .....	496
П3.1.2. Команда <i>clear</i> — очистка экрана .....	496
П3.1.3. Команда <i>date</i> .....	497
П3.1.4. Команда <i>echo</i> .....	497
П3.1.5. Команда <i>exit</i> — выход из системы .....	497
П3.1.6. Команда <i>man</i> — вывод справки .....	497
П3.1.7. Команда <i>passwd</i> — изменение пароля .....	497
П3.1.8. Команда <i>startx</i> — запуск графического интерфейса X.Org .....	497
П3.1.9. Команда <i>uptime</i> — информация о работе системы .....	498
П3.1.10. Команда <i>users</i> — информация о пользователях .....	498
П3.1.11. Команды <i>w</i> , <i>who</i> и <i>whoami</i> — информация о пользователях .....	498
П3.1.12. Команда <i>xf86config</i> — настройка графической подсистемы .....	499

ПЗ.2. Команды для работы с файлами и каталогами, ссылками, правами доступа .....	499
ПЗ.2.1. Работа с файлами.....	499
ПЗ.2.2. Работа с каталогами .....	501
ПЗ.2.3. Команда <i>ln</i> — создание ссылок, жестких и символических .....	503
ПЗ.2.4. Команда <i>chmod</i> — права доступа к файлам и каталогам .....	503
ПЗ.2.5. Команда <i>chown</i> — смена владельца файла .....	505
ПЗ.2.6. Команда <i>chattr</i> — изменение атрибутов файла, запрет изменения файла.....	505
ПЗ.2.7. Команда <i>mkfs</i> — создание файловой системы.....	505
ПЗ.2.8. Команда <i>fsck</i> — проверка и восстановление файловой системы.....	506
ПЗ.2.9. Команда <i>chroot</i> — смена корневой файловой системы .....	506
ПЗ.2.10. Установка скорости CD/DVD.....	506
ПЗ.2.11. Монтирование каталога к каталогу .....	507
ПЗ.2.12. Команды поиска файлов .....	507
ПЗ.2.13. Создание файла подкачки.....	508
ПЗ.3. Команды для работы с текстом .....	509
ПЗ.3.1. Команда <i>diff</i> — сравнение файлов .....	509
ПЗ.3.2. Команда <i>grep</i> — текстовый фильтр.....	509
ПЗ.3.3. Команды <i>more</i> и <i>less</i> — постраничный вывод.....	510
ПЗ.3.4. Команды <i>head</i> и <i>tail</i> — вывод начала и хвоста файла .....	510
ПЗ.3.5. Команда <i>wc</i> — подсчет слов в файле .....	510
ПЗ.4. Команды для работы с Интернетом .....	510
ПЗ.4.1. Команда <i>ftp</i> — стандартный FTP-клиент .....	510
ПЗ.4.2. Команда <i>lynx</i> — текстовый браузер.....	512
ПЗ.4.3. Команда <i>mail</i> — чтение почты и отправка сообщений .....	512
ПЗ.5. Команды системного администратора.....	512
ПЗ.5.1. Команды <i>free</i> и <i>df</i> — информация о системных ресурсах.....	512
ПЗ.5.2. Команда <i>md5sum</i> — вычисление контрольного кода MD5 .....	513
<b>Предметный указатель .....</b>	<b>515</b>



## Глава 3



# Основные сетевые устройства

### 3.1. Активное и пассивное сетевое оборудование

Для построения компьютерной сети, то есть для организации передачи информации между компьютерами, используется сетевое оборудование. Сетевое оборудование бывает активным и пассивным. *Активным* называется оборудование, обладающее неким "интеллектом" — например, коммутатор (switch), маршрутизатор (router). *Пассивное* сетевое оборудование "интеллектом" не наделено. К пассивному оборудованию относят кабели (например, коаксиальный или витая пара), розетки (RJ45, RG58 и др.), повторитель (repeater), концентратор (hub) и т. д.

Стоп! Если вы хоть немного знакомы с Ethernet-сетями, вы можете запутаться. Ведь концентратор, как и коммутатор, можно использовать в качестве центрального сетевого устройства в Ethernet-сети, почему тогда концентратор — это пассивное устройство, а коммутатор — активное? Дело в том, что концентратор не проявляет никакой интеллектуальной деятельности — он просто получает сигналы и копирует (повторяет) их на все свои порты, равно как и повторитель. Повторитель получает сигнал, усиливает его и повторяет на другой порт. Повторители обычно используются для увеличения дальности передаваемого сигнала. Коммутатор же "знает", к какому порту подключен какой компьютер, поэтому передает полученный сигнал не на все порты, а только на определенный порт, к которому подключен компьютер-назначение.

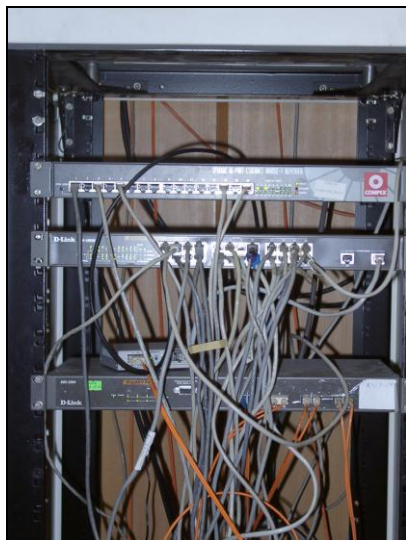
Различного сетевого оборудования очень много. Мы не будем пытаться объять необъятное, поэтому в этой книге рассмотрим только оборудование, необходимое для построения проводных Ethernet-сетей и беспроводных сетей Wi-Fi.

### 3.2. Оборудование, необходимое для построения Ethernet-сети

Для организации современной Ethernet-сети (имеются в виду спецификации Fast Ethernet и Gigabit Ethernet) необходим всего один коммутатор (switch). Конечно, если сеть большая, то понадобится несколько коммутаторов, общее количество портов которых сможет обеспечить подключение всех узлов сети. На рис. 3.1 изображен так называемый *промышленный* коммутатор от Linksys.



**Рис. 3.1.** 16-портовый коммутатор от Linksys



**Рис. 3.2.** Стойка с коммутаторами



**Рис. 3.3.** Шкаф с сетевым оборудованием



**Рис. 3.4.** 8-портовый гигабитный коммутатор от D-Link

Дизайн корпуса промышленного коммутатора обычно не очень эффектен, но сделано это умышленно — чтобы коммутатор можно было поместить в стойку сетевого оборудования. Ведь в больших корпоративных сетях обычно несколько коммутаторов, которые помещаются в специальную стойку (или в специальный шкаф сетевого оборудования, который можно закрыть и тем самым ограничить физический доступ к нему). На рис. 3.2 изображена типичная стойка с коммутаторами.

А на рис. 3.3 показан шкаф с коммутаторами. Такой шкаф может быть большего размера и содержать другое оборудование (например, серверы сети), но главное отличие шкафа от стойки — наличие двери, которая ограничивает доступ к сетевому оборудованию.

Если вы хотите построить небольшую домашнюю или офисную сеть, то можете выбрать коммутатор с более интересным дизайном, который лучше впишется в ваш интерьер. На рис. 3.4 представлен 8-портовый гигабитный коммутатор от D-Link. Вид у него более "дружелюбный", но в стойку его уже не поместишь (впрочем, при организации домашней сети никакой стойки у вас и не будет).

Давайте теперь уточним, почему в современных сетях не стоит использовать концентраторы (hub). Представим, что у нас есть сеть на четыре компьютера. Назовем их А, Б, В и Г. Пусть компьютер А отправляет данные компьютеру Г. Концентратор отправит полученный от компьютера А сигнал на все свои порты — то есть сигнал, отправленный компьютером А, получают все компьютеры сети. Затем каждый компьютер анализирует заголовки пакета, в которых указан компьютер-получатель. Если адрес компьютера совпадает с адресом получателя, компьютер принимает пакет, в противном случае — игнорирует его. Таким образом, использование концентратора приводит к "брожению" по сети паразитного трафика. По сути, концентратор — это обычный многопортовый повторитель (усилитель) сигналов. И чем больше сеть, тем медленнее она работает в случае использования концентратора, поскольку "брожение" паразитного трафика носит лавинообразный характер. Вы только представьте, что в сети не четыре компьютера, а несколько десятков... Поэтому в больших сетях концентраторы существенно снижают производительность сети.

Коммутатор же, в отличие от концентратора, строит специальную таблицу соответствия, позволяющую однозначно узнать, к какому порту какой компьютер подключен (см., например, табл. 3.1).

**Таблица 3.1.** Таблица соответствия портов коммутатора и адресов компьютеров

Номер порта	Адрес компьютера
1	Б
2	А
3	Г
4	В

Когда компьютер А, подключенный ко второму порту коммутатора, отправляет пакет компьютеру Г, коммутатор знает, что компьютер Г подключен к третьему порту, и отправляет пакет только на третий порт. При этом снижается нагрузка на сеть, потому что компьютеры не получают "лишних" пакетов.

Кроме того, поскольку концентратор отправляет данные каждому компьютеру сети, становится очень простым перехват данных. Существуют специальные программы, переводящие сетевой адаптер компьютера в режим мониторинга, в котором он осуществляет принятие всех данных, даже тех, которые не адресованы этому компьютеру. Поэтому, если в сети используется концентратор, все передаваемые данные становятся общим достоянием — их может перехватить любой компьютер, подключенный к концентратору.

Итак, использование коммутатора позволяет повысить производительность сети и повысить ее безопасность. Ранее сети в основном строились на базе концентрато-

ров, поскольку их стоимость была существенно ниже стоимости коммутаторов. Со снижением цен на коммутаторы концентраторы практически исчезли с магазинных полок. Однако в некоторых старых сетях они еще используются. Если вам придется обслуживать такую сеть, первым делом замените концентратор на коммутатор — вы сразу почувствуете разницу.

Какой коммутатор применить: Fast Ethernet (100Base-T) или Gigabit Ethernet (1000Base-T)? В первом случае максимальная (теоретическая) скорость передачи данных составляет 100 Мбит/с, во втором случае — 1000 Мбит/с. Коммутаторы Gigabit Ethernet стоят немного дороже (цены приводить не буду, поскольку через год они станут еще доступнее, а через два — о Fast Ethernet забудут, как в свое время забыли о коаксиале и концентраторах).

Учитывая, что сеть строится не на день и не на два, лучше выбрать Gigabit Ethernet. С точки зрения монтажа сети ничего не изменится — даже если вы сейчас установите коммутатор Fast Ethernet, то завтра без проблем сможете заменить его на Gigabit Ethernet. Но нужно помнить следующее: чтобы сеть работала в режиме 1000Base-T, необходимо, чтобы 1000Base-T поддерживали сетевые адаптеры компьютеров. Практически на всех современных материнских платах встроенные сетевые адаптеры уже поддерживают 1000Base-T, но если в вашей сети есть компьютеры, которым 2–3 года, скорее всего, вам придется докупать для них сетевые адаптеры с поддержкой 1000Base-T.

Идем дальше — количество портов. Обычно в продаже есть коммутаторы на 5, 8, 16, 24 порта. Промышленные коммутаторы могут иметь большее число портов, например 32 или 48. Может быть, в скором времени появятся коммутаторы с еще большим числом узлов, но я сомневаюсь. Поскольку обычно один коммутатор обслуживает одну подсеть, я не думаю, что в одной подсети будет больше 48 компьютеров. А если это случится, такую подсеть желательно (из соображений локализации трафика) разделить на несколько подсетей с меньшим числом компьютеров.

Так что для домашней сети покупайте коммутатор, способный подключить все имеющиеся дома компьютеры, — большой запас портов вам вряд ли понадобится. Обычно в домашней сети 2–4 компьютера. В этом случае вам будет достаточно 5-портового коммутатора — 5-й порт пригодится для подключения этого коммутатора к другому коммутатору сети. В коммутаторах с большим числом портов для подключения к другому коммутатору обычно используется один из имеющихся портов (например, порт 1).

Промышленные коммутаторы иногда имеют так называемый *магистральный* порт. Например, 16 портов, работающих в режиме 100Base-T, и один порт, работающий в режиме 1000Base-T, — для подключения к магистральной сети, работающей со скоростью 1000 Мбит/с. Иногда вместо порта 1000Base-T оборудуется оптоволоконный порт, например, 100Base-FB. В этом случае скорость магистральной сети такая же, как и скорость сети, но расстояние передачи сигнала намного выше (более 2 км), что позволяет использовать оптоволоконный кабель для соединения сетей двух (или более) зданий в одну большую сеть.

В случае с офисной сетью количество портов коммутатора должно в два раза превышать количество компьютеров сети. Например, если в вашей сети четыре компьютера, то нужен 8-портовый коммутатор. Дополнительные четыре порта

могут понадобиться, если придется подключить дополнительные компьютеры, например, ноутбуки ваших клиентов, если у вас пока еще нет для них точки доступа Wi-Fi.

По большому счету, для организации сети больше ничего и не нужно (разумеется, кроме кабеля и коннекторов RJ45, но это уже детали, о которых мы поговорим в *третьей части* книги).

### 3.3. Оборудование, необходимое для построения сети Wi-Fi

Как и в случае с Ethernet-сетью, нам понадобятся сетевые адаптеры и центральное устройство сети. Только сетевые адаптеры нужны не обычные, а беспроводные. А роль центрального устройства сети будет играть *точка доступа* (access point).

Все современные модели ноутбуков по умолчанию оснащены адаптером Wi-Fi, а вот стационарные (настольные) компьютеры придется дооснастить беспроводными сетевыми адаптерами. Проще всего купить беспроводной адаптер, подключающийся к компьютеру по USB. Есть также адаптеры, выполненные в виде PCI-карты, устанавливаемой в свободный PCI-слот компьютера. Такие адаптеры используются редко, поскольку их установка требует вскрытия корпуса компьютера, что несколько неудобно (особенно, если компьютер еще на гарантии — тогда придется нести его в сервисный центр, а что делать, если таких компьютеров много?).

USB-адаптеры могут быть выполнены в разных корпусах. На рис. 3.5 изображен небольшой беспроводной адаптер, напоминающий по своим размерам флешку. У такого адаптера антенна встроенная, поэтому его можно использовать только, если компьютер находится в зоне уверенного приема. Если же компьютер установлен ближе к "мертвой" зоне, лучше выбрать адаптер, выполненный в виде отдельного устройства (рис. 3.6). Такой адаптер обычно имеет небольшой размер и подключается к компьютеру USB-кабелем (питание адаптер получает тоже по USB). Преимущество этого адаптера заключается в следующем — его можно легко передвинуть в пределах длины USB-кабеля, чтобы попасть в зону уверенного приема сети. Ноутбук можно легко переместить в эту зону — просто взяли и перенесли. Со стационарным компьютером такого не сделаешь — у каждого стационарного компьютера есть свое место. А что делать, если в том месте, где установлен компьютер, не обеспечивается уверенный прием беспроводных сигналов? Не переносить же компьютер? В этой ситуации поможет адаптер, изображенный на рис. 3.6. Иногда перемещение адаптера всего на несколько сантиметров дает весьма ощутимые результаты. Да и антенна у такого адаптера обладает большей чувствительностью, чем встроенная антенна адаптера, изображенного на рис. 3.5. К тому же к подобным адаптерам (с внешней антенной) обычно можно подключить дополнительную антенну с еще большей чувствительностью. Обо всем этом мы поговорим, когда будем строить свою собственную беспроводную сеть. А сейчас перейдем лучше к точке доступа.

#### ПРИМЕЧАНИЕ

При выборе Wi-Fi-адаптера учитывайте наличие драйверов — особенно, если вы планируете использовать его в Linux. Чтобы не получилось так, что Linux не поддержит купленный Wi-Fi-адаптер.



**Рис. 3.5.** USB Wi-Fi-адаптер со встроенной антенной



**Рис. 3.6.** USB Wi-Fi-адаптер с внешней антенной



**Рис. 3.7.** Точка доступа от D-Link с тремя антеннами

Точка доступа (рис. 3.7) выполняет в беспроводной сети роль центрального устройства. Казалось бы, все здесь просто: устанавливаем Wi-Fi-адаптеры, подключаем точку доступа, и беспроводная сеть готова — беспроводные клиенты могут обмениваться данными. Однако, если вы планируете купить точку доступа прямо сейчас, не следует покупать первую попавшуюся. Сначала желательно определиться, какие функции точки доступа вам нужны, затем "вычислить" модели точек доступа, обеспечивающие необходимые вам функции, и просмотреть в Интернете отзывы об этих моделях. Только так можно выбрать лучшую точку доступа.

Точка доступа может предоставлять дополнительные функции — например, функции *маршрутизатора*. Предположим, у вас дома есть несколько ноутбуков. К одному ноутбуку подключен ADSL-модем. Как организовать общий доступ к Интернету? Покупается точка доступа, к которой этот ADSL-модем и подключается. Ноутбуки (беспроводные клиенты) будут подключаться к Интернету по Wi-Fi, а точка доступа выступит в роли маршрутизатора.

### 3.4. Дополнительные сетевые устройства

Представим, что у нас есть два (или более) обычных (настольных) компьютера и одно ADSL-соединение. И нужно обеспечить общий доступ к Интернету. Это можно сделать средствами Windows. Тогда в один компьютер надо будет установить дополнительный сетевой адаптер. Первый сетевой адаптер будет использоваться

для подключения к Интернету, а второй — для подключения к локальной сети (для связи с остальными компьютерами сети). Компьютер с двумя сетевыми адаптерами для остальных компьютеров сети будет выполнять роль *шлюза* (gateway). Преимущество такого решения — дешевизна: ведь мы обеспечили общий доступ к Интернету практически без дополнительных устройств. Недостаток заключается в том, что компьютер-шлюз должен быть постоянно включен, иначе остальные компьютеры не смогут подключиться к Интернету.

Решить эту проблему можно, купив отдельное устройство, называемое *маршрутизатором* (при рассмотрении выбора точки доступа мы это устройство уже упоминали). Маршрутизатор обеспечивает передачу пакетов по заданному маршруту. В нашем случае — от локальных компьютеров к интернет-провайдеру. Таким образом, все компьютеры сети будут подключаться к центральному коммутатору, а он, в свою очередь, — к маршрутизатору. Также к маршрутизатору будет подключен и ADSL-модем.

Маршрутизаторы бывают разные. Некоторые могут выполнять роль коммутатора. Купив такой маршрутизатор, вы сократите количество активного сетевого оборудования (а значит, сэкономите деньги) до двух единиц — маршрутизатора и ADSL-модема. Если же у вас в сети компьютеров немного (2–4), можно подыскать ADSL-модем с функциями маршрутизатора. В этом случае у вас будет всего одна "коробочка" — все компьютеры сети будут подключены к этому устройству, которое, в свою очередь, будет подключено к телефонной сети. Этим вы сэкономите еще больше средств. Поэтому очень важно перед построением сети спланировать сей процесс. Хорошее планирование не только позволяет сэкономить деньги, но и время, впоследствии потраченное на дальнейшую модернизацию сети.

А теперь представим, что в нашей сети есть два (или больше, количество — не принципиально) стационарных компьютера и несколько ноутбуков. Ноутбуки было бы хорошо подключать по Wi-Fi. Стационарные компьютеры принято подключать по Ethernet (хотя бы потому, что не хочется покупать для них беспроводные адаптеры). Так вот, можно купить устройство, которое одновременно является ADSL-модемом, беспроводной точкой доступа и коммутатором. Одним из таких устройств является DSL-2640U от D-Link (далее мы рассмотрим процесс настройки этого устройства). Это устройство (рис. 3.8) позволяет объединить в сеть несколько



**Рис. 3.8.** ADSL-модем, маршрутизатор, коммутатор и беспроводная точка доступа D-Link DSL-2640U

беспроводных клиентов (это наши ноутбуки) и четыре проводных клиента. Все клиенты (как проводные, так и беспроводные) автоматически настраиваются на доступ к Интернету по совместно используемому ADSL-каналу. Кроме того, это

устройство обладает встроенным брандмауэром, что позволяет защитить вашу сеть от вторжения извне.

Простота настройки сети с помощью такого устройства просто поражает. Все, что вам нужно — это включить устройство, подключить к нему клиентов, запустить программу настройки (как это сделать, написано в руководстве по устройству) и установить базовые параметры сети, а именно: имя пользователя и пароль для ADSL-соединения, идентификатор беспроводной сети (SSID) и выбрать тип шифрования беспроводных соединений. Вот и все — сеть будет работать. Клиентов можно вовсе не настраивать — они будут автоматически настроены по протоколу DHCP (Dynamic Host Configuration Protocol, протокол динамической настройки узла).

Впрочем, у всех комбинированных устройств есть один недостаток — плохая масштабируемость. Если ваша сеть будет расти, добавить новых клиентов в нее будет сложно, а в некоторых случаях вовсе невозможно. Тогда придется покупать отдельные устройства. Например, коммутатор, к которому будут подключаться до 48 проводных клиентов, и точку доступа для подключения беспроводных клиентов. В свою очередь, точка доступа и коммутатор будут подключаться к ADSL-маршрутизатору. Хотя в сложных случаях целесообразнее использовать программный (не аппаратный) маршрутизатор — компьютер под управлением UNIX/Linux. Такой компьютер можно использовать в роли маршрутизатора и на нем запустить брандмауэр, DNS-, WWW-, FTP- и почтовый серверы.

Итак, в этой главе мы ознакомились с основными сетевыми устройствами. Следующая глава будет сугубо теоретической. Мы поговорим о том, что должен знать каждый администратор и опытный пользователь любой сети, рассмотрим модель OSI и адресацию в TCP/IP-сети.



## Глава 4



# Планирование сети

## 4.1. Важность планирования

Вспомним старую русскую пословицу "семь раз отмерь, а один раз отрежь". Она очень точно подходит к нашему случаю. Конечно, бытует мнение, что пока семь раз будете мерить, кто-то уже отрежет. Согласен, но не сейчас. Сейчас вы планируете сеть, вы — главный, и вам никто не мешает. Очень важно продумать все нюансы, связанные с построением сети. Ведь корпоративная сеть — это очень сложная система, состоящая из тысяч различных компонентов. Это в маленькой домашней сети могут быть два-три компьютера, коммутатор, модем и принтер, подключенный к одному из компьютеров (не думаю, что в домашней сети кто-то организует принт-сервер). А в корпоративной сети могут быть самые разнообразные устройства, которые некоторые домашние пользователи даже ни разу в жизни и не видели. Скажем, кто из обычных домашних пользователей видел настоящий *мейнфрейм*, *кластер* или хотя бы обычный *терминал*, подключаемый к мейнфрейму?

Очень важно ориентироваться во всем этом оборудовании. Ведь жизнь не стоит на месте — все развивается с очень большой скоростью, особенно информационные технологии. Модель маршрутизатора, которая была популярна в прошлом году, уже давно такой не является — на ее место пришла новая, с более совершенными функциями, позволяющими эффективнее использовать всю систему в целом. Поэтому прежде чем закупать оборудование для сети, нужно ознакомиться с возможностями самых последних моделей устройств, а также сравнить устройства других производителей. Вот пример: всю жизнь вы считали, что устройства фирмы AAA (не хочется делать никому никакой рекламы — ни хорошей, ни плохой) — лучшие, но вот всего полгода назад на рынке появилась компания BBB, которая начала производство устройств, которые по всем своим характеристикам превосходят устройства компании AAA. Вы привыкли к компании AAA, поэтому всеми правдами и неправдами (мол, устройство от BBB еще не проверены временем и т. д.) будете уговаривать себя остановить свой выбор на устройстве от AAA, хотя прекрасно знаете, что устройство от BBB явно превосходит его характеристиками. С одной стороны, вы правы — проверенные временем, надежные устройства обеспечивают безотказную работу сети. А с другой стороны — нет, ведь уже через полгода все будут пользоваться принципиально новыми устройствами BBB, а вы построили свою сеть на устаревшем оборудовании от AAA.