



# Самоучитель

Денис Колисниченко

# Беспроводная СЕТЬ

## дома и в офисе



Основы построения компьютерных сетей

Сети Fast Ethernet и Gigabit Ethernet

Сети Wi-Fi: 802.11a, 802.11b, 802.11g и 802.11n

GPRS-соединение с Интернетом

Настройка сети в Windows XP, Vista и Linux

Защита сети: антивирусы, брандмауэры,  
виртуальные частные сети

Интернет «из розетки» – технология Powerline  
Communication

Модернизация и повышение производительности



**Денис Колисниченко**

# **Беспроводная СЕТЬ**

***дома и в офисе***

Санкт-Петербург

«БХВ-Петербург»

2009

УДК 681.3.06  
ББК 32.973.26-018.2  
К60

**Колисниченко Д. Н.**

К60 Беспроводная сеть дома и в офисе. — СПб.: БХВ-Петербург, 2009. — 480 с.: ил. — (Самоучитель)

ISBN 978-5-9775-0427-0

Книга поможет начинающему администратору домашней или офисной сети в кратчайшие сроки развернуть, настроить или модернизировать беспроводную сеть. Кратко изложены основы компьютерных сетей. Описаны беспроводные сети стандартов 802.11a, 802.11b, 802.11g, а также новейшего стандарта 802.11n. На практических примерах показано построение сети Wi-Fi, GPRS-соединение с Интернетом, а также объединение проводной и беспроводной сети Ethernet, реализация совместного доступа к Интернету, дан обзор технологии Power Line Communication (Интернет "из розетки"). Рассмотрены вопросы защиты с помощью антивирусов, брандмауэров, и на основе технологии виртуальных частных сетей даны рекомендации по повышению производительности сети. Все настройки приведены для операционных систем Windows XP, Vista и Linux.

*Для опытных пользователей и начинающих администраторов*

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>Иины Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.03.09.

Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 38,7.

Тираж 2000 экз. Заказ №

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

Санитарно-эпидемиологическое заключение на продукцию  
№ 77.99.60.953.Д.003650.04.08 от 14.04.2008 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 978-5-9775-0427-0

© Колисниченко Д. Н., 2009  
© Оформление, издательство "БХВ-Петербург", 2009

# Оглавление

<b>Введение</b> .....	<b>1</b>
<b>ЧАСТЬ I. ОСНОВЫ ПОСТРОЕНИЯ СЕТИ</b> .....	<b>3</b>
<b>Глава 1. Классификация сетей</b> .....	<b>5</b>
1.1. Краткая история сетей .....	5
1.1.1. 1941–1975 годы.....	5
1.1.2. 1976–1982 годы.....	6
1.1.3. 1983–1989 годы.....	7
1.1.4. 1990–1995 годы.....	9
1.1.5. 1996–1999 годы.....	10
1.1.6. 2000 — наше время .....	11
1.2. Классификация сетей.....	11
1.2.1. По занимаемой территории .....	11
1.2.2. По топологии.....	12
1.2.3. По ведомственной принадлежности .....	14
1.2.4. По скорости передачи данных .....	15
1.2.5. По типу среды передачи данных.....	15
1.2.6. По способу организации взаимодействия компьютеров .....	15
<b>Глава 2. Основные сетевые устройства</b> .....	<b>16</b>
2.1. Активное и пассивное сетевое оборудование .....	16
2.2. Оборудование, необходимое для построения Ethernet-сети .....	17
2.3. Оборудование, необходимое для построения сети Wi-Fi .....	21
2.4. Дополнительные сетевые устройства .....	23
<b>Глава 3. Модель OSI и адресация в современных сетях</b> .....	<b>26</b>
3.1. Способы передачи данных .....	26
3.2. Модель OSI .....	27
3.3. Что такое протокол?.....	30
3.4. Адресация компьютеров.....	32
3.5. Система DNS .....	36

<b>ЧАСТЬ II. ПОДКЛЮЧЕНИЕ К УЖЕ СУЩЕСТВУЮЩЕЙ СЕТИ .....</b>	<b>37</b>
<b>Глава 4. Подключаемся к беспроводной сети .....</b>	<b>39</b>
4.1. Подключение к беспроводной сети в Windows XP .....	39
4.2. Подключение к беспроводной сети в Windows Vista .....	44
4.3. Подключение к сети Wi-Fi в Linux .....	56
4.3.1. Простая настройка (Ubuntu 8.10/Denix/Fedora 10) .....	57
4.3.2. "Тяжелый случай" .....	59
<b>Глава 5. Подключаемся к Ethernet-сети.....</b>	<b>64</b>
5.1. Физическое подключение к сети .....	64
5.2. Настройка сети в Windows XP .....	66
5.3. Настройка сети в Windows Vista.....	68
5.4. Настройка сети в Linux.....	72
5.4.1. Fedora 10.....	72
5.4.2. openSUSE 11.....	80
5.4.3. Ubuntu 8.10.....	84
<b>Глава 6. Выбор соединения. Соединение с Интернетом в Windows .....</b>	<b>89</b>
6.1. Модемное соединение .....	89
6.1.1. Выбор модема .....	91
6.1.2. Подключение модема.....	93
6.1.3. Настройка модемного соединения в Windows XP .....	94
6.1.4. Настройка модемного соединения в Windows Vista.....	105
6.2. DSL-соединение .....	115
6.2.1. Основная причина популярности: дешево и быстро.....	115
6.2.2. Настройка ADSL-соединения в Windows XP .....	117
6.2.3. Настройка ADSL-соединения в Windows Vista.....	120
6.3. Альтернативные способы подключения к Интернету .....	123
6.3.1. Выделенная линия .....	123
6.3.2. Беспроводное подключение и Radio Ethernet .....	124
6.3.3. Спутниковое подключение.....	124
6.4. Правильное завершение работы в Интернете .....	125
6.5. Решение некоторых проблем.....	126
<b>Глава 7. Соединение с Интернетом в Linux.....</b>	<b>129</b>
7.1. Модемное соединение .....	129
7.1.1. Подключение модема.....	129
7.1.2. Программа KPPP .....	130
7.1.3. Программа GNOME PPP.....	136
7.1.4. Программа KInternet: модемное соединение в openSUSE.....	139
7.1.5. Настройка модемного соединения в Ubuntu.....	144

7.2. DSL-соединение .....	146
7.2.1. Настройка DSL-соединения в Fedora.....	146
7.2.2. Настройка DSL-соединения в openSUSE .....	148
7.2.3. Настройка DSL-соединения в Ubuntu.....	152
<b>Глава 8. GPRS-соединение с Интернетом .....</b>	<b>157</b>
8.1. Особенности GPRS-подключения .....	157
8.2. Подключаем мобильный телефон к компьютеру .....	158
8.3. Подготовка к настройке соединения.....	159
8.4. Настройка GPRS-соединения в Windows XP .....	160
8.5. Настройка GPRS-соединения в Windows Vista .....	171
8.6. Подключение мобильного телефона к ноутбуку по Bluetooth .....	177
8.7. Тонкости настройки: подробно о строке инициализации.....	183
<b>ЧАСТЬ III. ПОСТРОЕНИЕ ETHERNET-СЕТИ .....</b>	<b>185</b>
<b>Глава 9. Планирование сети .....</b>	<b>187</b>
9.1. Важность планирования .....	187
9.1.1. Планирование как основа безопасности .....	188
9.1.2. Построение транспортной системы корпоративной сети.....	190
Транспортная инфраструктура .....	190
Магистраль для корпоративной сети.....	191
Быстрый и экономичный доступ удаленных пользователей к сети компании .....	191
Помните о Wi-Fi.....	192
9.2. Обеспечение безопасности сети .....	192
9.2.1. Защита данных, передаваемых по публичным каналам связи.....	192
9.2.2. Выдача IP-адресов по рабочим местам .....	193
9.2.3. Привязка IP-адресов к MAC-адресам .....	193
9.2.4. Антивирусные серверные решения .....	194
9.2.5. Антивирусные клиентские решения.....	194
9.2.6. Необходим ли дежурный администратор?.....	194
9.3. Человеческий фактор .....	194
9.3.1. Ограничение доступа .....	195
9.3.2. Как быть с обиженными или уволенными сотрудниками?.....	195
9.3.3. Принцип "правая рука не знает, что делает левая" .....	195
9.3.4. Планирование безопасности серверной комнаты/этажа .....	196
9.4. Отдел системного администрирования и безопасности.....	196
9.4.1. Подбор персонала.....	196
9.4.2. Инструктаж отдела IT .....	197

9.4.3. Распределение задач и сфер ответственности .....	197
9.4.4. Контроль работы и иерархия .....	198
9.5. Программы для планирования сети .....	199
<b>Глава 10. Монтаж Ethernet-сети .....</b>	<b>200</b>
10.1. Развитие стандарта Ethernet .....	200
10.1.1. Модификации стандарта Ethernet .....	201
10.1.2. Стандарты Fast Ethernet (100 Мбит/с) .....	202
10.1.3. Gigabit Ethernet (1000 Мбит/с) .....	203
10.1.4. Наше будущее — 10 Gigabit Ethernet .....	204
10.2. Несколько слов о коллизиях .....	205
10.3. Монтаж сети .....	206
10.3.1. Основные компоненты Ethernet-сети .....	206
10.3.2. Подробнее о витой паре .....	208
Категории витой пары .....	208
Классификация витой пары по типу защиты .....	209
10.3.3. Обжим витой пары .....	209
Прямой кабель, Fast/Gigabit Ethernet .....	210
Перекрестный кабель (кроссовер) для соединения 100 Мбит/с .....	211
Перекрестный кабель (кроссовер) для соединения 1000 Мбит/с .....	211
Проверка правильности обжима кабеля .....	212
10.4. Ограничения при построении сети .....	212
<b>Глава 11. Общие папки и принтеры сети Microsoft .....</b>	<b>215</b>
11.1. Рабочие группы или домен? .....	215
11.2. Задание имени рабочей группы .....	217
11.2.1. В Windows .....	217
11.2.2. В Linux .....	219
11.3. Предоставление доступа к файлам и папкам в Windows XP .....	220
11.3.1. Простой способ — через учетную запись <i>Гость</i> .....	220
11.3.2. Сложный способ — по паролю .....	225
Общий пароль для учетной записи <i>Гость</i> .....	226
Создание пользователей и разрешение доступа к ресурсам определенным пользователям .....	227
11.4. Общий доступ в Windows Vista .....	233
11.5. Общий доступ к папкам в Linux .....	237
11.6. А нужен ли общий доступ к ресурсам в сети Microsoft? .....	238
<b>Глава 12. Совместное подключение к Интернету .....</b>	<b>241</b>
12.1. Небольшая домашняя сеть с выходом в Интернет .....	241
12.1.1. Основы маршрутизации .....	241
12.1.2. Преобразование сетевых адресов (NAT) .....	243

12.2. Аппаратный или программный маршрутизатор? .....	244
12.3. Настройка совместного доступа к Интернету .....	247
12.3.1. Установка дополнительного сетевого адаптера .....	247
12.3.2. Работаем в Windows XP .....	250
12.3.3. Работаем в Windows Vista .....	255

## **ЧАСТЬ IV. ПОСТРОЕНИЕ БЕСПРОВОДНОЙ СЕТИ .....261**

### **Глава 13. Введение в беспроводные сети .....263**

13.1. Преимущества и недостатки беспроводной сети .....	263
13.2. Зачем здесь теория? .....	265
13.3. Основные принципы работы беспроводной сети .....	266
13.4. Расширение спектра .....	268
13.5. Современные беспроводные службы передачи данных .....	269
13.5.1. Wi-Fi .....	269
13.5.2. WiMAX .....	273
13.5.3. Сотовые сервисы .....	273
13.5.4. Не забудем и о Bluetooth .....	274
13.6. Принципы работы Wi-Fi .....	274
13.6.1. Физический и канальный уровни Wi-Fi .....	274
13.6.2. Радиочастоты и каналы Wi-Fi .....	276
Стандарты 802.11b и 802.11g .....	276
Стандарт 802.11a .....	278
13.6.3. Режимы работы сети .....	278

### **Глава 14. Выбор оборудования для беспроводной сети .....280**

14.1. Основные сетевые устройства беспроводной сети .....	280
14.2. Выбор сетевых адаптеров .....	282
14.2.1. Форм-фактор .....	282
14.2.2. Поддерживаемые беспроводные стандарты .....	284
14.2.3. Тип антенны .....	285
14.2.4. Совместимость с операционной системой компьютера .....	285
14.2.5. Комбинированные адаптеры .....	286
14.3. Установка беспроводного адаптера .....	286
14.4. Выбор точки доступа .....	287
14.4.1. Поддерживаемые точкой доступа стандарты .....	288
14.4.2. Область применения и радиус действия точки доступа .....	288
14.4.3. Антенна точки доступа .....	289
14.4.4. Алгоритм шифрования .....	290
14.4.5. Дополнительные функции .....	290
14.4.6. Загадочный стандарт 802.11g+ .....	292

<b>Глава 15. Настройка беспроводной сети .....</b>	<b>294</b>
15.1. Выбор расположения точки доступа.....	294
15.2. Схемы сети.....	296
15.3. Точка доступа с точки зрения протокола TCP/IP.....	298
15.4. Физическая установка точки доступа .....	299
15.5. Практическая настройка беспроводной сети.....	300
15.5.1. Точка доступа D-Link DSL-2640U .....	300
15.5.2. Предварительная настройка .....	303
15.5.3. Настройка дополнительных параметров.....	307
15.6. Проблемы интерференции .....	313
15.7. Большая сеть: несколько точек доступа .....	314
15.8. Наружные антенны .....	314
<b>Глава 16. Решение проблем, возникающих при эксплуатации     беспроводной сети .....</b>	<b>316</b>
16.1. Компьютер не определяет беспроводной сетевой адаптер.....	316
16.2. Изменение длины преамбулы, номера канала и мощности передатчика беспроводной сети .....	317
16.3. Проблемы с присоединением к публичной сети.....	319
16.4. Беспроводной клиент "не видит" локальную сеть.....	320
16.5. Есть доступ к локальной сети, но нет доступа к Интернету.....	320
16.6. Компьютер самопроизвольно разрывает соединение — как его восстановить .....	320
16.7. Низкое качество сигнала или слабый сигнал .....	321
16.8. Сеть работает медленно.....	321
16.9. Беспроводной сети вообще нет.....	322
<b>ЧАСТЬ V. ЗАЩИТА СЕТИ.....</b>	<b>323</b>
<b>Глава 17. Защита беспроводной сети .....</b>	<b>325</b>
17.1. Беспроводные сети небезопасны .....	325
17.2. Десять шагов к безопасной беспроводной сети .....	326
17.2.1. Изменение параметров по умолчанию .....	326
17.2.2. Отключение широковещания SSID .....	327
17.2.3. Используйте WPA или WPA2 .....	327
17.2.4. Фильтрация MAC-адресов.....	328
17.2.5. Обновление прошивки оборудования .....	329
17.2.6. Использование аутентификации .....	329
17.2.7. Понижение мощности передачи .....	331
17.2.8. Отключайте точку доступа, когда вы не работаете.....	331

17.2.9. Защита портов управления .....	332
17.2.10. Защита от внешних угроз. Общая защита сети .....	332
17.3. Дополнительная защита сети .....	332
<b>Глава 18. Виртуальные частные сети .....</b>	<b>334</b>
18.1. Предназначение VPN .....	334
18.1.1. Сценарий 1 .....	334
18.1.2. Сценарий 2 .....	335
18.1.3. Преимущества VPN .....	335
18.2. VPN-протоколы, VPN-серверы .....	338
18.3. Необходимое программное обеспечение .....	339
18.4. Настройка соединения "сеть-сеть" .....	340
18.4.1. Установка OpenS/WAN .....	340
18.4.2. Немного терминологии .....	340
18.4.3. Генерирование ключей .....	341
18.4.4. Конфигурационный файл .....	341
18.4.5. Установка VPN-соединения .....	345
18.4.6. Настройка утилиты <i>iptables</i> .....	345
18.5. Настройка соединения "клиент-сеть" .....	345
18.5.1. Редактирование конфигурационных файлов .....	346
18.5.2. Настройка Linux-клиента .....	348
18.5.3. Настройка Windows-клиента .....	349
<b>Глава 19. Антивирусы и брандмауэры .....</b>	<b>355</b>
19.1. Windows — под прицелом .....	355
19.2. Выбор антивируса .....	360
19.3. Выбор брандмауэра .....	361
19.3.1. Брандмауэр для Windows .....	362
19.3.2. Брандмауэр для Linux .....	367
19.4. Использование программ AVZ и CureIt .....	372
19.4.1. Антивирус AVZ .....	372
19.4.2. Утилита CureIt .....	375
19.4.3. Создание и использование проверочных компакт-дисков .....	375
19.5. Отключение потенциально опасных служб .....	375
<b>Глава 20. Защита маршрутизатора .....</b>	<b>378</b>
20.1. О маршрутизаторе .....	378
20.2. Установка пароля .....	379
20.3. Ограничение доступа по сети .....	379
20.4. Только локальный доступ .....	380
20.5. Защита SNMP .....	380

20.6. Ведение журналов.....	380
20.7. Отключение ненужных сервисов.....	381
20.8. Ограничение протокола ICMP.....	381
20.9. Отключение потенциально опасных опций.....	381
20.10. Anti-spoofing и защита от DoS-атак.....	382
20.11. Отключение CDP.....	383
20.12. Вместо заключения.....	383

## **ЧАСТЬ VI. POWERLINE — ИНТЕРНЕТ "ИЗ РОЗЕТКИ" .....385**

### **Глава 21. Обзор технологии Power Line Communication.....387**

21.1. Почти беспроводная технология.....	387
21.2. Технология PLC и ее стандарты.....	388
21.3. PLC и Wi-Fi.....	389
21.4. Преимущества и недостатки PLC-сетей.....	390
21.5. Стоит ли использовать PLC?.....	392

### **Глава 22. Построение PLC-сети .....394**

22.1. Обзор PLC-адаптеров от ZyxEL.....	394
22.1.1. Адаптер PLA400.....	396
22.1.2. Адаптер PLA470.....	397
22.1.3. Интернет-центры P660HWP и NBG318S.....	398
22.1.4. Устройство DMA1100P.....	399
22.2. Подключение и настройка PLC-сети.....	401

## **ЧАСТЬ VII. ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ СЕТИ .....405**

### **Глава 23. Факторы повышения производительности сети .....407**

23.1. Модернизация старой сети.....	407
23.1.1. Сети 10Base на коаксиальном кабеле.....	407
23.1.2. Сети 10Base на витой паре.....	407
23.1.3. Сети Fast Ethernet.....	408
23.2. Служба QoS.....	409
23.3. Оптимизация сети с помощью реестра Windows.....	411
23.3.1. Повышение производительности локальной сети.....	411
23.3.2. Повышение производительности Интернета.....	411
23.4. Кэширующие серверы: DNS и прокси.....	412

### **Глава 24. DNS-сервер.....414**

24.1. Еще раз о том, что такое DNS.....	414
24.2. Кэширующий сервер DNS.....	415

24.3. Полноценный DNS-сервер .....	419
24.4. Вторичный DNS-сервер .....	424
<b>Глава 25. Прокси-сервер Squid.....</b>	<b>425</b>
25.1. Зачем нужен прокси-сервер в локальной сети?.....	425
25.2. Базовая настройка Squid .....	426
25.3. Практические примеры настройки.....	427
25.3.1. Управление доступом.....	427
25.3.2. Создание "черного" списка URL.....	428
25.3.3. Отказ от баннеров.....	428
25.4. Управление прокси-сервером .....	429
25.5. Настройка клиентов .....	429
25.6. Прозрачный прокси-сервер .....	430
25.7. Расширение squidGuard .....	431
<b>Глава 26. DHCP-сервер для вашей сети .....</b>	<b>434</b>
26.1. Протокол динамической конфигурации узла.....	434
26.2. Конфигурационный файл DHCP-сервера .....	435
26.3. База данных аренды .....	437
26.4. Полный листинг конфигурационного файла.....	437
26.5. Управление сервером DHCP .....	438
26.6. Настройка клиентов .....	438
<b>Глава 27. Виртуальная локальная сеть.....</b>	<b>439</b>
27.1. Виртуальность .....	439
27.2. Зачем нужны виртуальные сети?.....	439
27.3. Метим трафик.....	440
27.4. Порты и VLAN .....	441
27.5. Практика настройки VLAN на коммутаторах Cisco.....	442
27.6. Другие производители оборудования .....	446
27.7. Настройка VLAN в Linux .....	447
27.8. VLAN в Windows: миф или реальность? .....	448
27.9. Где применяется VLAN? .....	449
27.10. Вместо заключения .....	449
<b>Заключение.....</b>	<b>451</b>
<b>Предметный указатель .....</b>	<b>453</b>

## Глава 2



# Основные сетевые устройства

## 2.1. 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 Wi-Fi-сетей.

## 2.2. 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. 2.1 изображен так называемый *промышленный* коммутатор от Linksys.

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. 2.2 изображена типичная стойка с коммутаторами.



Рис. 2.1. 16-портовый коммутатор от Linksys

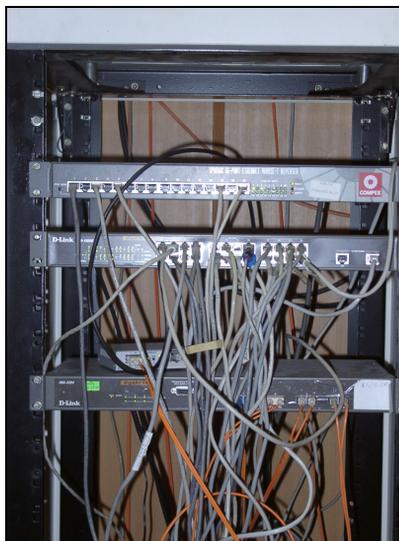


Рис. 2.2. Стойка с коммутаторами

А на рис. 2.3 изображен 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.



**Рис. 2.3.** Шкаф с сетевым оборудованием



**Рис. 2.4.** 8-портовый гигабитный коммутатор от D-Link

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. 2.4 изображен 8-портовый гигабитный коммутатор от D-Link. Вид у него более "дружелюбный", но в стойку его уже не поместишь, хотя 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 имеет 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. 2.1).

**Таблица 2.1.** 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 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 концентраторов, 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 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 магистрали сети, работающей со скоростью 1000 Мбит/с. Иногда вместо порта 1000Base-T оборудуется оптоволоконный порт, например, 100Base-FB. В этом случае скорость магистрали 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).

## 2.3. 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. 2.5 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. 2.6). 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. 2.6. 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. 2.5. 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. 2.5.** USB Wi-Fi-адаптер со встроенной антенной



**Рис. 2.6.** USB Wi-Fi-адаптер с внешней антенной



**Рис. 2.7.** Точка доступа от D-Link с тремя антеннами

Точка доступа (рис. 2.7) выполняет в беспроводной сети роль центрального устройства. Казалось бы, все здесь просто: устанавливаем Wi-Fi-адаптеры, подсоединяем 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 определить, 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.

## 2.4. 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.