

**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<br>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<br>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<br/>    беспроводной сети .....</b>   | <b>316</b> |
| 16.1. Компьютер не определяет беспроводной сетевой адаптер.....                                  | 316        |
| 16.2. Изменение длины преамбулы, номера канала и мощности<br>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 —<br>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> |

# Введение

Эта книга посвящена построению сети для дома и офиса. С одной стороны, построение сети — занятие не очень сложное и под силу пользователю средней квалификации. С другой стороны, есть определенные нюансы, разобраться в которых мы здесь и постараемся. Приведу простейший пример. С удешевлением беспроводных технологий вы решили, что ваша сеть будет беспроводной. Правильно: зачем тянуть кабели, обжимать витую пару, если можно купить точку доступа, включить ее — и сеть готова. Казалось бы, ничего сложного в этом нет. Однако пользователь, создавший сеть таким вот способом, обнаружит, что его сеть или вообще не работает, или работает медленно, или доступ к ней получил кто-то посторонний. В первом случае причина, скорее всего, в неправильной настройке точки доступа. Во втором — в интерференции сигналов. В третьем — в пренебрежении основными правилами безопасности. Какими правилами? Что такое интерференция сигналов? Как правильно настроить точку доступа? Обо всем этом вы здесь и узнаете.

- В *первой части* книги мы рассмотрим сугубо теоретические вопросы. Вы познакомитесь с краткой историей и классификацией сетей, с основными сетевыми устройствами и так называемой *моделью взаимодействия открытых систем* (Open System Interconnection, OSI) — базовым сетевым стандартом. Настоятельно рекомендую вам не пропустить *главу 3*, в которой модель OSI подробно описана, — в последующих главах книги мы не раз будем к ней обращаться.
- Во *второй части* мы поговорим о подключении к уже существующей сети. Поскольку я более чем уверен, что у вас именно беспроводная сеть (ну, или смешанная, где есть как беспроводные, так и проводные подключения), то эта часть книги начинается именно с рассмотрения подключения к беспроводной сети. Затем мы рассмотрим подключение к сети Ethernet, а после него — подключение к Интернету в Windows и Linux. Отдельная глава посвящена GPRS-подключению — одному из вариантов беспроводного подключения к Интернету.

- *Третья часть* книги посвящена построению Ethernet-сети. Ведь ни для кого не секрет, что абсолютно беспроводные сети — редкость (если не считать ad hoc-сети или сети из одной точки доступа и одного-двух компьютеров). Чаще всего в современной сети есть как беспроводные, так и проводные клиенты. И построение такой смешанной сети принято начинать с проводной части, а уже потом "прикручивать" точку доступа — как правило, беспроводная сеть является расширением существующей проводной сети. Особое внимание здесь будет уделено предоставлению общего сетевого доступа к файлам и принтерам, а также общему доступу к Интернету (*главы 11 и 12* соответственно). Чтобы не усложнять изложение, мы рассмотрим монтаж домашней и офисной сети небольшого и среднего размеров, а построение огромных корпоративных сетей оставим "за скобками".
- В *четвертой части* мы поговорим о построении собственной беспроводной сети (наконец-то!). Мы рассмотрим основные теоретические принципы (как именно данные передаются "по воздуху"), разберемся с беспроводными стандартами, поговорим о выборе оборудования и, конечно же, построим собственную беспроводную сеть. Отдельное внимание будет уделено решению проблем, возникающих при настройке беспроводной сети.
- Защита вашей сети — довольно ответственное занятие, поэтому ей посвящена *пятая часть* книги. Мы поговорим о том, как можно защитить беспроводную сеть в целом и конкретно маршрутизатор в частности, рассмотрим использование виртуальной частной сети (VPN) для защиты информации, а также разберемся с выбором брандмауэра и антивируса (все антивирусы хороши, но есть и лучшие).
- Последняя, *шестая*, часть книги посвящена повышению производительности нашей сети. Здесь кроме модернизации старой сети будет рассмотрена также установка серверов, позволяющих повысить производительность сети в целом.

Ну, а теперь можно приступить к чтению книги.



# Часть I

## ОСНОВЫ ПОСТРОЕНИЯ СЕТИ

В первой части книги мы рассмотрим краткую историю сетей, модель взаимодействия OSI и разберемся, для чего предназначены основные сетевые устройства.



# Глава 1

## Классификация сетей

### 1.1. Краткая история сетей

С появлением первых электронно-вычислительных машин (не персональных компьютеров, а именно первых огромных вычислительных машин, которые занимали целые комнаты) возникла проблема переноса данных между ними. С того момента было создано много различных сетей. Сейчас мы вкратце рассмотрим историю сетей, чтобы вы знали, откуда они появились, а потом попробуем классифицировать все имеющиеся виды сетей.

#### 1.1.1. 1941–1975 годы

*Первый период* развития вычислительных сетей начинается в 1941 году (тогда, если вы помните, появилась первая "большая" ЭВМ) и называется *лабораторным* — в то время сети, как впрочем и ЭВМ, не выходили за пределы лабораторий научных институтов. Казалось бы, как давно это было! Но самое интересное, что мы до сих пор используем решения, разработанные в то время. Последовательный интерфейс RS-232C и параллельный интерфейс Centronics (да, тот, который служит для подключения принтеров) используются до сих пор. Интерфейс RS-232C постепенно вытесняется современными последовательными интерфейсами: USB и IEEE 1394 (FireWire), и на некоторых современных компьютерах его больше нет вообще. Однако интерфейс Centronics имеется на каждом современном стационарном компьютере, хотя большинство производителей принтеров уже практически перешло на USB. Наличие "старых" интерфейсов зависит только от производителя материнской платы — как он решит, так и будет. Мой компьютер, на котором я пишу эти строки, был куплен в феврале 2008 года. Тогда я не обратил внимания на наличие/отсутствие старых интерфейсов, но потом выяснилось, что на материнской плате отсутствует RS-232C, но есть Centronics, а также USB, IEEE 1394, HDMI (правда, он не имеет никакого отношения к сетевым интерфейсам)

и другие современные разъемы, которых не было на более старых компьютерах. С другой стороны, в продаже до сих пор имеются материнские платы с RS-232C, а также предлагаются отдельные PCI-контроллеры, добавляющие два порта RS-232C, если в них возникает острая необходимость.

Интерфейсы RS-232C и Centronics — это, в принципе, хорошо, но они годятся только для связи "точка-точка", то есть для непосредственной связи отправителя и получателя данных. Понятно, что в сети может быть ЭВМ гораздо больше чем две, поэтому разработчики сетей на этом не остановились. С самого начала ставилась задача объединения в сеть ЭВМ без привязки к конкретной аппаратуре.

В 1974 году компания IBM представила универсальную архитектуру вычислительных сетей: SNA (System Network Architecture). Эта архитектура, помимо всего прочего, поддерживала *адресацию узлов* сети, смысл которой в том, что каждому узлу сети присваивается уникальный адрес, по которому можно обратиться к этому узлу. Сейчас для адресации узлов преимущественно используются протоколы IPv4 и IPv6, о которых мы поговорим в *главе 3*.

### 1.1.2. 1976–1982 годы

*Второй период* развития сетей начался в 1976 году, когда сети вышли за пределы лабораторий и начали активно разрабатываться сетевые архитектуры и технологии передачи данных. Тогда и появилось семейство протоколов X.25 — протоколов передачи данных в системах с коммутацией пакетов. Разработка протоколов X.25 стала очень важным событием, поскольку до появления Интернета они были единственными протоколами, используемыми для создания глобальных сетей, — именно X.25-сети связывали весь мир в единое целое. Далее на базе X.25 был создан протокол Frame Relay, а на его базе — технология АТМ. Подробно рассматривать все производные протоколов X.25 мы не будем, поскольку нас сейчас интересуют только ключевые события в развитии сетей (описание истории появления каждого сетевого протокола займет целую книгу, прочитать которую у вас не хватит терпения). Отмечу только, что Frame Relay, как и АТМ, здравствуют и по сей день.

В 1979 году был создан первый модем для персональных (!) компьютеров. Я даже догадываюсь о чем вы сейчас подумали: какие, мол, персональные компьютеры в 1979 году? Какой модем? Да, Personal Computer (PC) от IBM появился в 1981 году, но это не означает, что до этого не было *персональных компьютеров*. Персональный компьютер — это компьютер, предназначенный только для одного человека, для одного пользователя. Для работы с первыми ЭВМ обычно требовался целый штат специалистов, а настоящие персональные компьютеры появились еще до 1980 года — это были компью-



теры компании Apple. А то, что появилось в 1981 году, — всего лишь название продукта компании IBM. Конечно, IBM первая ввела термин PC (Personal Computer), и с того времени все компьютеры со сходной архитектурой команд считаются PC-совместимыми.

А все современные модемы являются Hayes AT-совместимыми. AT — это набор команд управления модемом, разработанный компанией Hayes. Несложно догадаться, что в 1979 году первый модем был разработан именно компанией Hayes. Он назывался Micromodem II и развивал скорость в 300 бод (бит/с). Этот модем и был предназначен для компьютеров Apple.

Еще в лабораторном периоде были разработаны *системы с произвольным доступом*. Впервые они были использованы в начале 1970-х годов в сети Alohanet, объединяющей Гавайские острова. Сначала эти системы считались бесперспективными, но в мае 1973 года Боб Меткалф (Bob Metcalf) усовершенствовал метод CSMA, на котором они были основаны. Усовершенствованный метод назвали CSMA/CD (Carrier-Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий). Боб Меткалф планировал использовать этот метод для совместного доступа к сетевым принтерам, но он позже "перерос" в то, что сейчас называется Ethernet-сетью. Тогда сеть CSMA/CD передавала данные по коаксиальному кабелю (как первые Ethernet-сети) со скоростью 2,94 Мбит/с (для того времени это была значительная скорость), а максимальное расстояние передачи данных составляло 1,5 км. В 1978 году Меткалф зарегистрировал копию ZCom Corporation (наверное, все мы слышали название этой компании), а в 1982 году выпустил первый в мире серийный Ethernet-адаптер для компьютера Apple.

В 1979 году произошло еще одно важное событие — был организован альянс DIX (DEC, Intel, Xerox), результатом деятельности которого стала в 1980 году разработка стандарта Ethernet.

В 1980 году была разработана *модель взаимосвязи открытых систем* (Open System Interconnect, OSI), которую мы подробно рассмотрим в *главе 3*. Эта модель четко определяет семь уровней, которые обеспечивают передачу данных по сети. Модель OSI сугубо теоретическая, но она лежит в основе всех современных сетей.

### 1.1.3. 1983–1989 годы

Начиная с 1983 года, в институтах и даже некоторых офисах стали появляться первые локальные сети, связывающие компьютеры толстым коаксиальным кабелем. В то время сетевой адаптер стоил очень дорого (например,

для ЭВМ VAX стоимость сетевого адаптера превышала 3 тыс. долларов), поэтому локальную сеть могли себе позволить только самые крупные фирмы. Найти тогда "персоналку" с сетевым адаптером было сложно.

В 1985 году Институтом инженеров по электротехнике и электронике (IEEE) был принят стандарт IEEE 802.3 (10Base-5) — Ethernet-сеть на "толстом" коаксиальном кабеле. В 1989 году был принят стандарт IEEE 802.3a (10Base-2), предусматривающий передачу данных по "тонкому" коаксиальному кабелю. Подробно о стандартах Ethernet мы поговорим чуть позже в этой книге.

Понятно, что Ethernet-сети — не единственный вид локальной сети. В 1988 году IBM превзошла стандарт Ethernet, представив технологию Token Ring с максимальной скоростью передачи данных в 16 Мбит/с (Ethernet предусматривал передачу данных с максимальной скоростью в 10 Мбит/с).

В 1985 году компания StrataCom начала эксплуатацию первых линий T1 со скоростью передачи данных 1,54 Мбит/с. Чуть позже линии T1 стали доступны крупным компаниям и использовались в качестве магистралей для быстрой передачи данных на большие расстояния.

Индивидуальным пользователям в 1980-х годах сети "особо не светили", поскольку сетевое оборудование продолжало стоить весьма дорого. Так, в 1989 году компания Arc Electronics представила высокоскоростной модем (19,2 Кбит/с) стоимостью "всего" 3595 долларов. Интересно, что этот модем был относительно дешевле модемов других производителей, которые, к тому же, не обеспечивали достигаемой им скорости.

Кто мог позволить себе сети ISDN, радовался скорости передачи данных в 128 Кбит/с (сети ISDN BRI) или 1,54 Мбит/с (ISDN PRI). О цене говорить не будем — ISDN-сети стоили неприлично дорого.

Технологии — это, конечно, хорошо. Но сетевые адаптеры и прочее сетевое оборудование без программного обеспечения — просто железки. Чтобы компьютер мог работать в сети, нужна сетевая операционная система. В 1980-х годах сеть поддерживали следующие ОС: UNIX (и ее вариации), Novell Netware, Microsoft LAN Manager (оболочка для OS/2, появившаяся в 1987 году).

В 80-х годах прошлого века появились и первые сотовые сети — да, сотовая телефония! Первая система сотовой телефонной связи Nordic Mobile Telephone System (кто помнит — первые "мобилки", появившиеся у нас в 1990-х годах, поддерживали стандарт NMT) была запущена в Дании, Швеции, Финляндии и Норвегии в 1981 (!) году. В 1983 году заработали две сотовые сети в Северной Америке: AURORA-400 и AMPS.

### 1.1.4. 1990–1995 годы

В 1990 году произошел очередной "переворот" в Ethernet-сетях — был принят стандарт IEEE 802.3i (10Base-T), предусматривающий передачу данных по витой паре 3-й категории со скоростью 10 Мбит/с. Переворот заключался в том, что Ethernet-сети стали:

- *надежнее* — при использовании коаксиального кабеля все компьютеры подключались к общему кабелю, и если этот кабель обрывался, то вся сеть "падала". В случае с витой парой все компьютеры сети подключаются к центральному устройству сети — Ethernet-концентратору. Если происходит обрыв кабеля, ведущего к какому-нибудь узлу сети, этот узел исчезает из сети, но вся сеть продолжает работать;
- *проще в установке* — монтаж витой пары намного проще, чем коаксиального кабеля, особенно, если речь идет о "толстом" коаксиальном кабеле.

Позднее был принят стандарт IEEE 802.1D, в котором было определено понятие *моста* (bridge), и Ethernet-сети наконец-то стало можно делить на сегменты для локализации трафика. Сегментация сети особо важна для крупных сетей — ведь чем больше узлов, тем меньше производительность сети.

Через три года сети того времени стали напоминать уже современные сети — в них активно начали использоваться концентраторы и мосты, появились первые коммутаторы и двухуровневые сети. В двухуровневых сетях компьютеры одной рабочей группы (одного отдела компании) объединялись между собой концентратором, а сами рабочие группы (то есть концентраторы рабочих групп) подключались через мосты к общей корпоративной магистрали. В качестве магистрали обычно использовалось оптоволокно (стандарт 10Base-FL или IEEE 802.3j, принятый в 1993 году). С появлением 10Base-FL на оптоволокне Ethernet-сети выходят за пределы зданий и становятся средством для создания "кампусных" сетей. То есть если раньше Ethernet-сети использовались только для создания локальных сетей, то в 1994–1995 годах стандарт 10Base-FL применялся для связи локальных сетей, находящихся в разных зданиях.

Следующим шагом в создании корпоративных сетей стало изобретение многопортового устройства — центрального коммутатора, в котором были объединены все мосты сети. Такая конфигурация получила название collapsed-backbone ("магистраль в точке"). Примерно в это же время родилось понятие *структурированных кабельных сетей* (СКС).

Понятно, что сети росли и что скорости 10 Мбит/с для магистрали стало недостаточно. На тот момент существовала всего одна "быстрая" технология, обеспечивающая передачу данных по оптоволоконному кабелю со скоростью

100 Мбит/с — FDDI (Fiber Distributed Data Interface — распределенный волоконный интерфейс данных). Но в 1992 году компания Grand Junction начала разработку Ethernet-сети, работающей на скорости 100 Мбит/с, и она была стандартизирована в 1995 году (стандарт IEEE 802.3u, сети 100Base-TX, 100Base-T4 и 100Base-FX). В том же 1995 году компания Grand Junction была поглощена компанией Cisco Systems: закон выживания — выживают лишь сильнейшие. После принятия стандартов 100Base-\* спрос на технологию FDDI резко пошел вниз, поскольку Ethernet-сети обеспечивали ту же скорость передачи данных, но стоили намного дешевле только за счет среды передачи данных — витая пара стоит намного дешевле, чем оптоволокно. А в 1998 году появились Ethernet-сети, передающие данные со скоростью 1 Гбит/с, но об этом позже.

А что же происходило в мире глобальных сетей? В 1990 году компания US Sprint начала предоставлять услуги объединения точек через Frame Relay по всей территории США. Тогда почти все высокоскоростные магистрали переводились на технологию ATM, но для подключения клиентов использовался Frame Relay. Однако в 1994 году компания Bell Atlantic начинает предлагать подключение клиентов по технологии ATM.

Не стоит забывать и об операционных системах. В 1993 году появилась первая действительно сетевая ОС от Microsoft — Windows NT, а в 1995 году — нашумевшая ОС Windows 95.

### 1.1.5. 1996–1999 годы

В эти годы ничего революционного в магистральных каналах связи не случилось, если не считать появления сервисов гарантирования качества обслуживания (QoS, Quality of Service). Но нас интересуют технологии, более близкие к пользователю. Можно сказать, что в эти годы (1995–1999) завершилась эра развития аналоговых модемов. В 1998 году был принят стандарт V.90, который используется и по сей день (если не считать его небольшого усовершенствования V.92, появившегося в 2000 году). Судя по всему, телефонные модемы отжили свое. Сегодня все больше и больше провайдеров предоставляют высокоскоростной доступ к Интернету, а обычные аналоговые модемы практически уже не используются.

Зарождение высокоскоростного доступа произошло как раз в 1995–1999 годах, когда появились первые кабельные и ADSL-модемы. Кабельные модемы (они передают данные по сетям операторов кабельного телевидения) преимущественно применялись в США. В Европе получили большее распространение ADSL-модемы, использующие для передачи данных обычный

телефонный кабель. К сожалению, в те годы в России о таких модемах только слышали, но никто их практически не видел.

В мире локальных сетей в 1998 году появилась технология 1000Base-X, передающая данные со скоростью 1 Гбит/с по оптоволокну, а в 1999 году — технология 1000Base-T, передающая данные со скоростью 1 Гбит/с по витой паре.

### 1.1.6. 2000 — наше время

Понятно, что развитие сетей не останавливается, а только начинается. Все еще впереди. Лет через десять все современные технологии будут казаться нам такими же "древними", какими сейчас кажутся решения 20-летней давности.

Из интересного в мире Ethernet можно отметить появление в 2003 году технологий передачи данных со скоростью 10 Гбит/с (10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-SW, 10GBase-LW, 10GBase-EW) и технологии PLC, обеспечивающей передачу данных по сети электропитания. В 2003 году это казалось странным, но сейчас — вполне нормально.

Если вы заметили, то в этой краткой истории практически ничего не было сказано о развитии беспроводных сетей. Это сделано умышлено. В *главе 9* мы поговорим о том, как данные передаются "по воздуху", рассмотрим краткую историю беспроводных сетей и существующие беспроводные стандарты.

## 1.2. Классификация сетей

Сети можно классифицировать по:

- занимаемой территории;
- топологии;
- ведомственной принадлежности;
- скорости передачи данных;
- типу среды передачи данных;
- организации взаимодействия компьютеров.

### 1.2.1. По занимаемой территории

По занимаемой территории сети могут быть локальными, региональными (они же муниципальные сети) и глобальными:

- локальные* (LAN, Local Area Network) — сети, занимающие небольшую территорию, например, одну комнату или одно здание;

- *региональные* (MAN, Metropolitan Area Network) — сети, охватывающие город (отсюда другое название — муниципальные) или даже область;
- *глобальные* (WAN, Wide Area Network) — такие сети охватывают территории одного или нескольких государств или даже весь мир. Пример всемирной сети — Интернет.

С локальными и глобальными сетями все понятно, разберемся с сетями региональными. Сеть MAN, как правило, объединяет несколько сетей — например, MAN может объединять в единое целое сети двух или более зданий. При этом среда передачи данных сети MAN может как проводной, так и беспроводной. Беспроводная сеть обходится намного дешевле, чем сеть на базе оптоволокну, но она менее надежна и менее безопасна.

Беспроводные технологии очень полезны для MAN — не всегда есть возможность проложить кабель. С другой стороны, MAN часто выступает в качестве магистральной сети, поэтому производительности беспроводной сети может быть недостаточно.

Сейчас особой необходимости в MAN-сетях нет, поскольку можно организовать *виртуальную частную сеть* (VPN, Virtual Private Network), использующую каналы Интернета для передачи данных. Представим следующую ситуацию: есть организация, главный офис которой находится в Москве, затем эта компания открыла свой филиал в Санкт-Петербурге. Как объединить сети офисов вместе? Вы только представьте себе, сколько кабеля для этого понадобится! Причем витой парой здесь не отделаешься, придется использовать дорогой оптоволоконный кабель — ведь расстояние-то большое. Беспроводные технологии тоже из-за расстояния отпадают. Остается только одно — использовать для передачи данных каналы Интернета. Сеть каждого офиса подключается к Интернету через каналы местного интернет-провайдера, и через Интернет создается виртуальная частная сеть. И дешево, и быстро — ведь высокоскоростное подключение к Интернету в настоящее время вполне доступно. Понятно, что данные будут передаваться по незащищенным каналам, поэтому в виртуальной частной сети используется шифрование всех передаваемых данных. Механизмы VPN позволяют не только объединить две разные сети в единое целое, но и обеспечить безопасность передаваемых данных.

### 1.2.2. По топологии

Существуют следующие топологии сети:

- *линейная* (рис. 1.1) — подключение по принципу гирлянды: каждый узел сети подключается к следующему узлу сети. В такой сети от узла с номе-

ром 1 до узла  $N$  будет всегда одинаковый маршрут: через узлы 2, 3, 4, ...,  $N - 1$ . Понятно, в случае отказа одного из узлов сети, линейная сеть прекратит свое существование. В настоящее время линейные сети практически не используются (если не принимать во внимание нуль-модемное соединение);

- *кольцевая* (рис. 1.2) — каждый узел сети соединен с двумя соседними узлами, все узлы сети образуют кольцо. Кольцевая топология используется технологиями Token Ring, FDDI и некоторыми другими;
- *звездообразная* (рис. 1.3) — в такой сети есть один центральный узел, с которым связан каждый узел сети. Такие сети еще называются *централизованными*. "Падение" центрального узла означает "падение" всей сети. Обычно в качестве центрального узла используется концентратор (hub) или коммутатор (switch). Пример звездообразной сети — Ethernet на базе витой пары;
- *общая шина* (рис. 1.4) — все узлы сети подключаются к единой среде передачи данных, например, к коаксиальному кабелю. Слабое место такой сети — сама среда передачи данных: обрыв кабеля означает сбой всей сети. Пример сети на общей шине — Ethernet на базе коаксиала;
- *древовидная* (рис. 1.5) — топологию этой сети проще представить, чем описать или вникать в определение. В древовидной сети есть более двух конечных узлов и, по крайней мере, два промежуточных узла. В древовидной сети между двумя узлами есть только один путь. Чтобы вникнуть в правильное определение древовидной сети, нужно знать теорию графов, поскольку древовидная сеть — это неориентированный ациклический граф, не содержащий замкнутых путей и позволяющий соединить единственным образом пару узлов;
- *ячеистая* (рис. 1.6) — в такой сети есть, по крайней мере, два узла, имеющих два или более пути между ними;
- *полносвязная* (рис. 1.7) — сеть, в которой есть связь между любыми двумя узлами. Это самая надежная топология сети, но она практически никогда не используется, поскольку является самой дорогой и труднообслуживаемой.

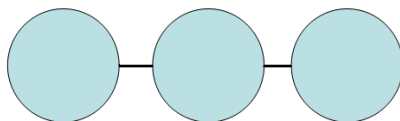


Рис. 1.1. Линейная топология

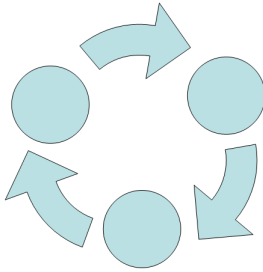


Рис. 1.2. Кольцевая топология

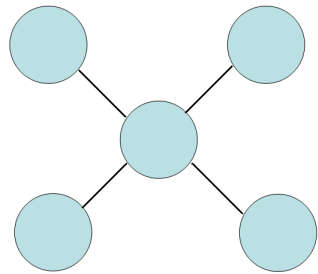


Рис. 1.3. Звезда

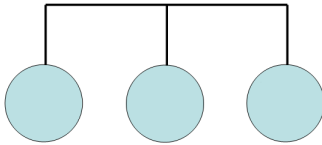


Рис. 1.4. Общая шина

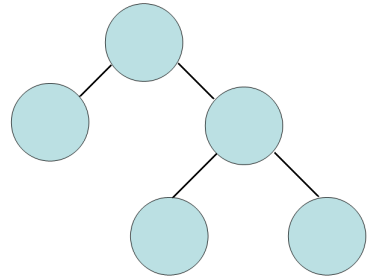


Рис. 1.5. Дрвовидная топология

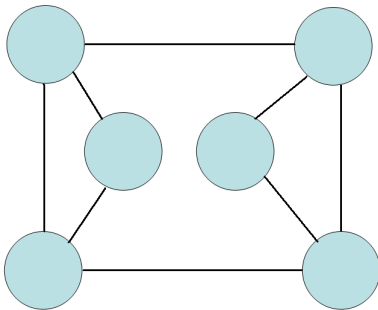


Рис. 1.6. Ячеистая топология

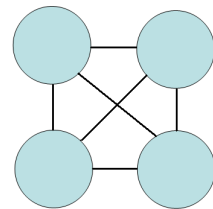


Рис. 1.7. Полносвязная топология

### 1.2.3. По ведомственной принадлежности

По ведомственной принадлежности различают следующие виды сетей:

- ведомственные* — принадлежат какой-то организации и находятся на ее территории;
- государственные* — используются в госструктурах.



### 1.2.4. По скорости передачи данных

По скорости передачи данных сети делятся на низко-, средне- и высокоскоростные. Основным критерий разделения — скорость передачи данных. Понятно, что скорость передачи данных — понятие непостоянное. То, что сегодня считается среднескоростным соединением, завтра будет отнесено к низкоскоростным. Тем не менее, сегодня низкоскоростной сетью считается сеть со скоростью передачи информации до 10 Мбит/с. Среднескоростная сеть передает данные со скоростью до 100 Мбит/с, а высокоскоростные сети передают информацию со скоростью свыше 100 Мбит/с.

### 1.2.5. По типу среды передачи данных

Казалось бы, тут все просто: сети бывают проводными или беспроводными. Но очень часто "в природе" встречаются *смешанные*, или *гибридные* сети, сочетающие как проводные, так и беспроводные технологии. В этой книге больше внимания будет уделяться именно таким сетям. Представьте, что у вас дома есть компьютер и ADSL-модем. Вы купили ноутбук. Подключать ноутбук по Ethernet-кабелю не очень-то хочется — ноутбук по своей природе мобильное устройство, и хотелось бы использовать его по всей квартире (а если у вас свой дом, то и во дворе). Поэтому вам понадобится *точка доступа*, которую вы подключите к существующей сети. Точка доступа в данном случае будет выполнять функцию моста между беспроводной и проводной сетью. Именно с ее помощью ваш ноутбук сможет подключиться к Интернету. Поэтому у вас дома появится смешанная сеть, созданная "своими руками".

### 1.2.6. По способу организации взаимодействия компьютеров

Сети бывают одноранговыми и типа клиент/сервер. В *одноранговой* сети нет выделенного сервера: каждый клиент сети может выступать как в роли сервера, то есть предоставлять услуги другим узлам сети, так и в роли клиента, то есть пользоваться услугами, которые предоставляют другие узлы сети.

В сети *клиент/сервер* есть выделенный сервер, предоставляющий определенные сетевые услуги (какие именно, зависит от самой сети).

Здесь мы остановимся, а в следующей главе поговорим об основных сетевых устройствах.



## 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

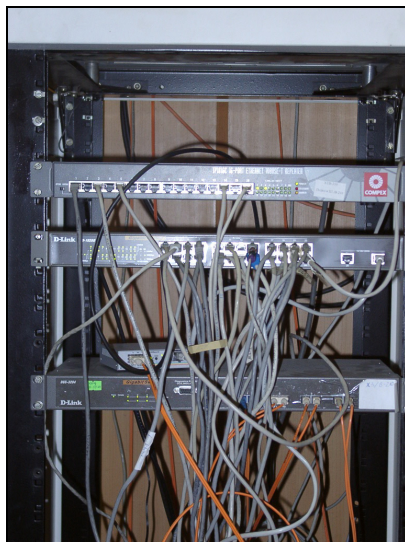


Рис. 2.2. Стойка с коммутаторами

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).