

# СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ LINUX

Характеристики и возможности  
протоколов семейства TCP/IP

Настройка сервисов и служб

Защищенный удаленный доступ

Управление сетевым трафиком

Диагностика и аудит сети  
и служб

СИСТЕМНЫЙ  
АДМИНИСТРАТОР

**Алексей Стахнов**

# **СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ LINUX**

Санкт-Петербург

«БХВ-Петербург»

2004

УДК 681.3.06  
ББК 32.973-018.2  
С78

**Стахнов А. А.**

С78 Сетевое администрирование Linux. — СПб.: БХВ-Петербург, 2004. — 480 с.: ил.

ISBN 5-94157-277-8

В книге представлены теоретические и практические знания, позволяющие хорошо понимать процессы, происходящие в сети. Рассматриваются сетевые модели, протоколы, адреса, службы, конфигурирование сетевых интерфейсов, настройка серверов FTP, Proxu, INN, Apache, Samba, Mars, обсуждается сетевая файловая система, взаимодействие Linux с другими операционными системами. Описывается конфигурирование локальной сети: сетевые принтеры, шлюз в Интернет, настройка Firewall, учет трафика и т. п. Приведено множество программ, помогающих обслуживать сеть и заботиться о ее безопасности. Рассказано, как создать, настроить и обеспечить надежное функционирование сервера небольшой локальной сети, способного выполнять большинство типовых задач. На прилагаемом компакт-диске находятся последние версии программного обеспечения, рассмотренного в книге.

*Для системных администраторов*

УДК 681.3.06  
ББК 32.973-018.2

### **Группа подготовки издания:**

|                         |                             |
|-------------------------|-----------------------------|
| Главный редактор        | <i>Екатерина Кондукова</i>  |
| Зам. главного редактора | <i>Евгений Рыбаков</i>      |
| Зав. редакцией          | <i>Григорий Добин</i>       |
| Редактор                | <i>Екатерина Капальгина</i> |
| Компьютерная верстка    | <i>Ольги Сергиенко</i>      |
| Корректор               | <i>Зинаида Дмитриева</i>    |
| Оформление серии        | <i>Via Design</i>           |
| Дизайн обложки          | <i>Игоря Цырульников</i>    |
| Зав. производством      | <i>Николай Тверских</i>     |

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 27.02.04.

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

Тираж 4000 экз. Заказ №

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

Гигиеническое заключение на продукцию, товар № 77.99.02.953 Д.001537.03.02 от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов  
в Академической типографии "Наука" РАН  
199034, Санкт-Петербург, 9 линия, 12.

ISBN 5-94157-277-8

© Стахнов А. А., 2004

© Оформление, издательство "БХВ-Петербург", 2004

# Содержание

|                                                                |           |
|----------------------------------------------------------------|-----------|
| <b>Введение .....</b>                                          | <b>15</b> |
| Благодарности .....                                            | 15        |
| Почему написана эта книга .....                                | 16        |
| Для кого написана эта книга .....                              | 16        |
| Структура книги .....                                          | 16        |
| Как со мной связаться .....                                    | 18        |
| <br><b>ЧАСТЬ I. СЕТЕВЫЕ ПРОТОКОЛЫ И КОНФИГУРИРОВАНИЕ .....</b> | <b>19</b> |
| <br><b>Глава 1. Сетевые протоколы .....</b>                    | <b>21</b> |
| Модели сетевых взаимодействий .....                            | 21        |
| Терминология .....                                             | 21        |
| Модель взаимодействия открытых систем (OSI) .....              | 23        |
| Модель сетевого взаимодействия TCP/IP .....                    | 25        |
| Сопоставление сетевых моделей OSI и TCP/IP .....               | 25        |
| Сетевые протоколы .....                                        | 25        |
| Семейство протоколов TCP/IP .....                              | 26        |
| Протоколы межсетевого уровня (Интернет) .....                  | 27        |
| Протокол IP .....                                              | 27        |
| Формат пакета IPv4 .....                                       | 27        |
| Протокол IPv6 .....                                            | 29        |
| Адресация в IPv6 .....                                         | 30        |
| Сетевые пакеты .....                                           | 30        |
| Маршрутизация пакетов .....                                    | 31        |
| Протоколы маршрутизации .....                                  | 31        |
| Адресация в TCP/IP .....                                       | 32        |
| Протокол адресации ARP/RARP .....                              | 34        |
| Протокол ICMP .....                                            | 34        |
| Протоколы транспортного уровня .....                           | 37        |
| Протокол TCP .....                                             | 38        |
| Протокол UDP .....                                             | 39        |
| Протоколы уровня приложений .....                              | 39        |
| Протокол FTP .....                                             | 39        |
| Протокол SMTP .....                                            | 40        |
| Протокол Telnet .....                                          | 40        |
| Сетевая файловая система NFS .....                             | 40        |
| Протокол IPX .....                                             | 40        |
| Протокол AppleTalk .....                                       | 41        |
| Протокол NetBIOS .....                                         | 41        |
| Протокол DECnet .....                                          | 41        |
| Литература и ссылки .....                                      | 41        |
| <br><b>Глава 2. Настройка сети TCP/IP .....</b>                | <b>43</b> |
| Конфигурирование сетевых интерфейсов .....                     | 43        |
| Настройка локального интерфейса lo .....                       | 44        |

|                                                                      |           |
|----------------------------------------------------------------------|-----------|
| Настройка Ethernet-карты (eth0) .....                                | 44        |
| Конфигурирование статических маршрутов и маршрута по умолчанию ..... | 45        |
| Использование DHCP .....                                             | 46        |
| Статический ARP .....                                                | 46        |
| Настройка DNS .....                                                  | 47        |
| Протокол PPP .....                                                   | 49        |
| Общая информация .....                                               | 49        |
| Свойства протокола PPP .....                                         | 50        |
| Составляющие PPP .....                                               | 51        |
| Функционирование протокола PPP .....                                 | 51        |
| Поддерживаемое оборудование .....                                    | 51        |
| Структура пакета протокола PPP .....                                 | 52        |
| PPP-протокол управления соединением (LCP) .....                      | 53        |
| Сокращения, используемые при описании протокола PPP .....            | 53        |
| Стандарты, описывающие протокол PPP .....                            | 55        |
| Протокол SLIP/CSLIP .....                                            | 56        |
| Протокол SLIP .....                                                  | 56        |
| Протокол CSLIP .....                                                 | 57        |
| Процесс init .....                                                   | 57        |
| Конфигурационный файл init (/etc/inittab) .....                      | 59        |
| Основные конфигурационные файлы .....                                | 63        |
| Файл rc.sysinit .....                                                | 64        |
| Файл rc .....                                                        | 65        |
| Файл rc.local .....                                                  | 70        |
| Другие файлы, влияющие на процесс загрузки .....                     | 70        |
| Средства тестирования сети и сетевых настроек .....                  | 71        |
| Утилита ifconfig .....                                               | 71        |
| Утилита hostname .....                                               | 71        |
| Утилита ping .....                                                   | 72        |
| Утилита tracoute .....                                               | 72        |
| Утилита arp .....                                                    | 72        |
| Утилита netstat .....                                                | 72        |
| Утилита TCPdump .....                                                | 73        |
| Литература и ссылки .....                                            | 73        |
| <b>Глава 3. Настройка модемного соединения .....</b>                 | <b>75</b> |
| Начальные установки .....                                            | 75        |
| Настройка модема и последовательного порта .....                     | 76        |
| Связь с провайдером .....                                            | 77        |
| Схема организации подключения локальной сети .....                   | 77        |
| Организация связи по коммутируемому соединению .....                 | 78        |
| Настройка программ .....                                             | 78        |
| Настройка связи с провайдером .....                                  | 78        |
| Команды rppd .....                                                   | 80        |
| Настройка diald .....                                                | 83        |
| Создание скрипта соединения: /etc/diald/connect .....                | 84        |
| Настройка основной конфигурации: /etc/diald.conf .....               | 85        |
| Настройка правил тайм-аутов: /etc/diald/standard.filter .....        | 87        |
| Комплексное тестирование .....                                       | 87        |
| Настройка сервера входящих звонков (Dial-in) .....                   | 88        |
| Настройка mgetty .....                                               | 88        |
| Настройка pppd .....                                                 | 89        |
| Настройка Callback-сервера .....                                     | 90        |
| Конфигурация Callback-сервера .....                                  | 90        |

|                                          |    |
|------------------------------------------|----|
| Конфигурация клиентов .....              | 91 |
| Конфигурирование Linux-клиента .....     | 91 |
| Конфигурирование клиента MS Windows..... | 92 |
| Литература и ссылки .....                | 92 |

## **ЧАСТЬ II. СЕТЕВЫЕ СЛУЖБЫ..... 95**

### **Глава 4. DHCP .....** 97

|                                                     |     |
|-----------------------------------------------------|-----|
| DHCP-протокол.....                                  | 97  |
| Архитектура и формат сообщений .....                | 97  |
| Режимы выдачи IP-адресов .....                      | 98  |
| Параметры конфигурации (поле <i>options</i> ) ..... | 100 |
| Недостатки DHCP .....                               | 100 |
| DHCP-сервер .....                                   | 101 |
| Файл <code>dhcpd.conf</code> .....                  | 101 |
| Файл <code>dhcpd.leases</code> .....                | 104 |
| Пример файла <code>dhcpd.conf</code> .....          | 105 |
| DHCP-клиент .....                                   | 106 |
| Файл <code>dhclient.conf</code> .....               | 106 |
| Файл <code>dhclient.leases</code> .....             | 108 |
| Литература и ссылки .....                           | 109 |

### **Глава 5. DNS .....** 110

|                                                  |     |
|--------------------------------------------------|-----|
| Настройка сетевых параметров .....               | 111 |
| Файл <code>host.conf</code> .....                | 111 |
| Файл <code>/etc/hosts</code> .....               | 111 |
| Файл <code>/etc/resolv.conf</code> .....         | 112 |
| Настройка кэширующего сервера .....              | 112 |
| Файл <code>/etc/named.conf</code> .....          | 112 |
| Файл <code>/etc/127.0.0</code> .....             | 114 |
| Запуск <code>named</code> .....                  | 115 |
| Настройка полнофункционального DNS-сервера ..... | 116 |
| Файл <code>/etc/named.conf</code> .....          | 116 |
| Файл <code>/etc/named/ivan.petrov</code> .....   | 117 |
| Файл <code>/etc/192.168.0</code> .....           | 118 |
| Некоторые тонкости.....                          | 119 |
| Записи ресурсов (RR) службы DNS.....             | 119 |
| Реверсная зона .....                             | 121 |
| Два сервера DNS.....                             | 121 |
| Иерархические поддомены .....                    | 121 |
| Вторичные DNS-серверы .....                      | 121 |
| Используйте серверы кэширования .....            | 121 |
| Инструменты.....                                 | 121 |
| Литература и ссылки .....                        | 122 |

### **Глава 6. Почта .....** 123

|                                             |     |
|---------------------------------------------|-----|
| Протокол SMTP.....                          | 124 |
| Протокол POP3 .....                         | 124 |
| Протокол IMAP .....                         | 125 |
| Формат почтового сообщения .....            | 125 |
| Спецификация MIME.....                      | 126 |
| Поле <i>MIME-Version</i> .....              | 126 |
| Поле <i>Content-Type</i> .....              | 127 |
| Поле <i>Content-Transfer-Encoding</i> ..... | 127 |

|                                                  |     |
|--------------------------------------------------|-----|
| Программное обеспечение.....                     | 128 |
| Спецификация S/MIME .....                        | 128 |
| PGP, GPG .....                                   | 128 |
| Программа sendmail .....                         | 129 |
| Принцип работы.....                              | 129 |
| Настройка программы .....                        | 130 |
| Тестирование отправки почты sendmail.....        | 131 |
| Тестирование обслуживания по протоколу SMTP..... | 131 |
| Тестирование обслуживания по протоколу POP3..... | 135 |
| Программа Postfix .....                          | 137 |
| Конфигурационные файлы .....                     | 138 |
| Литература и ссылки .....                        | 138 |

## **Глава 7. Сетевая информационная система NIS (NIS+) и ее конфигурирование.**

|                                                    |            |
|----------------------------------------------------|------------|
| <b>LDAP.....</b>                                   | <b>140</b> |
| NIS .....                                          | 140        |
| Как работает NIS .....                             | 140        |
| Программа-сервер ypserv .....                      | 141        |
| NIS+ .....                                         | 141        |
| Как работает NIS+ .....                            | 142        |
| LDAP .....                                         | 142        |
| Установка LDAP-сервера .....                       | 143        |
| Настройка LDAP-сервера.....                        | 143        |
| Формат конфигурационного файла.....                | 143        |
| Ключи командной строки .....                       | 149        |
| База данных LDAP.....                              | 150        |
| Механизмы баз данных LDAP, объекты и атрибуты..... | 150        |
| Создание и поддержание базы данных .....           | 152        |
| Утилиты .....                                      | 154        |
| Slapindex.....                                     | 154        |
| Slapcat .....                                      | 154        |
| Ldapsearch .....                                   | 155        |
| Ldapdelete.....                                    | 155        |
| Ldapmodify .....                                   | 156        |
| Ldapadd .....                                      | 156        |
| Kldap .....                                        | 156        |
| GQ .....                                           | 156        |
| Взаимодействие программ с LDAP.....                | 156        |
| Литература и ссылки .....                          | 158        |

## **Глава 8. FTP .....**

|                                         |            |
|-----------------------------------------|------------|
| <b>Протокол FTP.....</b>                | <b>159</b> |
| Представление данных .....              | 159        |
| Тип файла.....                          | 159        |
| Управление форматом .....               | 160        |
| Структура.....                          | 160        |
| Режим передачи .....                    | 160        |
| Управляющие команды FTP.....            | 161        |
| Ответы на управляющие FTP-команды ..... | 161        |
| Управление соединением .....            | 163        |
| Программное обеспечение.....            | 164        |
| Пакет wu-ftp .....                      | 164        |
| Команды .....                           | 164        |

|                                                                        |            |
|------------------------------------------------------------------------|------------|
| Конфигурирование сервера.....                                          | 166        |
| Файл ftpaccess.....                                                    | 166        |
| Файл ftpservers.....                                                   | 172        |
| Файл ftpconversions.....                                               | 172        |
| Файл ftpgroups.....                                                    | 173        |
| Файл ftphosts.....                                                     | 173        |
| Файл ftpusers.....                                                     | 173        |
| Параметры запуска программ, входящих в пакет.....                      | 173        |
| Программа ftpd.....                                                    | 173        |
| Программа ftpwho.....                                                  | 174        |
| Программа ftpcount.....                                                | 174        |
| Программа ftpshut.....                                                 | 174        |
| Программа ftprestart.....                                              | 175        |
| Программа ckconfig.....                                                | 175        |
| Формат файла журнала xferlog.....                                      | 175        |
| Безопасность.....                                                      | 176        |
| Литература и ссылки.....                                               | 177        |
| <b>Глава 9. NNTP. Сервер новостей INN.....</b>                         | <b>178</b> |
| Протокол NNTP.....                                                     | 178        |
| Основные команды протокола NNTP.....                                   | 181        |
| <i>ARTICLE</i> .....                                                   | 181        |
| <i>BODY</i> .....                                                      | 181        |
| <i>HEAD</i> .....                                                      | 181        |
| <i>STAT</i> .....                                                      | 181        |
| <i>GROUP ggg</i> .....                                                 | 182        |
| <i>HELP</i> .....                                                      | 182        |
| <i>IHAVE &lt;message-id&gt;</i> .....                                  | 182        |
| <i>LAST</i> .....                                                      | 182        |
| <i>LIST</i> .....                                                      | 182        |
| <i>NEWGROUPS date time [GMT] [&lt;distributions&gt;]</i> .....         | 183        |
| <i>NEWNEWS newsgroups date time [GMT] [&lt;distribution&gt;]</i> ..... | 183        |
| <i>NEXT</i> .....                                                      | 183        |
| <i>POST</i> .....                                                      | 183        |
| <i>QUIT</i> .....                                                      | 184        |
| <i>SLAVE</i> .....                                                     | 184        |
| Сервер новостей INN.....                                               | 184        |
| Работа пакета INN.....                                                 | 184        |
| Управляющие сообщения.....                                             | 184        |
| Настройка системы INN.....                                             | 185        |
| Файл active.....                                                       | 195        |
| Файлы базы данных и журналы.....                                       | 196        |
| Настройка списка получаемых групп новостей.....                        | 197        |
| Журналирование пакета INN.....                                         | 200        |
| Программы пакета INN.....                                              | 201        |
| Литература и ссылки.....                                               | 202        |
| <b>Глава 10. Web-сервер Apache.....</b>                                | <b>204</b> |
| Конфигурация.....                                                      | 205        |
| Используемые обозначения.....                                          | 205        |
| Права доступа и свойства объекта.....                                  | 206        |
| Общие характеристики сервера.....                                      | 208        |
| Виртуальные серверы.....                                               | 210        |

|                                                         |     |
|---------------------------------------------------------|-----|
| Преобразование адресов .....                            | 211 |
| Преобразование HTTP-заголовков .....                    | 211 |
| Безопасность .....                                      | 212 |
| Индекс каталога .....                                   | 212 |
| Перекодировка (русификация) .....                       | 213 |
| Файл access.conf .....                                  | 216 |
| Файл srm.conf .....                                     | 217 |
| Файл httpd.conf .....                                   | 217 |
| Настройка виртуальных серверов в файле httpd.conf ..... | 217 |
| Литература и ссылки .....                               | 219 |

## **Глава 11. Прoxy-сервер..... 220**

|                                                             |     |
|-------------------------------------------------------------|-----|
| Squid.....                                                  | 221 |
| Протокол ICP.....                                           | 221 |
| Cache digest .....                                          | 221 |
| Иерархия кэшей.....                                         | 222 |
| Алгоритм получения запрошенного объекта.....                | 222 |
| Конфигурирование пакета Squid .....                         | 222 |
| Сетевые параметры.....                                      | 222 |
| Соседи .....                                                | 223 |
| Размер кэша .....                                           | 224 |
| Имена и размеры файлов .....                                | 224 |
| Параметры внешних программ.....                             | 225 |
| Тонкая настройка кэша.....                                  | 226 |
| Время ожидания.....                                         | 227 |
| ACL .....                                                   | 228 |
| Права доступа.....                                          | 229 |
| Параметры администрирования .....                           | 229 |
| Параметры для работы в режиме ускорителя HTTP-сервера ..... | 229 |
| Разное .....                                                | 230 |
| Пример конфигурации Squid.....                              | 232 |
| Создание иерархии Proху-серверов .....                      | 233 |
| Transparent proxy .....                                     | 234 |
| Ключи запуска Squid .....                                   | 235 |
| Файлы журналов Squid.....                                   | 236 |
| Файл access.log.....                                        | 236 |
| Файл store.log.....                                         | 237 |
| Файл useragent.log .....                                    | 238 |
| Нестандартные применения .....                              | 238 |
| Борьба с баннерами.....                                     | 238 |
| Разделение внешнего канала.....                             | 239 |
| Обработка статистики .....                                  | 240 |
| Программа Squid Cache and Web Utilities (SARG) .....        | 241 |
| Программа MRTG .....                                        | 241 |
| Литература и ссылки .....                                   | 241 |

## **Глава 12. Синхронизация времени через сеть, настройка временной зоны..... 242**

|                                        |     |
|----------------------------------------|-----|
| Сетевой протокол времени .....         | 242 |
| Классы обслуживания .....              | 243 |
| Обеспечение достоверности данных ..... | 243 |
| Формат NTP-пакета.....                 | 244 |
| Рекомендуемая конфигурация .....       | 244 |
| Стандарты.....                         | 245 |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Сервер xntpd .....                                              | 245 |
| Конфигурация сервера .....                                      | 245 |
| Класс <i>symmetric</i> .....                                    | 246 |
| Класс <i>procedure-call</i> .....                               | 246 |
| Класс <i>multicast</i> .....                                    | 246 |
| Общие параметры .....                                           | 247 |
| Обеспечение безопасности сервера .....                          | 249 |
| Программы и утилиты, относящиеся к службе точного времени ..... | 250 |
| ntpd .....                                                      | 250 |
| ntpq .....                                                      | 250 |
| ntptrace .....                                                  | 250 |
| xntpd .....                                                     | 251 |
| xntpdcc .....                                                   | 251 |
| Публичные NTP-серверы .....                                     | 251 |
| Клиентские программы для синхронизации времени .....            | 251 |
| UNIX/Linux .....                                                | 252 |
| Apple .....                                                     | 252 |
| Windows .....                                                   | 252 |
| Литература и ссылки .....                                       | 252 |

## **ЧАСТЬ III. СЕТЕВЫЕ РЕСУРСЫ. ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ОПЕРАЦИОННЫМИ СИСТЕМАМИ ..... 253**

### **Глава 13. NFS — сетевая файловая система ..... 255**

|                                         |     |
|-----------------------------------------|-----|
| Установка и настройка NFS-сервера ..... | 255 |
| Установка и настройка NFS-клиента ..... | 256 |
| Опции монтирования .....                | 257 |
| <i>rsizе</i> .....                      | 257 |
| <i>wsizе</i> .....                      | 257 |
| <i>soft</i> .....                       | 258 |
| <i>hard</i> .....                       | 258 |
| <i>timeo=n</i> .....                    | 258 |
| <i>retrans=n</i> .....                  | 258 |
| Безопасность NFS .....                  | 258 |
| Безопасность клиента .....              | 258 |
| Безопасность сервера .....              | 259 |
| Литература и ссылки .....               | 259 |

### **Глава 14. Сервер Samba для клиентов Windows ..... 260**

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| Файл конфигурации smb.conf .....                                      | 262 |
| Секция <i>[global]</i> .....                                          | 267 |
| Секция <i>[homes]</i> .....                                           | 270 |
| Секция <i>[comm]</i> .....                                            | 270 |
| Секция <i>[tmp]</i> .....                                             | 271 |
| Пароли пользователей .....                                            | 271 |
| Добавление пользователей Samba .....                                  | 272 |
| Принтеры .....                                                        | 273 |
| Использование ресурсов Samba .....                                    | 273 |
| Конфигурирование Samba в качестве первичного контроллера домена ..... | 275 |
| Утилиты .....                                                         | 277 |
| SWAT .....                                                            | 277 |
| Webmin .....                                                          | 278 |
| Ksamba .....                                                          | 278 |
| SambaSentinel .....                                                   | 278 |
| Литература и ссылки .....                                             | 278 |

|                                                                                           |                |
|-------------------------------------------------------------------------------------------|----------------|
| <b>Глава 15. Mars — клиентам Novell .....</b>                                             | <b>280</b>     |
| Термины, используемые в тексте .....                                                      | 280            |
| Linux и IPX .....                                                                         | 282            |
| Файлы в каталоге /proc, относящиеся к IPX .....                                           | 282            |
| Linux-утилиты IPX .....                                                                   | 282            |
| IPX-клиент .....                                                                          | 283            |
| Настройка сетевого программного обеспечения IPX .....                                     | 283            |
| Проверка конфигурации .....                                                               | 283            |
| Монтирование сервера или тома Novell .....                                                | 283            |
| Посылка сообщения пользователю Novell .....                                               | 283            |
| IPX-сервер .....                                                                          | 284            |
| Пакет Mars_nwe .....                                                                      | 284            |
| Пакет Lwared .....                                                                        | 290            |
| IPX-маршрутизатор .....                                                                   | 291            |
| Настройка Linux как клиента печати сервера Novell .....                                   | 292            |
| Настройка Linux как сервера печати Novell .....                                           | 292            |
| Пользовательские и административные команды ncpfs .....                                   | 292            |
| Команды пользователя .....                                                                | 293            |
| Утилиты администрирования .....                                                           | 293            |
| Туннелирование IPX через IP .....                                                         | 294            |
| Настройка .....                                                                           | 294            |
| Литература и ссылки .....                                                                 | 295            |
| <br><b>ЧАСТЬ IV. НА СЛУЖБЕ .....</b>                                                      | <br><b>297</b> |
| <b>Глава 16. Firewall .....</b>                                                           | <b>299</b>     |
| Типы брандмауэров .....                                                                   | 300            |
| Брандмауэр с фильтрацией пакетов .....                                                    | 301            |
| Политика организации брандмауэра .....                                                    | 302            |
| Фильтрация сетевых пакетов .....                                                          | 303            |
| Фильтрация входящих пакетов .....                                                         | 303            |
| Фильтрация исходящих пакетов .....                                                        | 306            |
| Защита локальных служб .....                                                              | 307            |
| Программа ipchains .....                                                                  | 307            |
| Опции ipchains .....                                                                      | 309            |
| Символьные константы .....                                                                | 310            |
| Создание правил фильтрации .....                                                          | 311            |
| Удаление существующих правил .....                                                        | 311            |
| Определение политики по умолчанию .....                                                   | 312            |
| Разрешение прохождения пакетов через интерфейс обратной петли .....                       | 312            |
| Запрет прохождения пакетов с фальсифицированными адресами .....                           | 313            |
| Фильтрация ICMP-сообщений .....                                                           | 315            |
| Сообщения об ошибках и управляющие сообщения .....                                        | 316            |
| Противодействие smurf-атакам .....                                                        | 319            |
| Разрешение функционирования служб .....                                                   | 319            |
| Запрет доступа с "неблагонадежных" узлов .....                                            | 325            |
| Поддержка обмена в локальной сети .....                                                   | 325            |
| Разрешение доступа к внутреннему сетевому интерфейсу брандмауэра .....                    | 325            |
| Выбор конфигурации для пользующейся доверием локальной сети .....                         | 325            |
| Организация доступа из локальной сети к брандмауэру бастионного типа .....                | 326            |
| Перенаправление трафика .....                                                             | 326            |
| Разрешение доступа в Интернет из локальной сети: IP-перенаправление<br>и маскировка ..... | 327            |
| Организация демилитаризованной зоны .....                                                 | 329            |
| Защита подсетей с помощью брандмауэров .....                                              | 329            |

|                                                                       |            |
|-----------------------------------------------------------------------|------------|
| Отладка брандмауэра.....                                              | 330        |
| Общие рекомендации по отладке брандмауэра.....                        | 330        |
| Отображение списка правил брандмауэра.....                            | 332        |
| Утилиты.....                                                          | 332        |
| Iptables.....                                                         | 332        |
| Порядок движения транзитных пакетов.....                              | 334        |
| Порядок движения пакетов для локальной программы.....                 | 335        |
| Порядок движения пакетов от локальной программы.....                  | 336        |
| Таблица mangle.....                                                   | 336        |
| Таблица nat.....                                                      | 337        |
| Таблица filter.....                                                   | 337        |
| Построение правил для iptables.....                                   | 337        |
| Команды ipchains.....                                                 | 338        |
| Критерии проверки пакетов.....                                        | 339        |
| Общие критерии.....                                                   | 340        |
| TCP-критерии.....                                                     | 341        |
| UDP-критерии.....                                                     | 342        |
| ICMP-критерии.....                                                    | 343        |
| Специальные критерии.....                                             | 343        |
| Действия и переходы.....                                              | 345        |
| Действие ACCEPT.....                                                  | 346        |
| Действие DNAT.....                                                    | 346        |
| Действие DROP.....                                                    | 346        |
| Действие LOG.....                                                     | 346        |
| Действие MARK.....                                                    | 347        |
| Действие MASQUERADE.....                                              | 347        |
| Действие MIRROR.....                                                  | 347        |
| Действие QUEUE.....                                                   | 347        |
| Действие REDIRECT.....                                                | 347        |
| Действие REJECT.....                                                  | 347        |
| Действие RETURN.....                                                  | 347        |
| Действие SNAT.....                                                    | 348        |
| Действие TOS.....                                                     | 348        |
| Действие TTL.....                                                     | 348        |
| Действие ULOG.....                                                    | 348        |
| Утилиты iptables.....                                                 | 348        |
| Iptables-save.....                                                    | 348        |
| Iptables-restore.....                                                 | 349        |
| Литература и ссылки.....                                              | 349        |
| <b>Глава 17. Сетевые принтеры.....</b>                                | <b>350</b> |
| Способы вывода на принтер.....                                        | 350        |
| Система печати CUPS.....                                              | 351        |
| Программный пакет LPD.....                                            | 351        |
| Настройка LPD.....                                                    | 353        |
| Учет ресурсов.....                                                    | 354        |
| Настройка сетевого принтера.....                                      | 355        |
| Использование принт-сервера.....                                      | 355        |
| Печать на Ethernet-принтер.....                                       | 357        |
| Литература и ссылки.....                                              | 357        |
| <b>Глава 18. Организация шлюза в Интернет для локальной сети.....</b> | <b>359</b> |
| Начальные установки.....                                              | 360        |
| Связь с провайдером.....                                              | 360        |
| Схема организации подключения локальной сети.....                     | 361        |

|                                                                 |            |
|-----------------------------------------------------------------|------------|
| Организация связи по коммутируемому соединению .....            | 361        |
| Настройка программ .....                                        | 361        |
| Настройка связи с провайдером .....                             | 362        |
| Настройка diald .....                                           | 364        |
| Создание скрипта соединения: /etc/diald/connect .....           | 365        |
| Настройка основной конфигурации: /etc/diald.conf .....          | 367        |
| Настройка правил тайм-аутов: /etc/diald/standard.filter .....   | 368        |
| Комплексное тестирование .....                                  | 368        |
| Организация связи по выделенному каналу .....                   | 369        |
| Настройка связи с провайдером .....                             | 369        |
| Комплексное тестирование .....                                  | 370        |
| Защита локальной сети .....                                     | 371        |
| Установка Proxy-сервера .....                                   | 371        |
| Transparent Proxy .....                                         | 371        |
| Борьба с баннерами .....                                        | 372        |
| Разделение внешнего канала (ограничение трафика) .....          | 372        |
| Мониторинг загрузки каналов .....                               | 373        |
| Программа MRTG .....                                            | 373        |
| Конфигурирование MRTG .....                                     | 373        |
| Программа RRDtool .....                                         | 377        |
| Подсчет трафика .....                                           | 377        |
| Литература и ссылки .....                                       | 378        |
| <b>Глава 19. Учет сетевого трафика .....</b>                    | <b>380</b> |
| Простой учет трафика .....                                      | 380        |
| Учет трафика при помощи net-acct .....                          | 385        |
| Naccttab .....                                                  | 385        |
| Nacctpeering .....                                              | 387        |
| Литература и ссылки .....                                       | 388        |
| <b>Глава 20. Виртуальные частные сети .....</b>                 | <b>389</b> |
| Протокол IPSec .....                                            | 390        |
| VPN-сервер FreeS/WAN .....                                      | 391        |
| Ipsec.conf .....                                                | 392        |
| Ipsec.secrets .....                                             | 393        |
| MS Windows NT VPN (PPTP) .....                                  | 394        |
| Linux PPTP-сервер .....                                         | 395        |
| Linux PPTP-клиент .....                                         | 396        |
| Литература и ссылки .....                                       | 396        |
| <b>Глава 21. Бездисковые компьютеры .....</b>                   | <b>397</b> |
| Что такое бездисковый компьютер .....                           | 397        |
| Преимущества использования бездискового компьютера .....        | 397        |
| Недостатки использования бездискового компьютера .....          | 398        |
| Области применения .....                                        | 399        |
| Процесс загрузки бездискового компьютера .....                  | 399        |
| Предварительные действия .....                                  | 400        |
| Установка и настройка программного обеспечения на сервере ..... | 401        |
| Linux-клиент .....                                              | 401        |
| Создание загрузочного ПЗУ (загрузочной дискеты) .....           | 402        |
| Настройка сервера .....                                         | 403        |
| Конфигурация клиента .....                                      | 404        |
| Windows-клиенты .....                                           | 404        |
| Установка и настройка программного обеспечения на клиенте ..... | 405        |

|                                           |     |
|-------------------------------------------|-----|
| Создание загрузочного образа дискеты..... | 407 |
| Загрузка бездискковой машины .....        | 407 |
| Оптимизация бездискковой загрузки.....    | 408 |
| Литература и ссылки .....                 | 411 |

## **ЧАСТЬ V. УТИЛИТЫ АДМИНИСТРИРОВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ..... 413**

### **Глава 22. Доступ к удаленным компьютерам ..... 415**

|                                          |     |
|------------------------------------------|-----|
| Telnet.....                              | 415 |
| Протокол Telnet .....                    | 415 |
| Команды Telnet .....                     | 417 |
| Программа-клиент telnet .....            | 418 |
| Программа-сервер telnetd .....           | 419 |
| Применение Telnet и безопасность .....   | 419 |
| Семейство r-команд .....                 | 420 |
| Команда <i>rlogin</i> .....              | 420 |
| Команда <i>rsh</i> .....                 | 420 |
| Команда <i>rcp</i> .....                 | 420 |
| Команда <i>rsync</i> .....               | 420 |
| Команда <i>rdist</i> .....               | 420 |
| Применение r-команд и безопасность ..... | 421 |
| SSH и OpenSSH .....                      | 421 |
| Принцип работы SSH.....                  | 421 |
| OpenSSH .....                            | 422 |
| Конфигурирование OpenSSH.....            | 422 |
| Ключи запуска сервера SSH .....          | 428 |
| Ключи запуска клиента SSH.....           | 428 |
| Программы, входящие в пакет OpenSSH..... | 430 |
| Программа <i>ssh-keygen</i> .....        | 430 |
| Программа <i>ssh-agent</i> .....         | 431 |
| Программа <i>ssh-add</i> .....           | 431 |
| Программа <i>sftp</i> .....              | 431 |
| Программа <i>scp</i> .....               | 432 |
| Программа <i>ssh-keyscan</i> .....       | 433 |
| Литература и ссылки .....                | 434 |

### **Глава 23. Обеспечение безопасности и администрирование сети ..... 435**

|                                                |     |
|------------------------------------------------|-----|
| Расширенное управление доступом к файлам ..... | 435 |
| Установка Linux ACL .....                      | 436 |
| Установка и изменение прав доступа .....       | 437 |
| Шифрование трафика .....                       | 438 |
| Stunnel.....                                   | 439 |
| Установка.....                                 | 439 |
| Организация шифрованного туннеля .....         | 439 |
| Stunnel и приложения, поддерживающие SSL ..... | 440 |
| Сертификаты .....                              | 440 |
| Утилиты сканирования и защиты сети.....        | 441 |
| SATAN .....                                    | 441 |
| Port Sentry .....                              | 442 |
| Установка и настройка .....                    | 442 |
| Запуск .....                                   | 444 |

|                                                   |            |
|---------------------------------------------------|------------|
| Сетевая статистика .....                          | 444        |
| NeTraMet .....                                    | 444        |
| Ключи запуска NeTraMet .....                      | 445        |
| Ключи запуска NeMaC .....                         | 445        |
| Протоколирование .....                            | 445        |
| Демон syslogd .....                               | 446        |
| Параметры запуска .....                           | 446        |
| Файл конфигурации .....                           | 446        |
| Сетевое протоколирование .....                    | 448        |
| Демон klogd .....                                 | 448        |
| Защита системы после взлома .....                 | 449        |
| Rootkit .....                                     | 449        |
| Обнаружение rootkit .....                         | 451        |
| Сканирование портов .....                         | 451        |
| Использование RPM .....                           | 451        |
| Сканер для rootkit .....                          | 452        |
| После обнаружения .....                           | 452        |
| LIDS .....                                        | 453        |
| Установка .....                                   | 453        |
| Конфигурирование LIDS .....                       | 455        |
| Способности .....                                 | 455        |
| Правила доступа .....                             | 458        |
| Tripwire .....                                    | 459        |
| PortSentry .....                                  | 460        |
| LogSentry .....                                   | 460        |
| AIDE .....                                        | 460        |
| RSBAC .....                                       | 460        |
| Security-Enhanced Linux .....                     | 461        |
| Литература и ссылки .....                         | 461        |
| <br>                                              |            |
| <b>Приложение 1. Литература .....</b>             | <b>463</b> |
| <b>Приложение 2. Ссылки .....</b>                 | <b>466</b> |
| <b>Приложение 3. Описание компакт-диска .....</b> | <b>473</b> |
| <b>Предметный указатель .....</b>                 | <b>477</b> |

# Введение

Традиционным элементом практически любой книги является введение. Любой человек, взяв незнакомую книгу в руки, первым делом интересуется тремя вещами: аннотацией, введением и оглавлением книги. Позвольте представить вам введение моей книги.

## Благодарности

Хотелось бы сказать о людях, благодаря которым эта книга в конце концов была создана.

Огромное спасибо моей жене Светлане и дочке Наталье за проявленное терпение, поддержку и понимание — мало людей согласится видеть мужа и отца на протяжении многих месяцев спиной к окружающей действительности и лицом к монитору. Спасибо всем остальным членам моей семьи — без их чуткости и поддержки мне было бы намного тяжелее работать.

Отдельное спасибо Юрию Осьмеркину — это он меня привел в мир Linux и консультировал по множеству вопросов, связанных с материалом книги.

Я благодарен коллективу издательства "БХВ-Петербург" за веру в молодых авторов и терпение в работе с ними. Особо хочется отметить следующих людей: Екатерину Капалыгину, моего редактора, благодаря ее стараниям книга приобрела единый стиль подачи материала; Евгения Рыбакова — за решение общих проблем; и других специалистов, создавших книгу в том виде, в котором читатель увидит ее в магазинах.

Я благодарен сотням и тысячам энтузиастов, плодами работы которых я воспользовался при написании книги, — составителям и переводчикам разнообразной документации, FAQ, How To и различных статей, авторам программ и просто их пользователям.

## Почему написана эта книга

Достаточно сложный вопрос. Здесь переплелись и меркантильный интерес, и честолубие, желание попробовать себя в другой области, попытка побороть свою неуверенность и лень, и не в последнюю очередь — хотелось сделать книгу для наших реалий и нашей специфики. Не секрет, что большинство переводной литературы неадекватно для нашей полунищей действительности. Часто можно встретить несколько "раздражающие" для глаза администратора бюджетной организации советы типа "в качестве маршрутизатора мы рекомендуем использовать устройство фирмы Cisco со следующими параметрами...". Конечно, с точки зрения надежности, простоты в обслуживании и тому подобных вещей такой совет верен. А с точки зрения банального бюджета какой-нибудь государственной конторы — заплатить 4—5 тысяч американских долларов за "железку" размером с кирпич — полный абсурд. Поэтому для наших реалий нужна книга, описывающая построение сетевой и программной инфраструктуры, позволяющей решать большинство типовых задач. Помимо этого, одной из причин для создания книги явилось желание систематизировать и углубить свои собственные знания об операционной системе Linux и ее приложениях.

## Для кого написана эта книга

Прежде чем создавать какое-то произведение, автор всегда должен определить своего потенциального читателя. Каким же я его вижу? Это должен быть человек, увлекающийся информационными технологиями, который обладает достаточно приличным багажом знаний в области программного обеспечения (как правило, операционная система Windows), почти наверняка тем или иным образом связанный с администрированием (по крайней мере, как администратор своего собственного персонального компьютера), которому интересно возиться с программным обеспечением и который собирается перейти, или недавно это сделал, к использованию операционной среды Linux. При этом уровень книг серии "для чайников" или "сделай все за 21 день" его заведомо не устраивает, поскольку ему необходимо четко представлять себе возможности операционной системы, ее структуру, решаемые с ее помощью прикладные задачи, наиболее популярное программное обеспечение, его установка, настройка и использование.

Вот так я представляю себе читателя книги.

## Структура книги

Книга разбита на пять частей плюс приложения. Рассмотрим, что в них описывается и для кого они предназначены.

*Часть I* представляет интерес для новичков в мире Linux. В ней содержится обзор протоколов семейства TCP/IP, процесс настройки и отладки сетевых интерфейсов, а также настройка модемного соединения. Этот раздел является вводным (базисным), поскольку дальнейшее изложение материала подразумевает знание специфики протоколов TCP/IP и настроенной сети. Он будет интересен в первую очередь новичкам и "продвинутым" пользователям, поскольку администраторы со стажем должны знать данную тему "на зубок".

*Часть II* представляет интерес как для новичков, так и для опытных пользователей операционной системы Linux, поскольку именно здесь рассматриваются вопросы конфигурирования сетевых служб. В этой части описывается конфигурирование DHCP, DNS, почтового сервера, службы LDAP, FTP, NNTP, Apache, Прoxy-сервера и NTP-сервера. Именно эта часть позволит вам создать полнофункциональный сервер, способный выполнить около 90% задач типичного сервера небольшой организации. Вторую часть я старался сделать доступной для понимания начинающему пользователю. Она содержит большой объем информации в достаточно сжатом виде и требует размышлений и экспериментов от читателя.

В *части III* я опять возвращаюсь к настройке сетевых сервисов. Поскольку мы за плюрализм и демократию, наша сеть не является гомогенной средой и волей-неволей приходится взаимодействовать с различными операционными системами. В этой части мы ознакомимся с NFS (сетевой файловой системой UNIX), научимся предоставлять и получать доступ к каталогам операционных систем Windows и Novell.

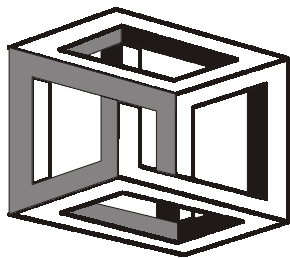
Предыдущие части книги были подготовительным этапом для *части IV*. Она предназначена больше для опытных пользователей, т. к. я хотел, чтобы моя книга служила вам верой и правдой в качестве справочного пособия долгое время, и вы периодически возвращались к ней для решения специфических задач, возникающих в вашей работе. Здесь вы найдете описание основных приложений, используемых для организации НОРМАЛЬНОГО функционирования сети организации, подключенной к Интернету. В этой части рассмотрена защита сети от нежелательного воздействия, организация виртуальных частных сетей, учета сетевого трафика, настройка сетевых принтеров, изготовление бездисковых компьютеров и организация шлюза в Интернете.

*Часть V* посвящена администрированию системы. Здесь рассмотрен удаленный безопасный доступ к хостам, а также утилиты для администрирования и мониторинга сети.

В *приложениях* находится список рекомендуемой литературы, небольшая коллекция ссылок, тем или иным образом касающихся Linux и программ для этой операционной системы, а также список наиболее часто применяемых сетевых портов и программ, их использующих.

## Как со мной связаться

Те читатели, которые хотят внести свои предложения или уточнения по содержанию данной книги, поделиться интересными идеями, темами и т. п., могут воспользоваться электронным адресом **alst@farlep.net**. Я постараюсь ответить на все письма. Также можно воспользоваться моим сайтом **www.alst.od.ua**.



# ЧАСТЬ I

---

---

## Сетевые протоколы и конфигурирование

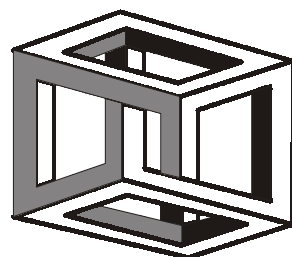
Эта часть является вводной. Как в хорошем детективе, прежде чем приступить к поиску преступника, нужно осмотреть место происшествия. Продолжая аналогию — прежде чем углубляться в дебри специфического программного обеспечения, необходимо узнать фундамент, на котором оно стоит, те общие моменты, которые используются большинством программ.

Данная часть интересна в первую очередь новичкам и опытным пользователям, поскольку администраторы со стажем должны хорошо знать эту тему. В ней содержится обзор протоколов семейства TCP/IP, процесс настройки и отладки сетевых интерфейсов, настройка модемного соединения, поскольку дальнейшее изложение материала подразумевает знание специфики протоколов TCP/IP и настроенной сети.

**Глава 1.** Сетевые протоколы

**Глава 2.** Настройка сети TCP/IP

**Глава 3.** Настройка модемного соединения



# ГЛАВА 1

## Сетевые протоколы

В данной главе будут рассмотрены базовые понятия, сетевые модели и протоколы, используемые в сетях. На фундаменте, заложенном этой главой, выстроена вся книга, поэтому рекомендую начинающим ознакомиться с ней, а более опытным полистать, освежить свои знания.

### Модели сетевых взаимодействий

Как и любая сложная система, сеть опирается на стандарты, без которых невозможно ее нормальное функционирование. За последние двадцать лет было создано множество концепций сетевых взаимодействий, однако наибольшее распространение получили всего две:

- ☐ модель взаимодействия открытых систем (OSI);
- ☐ модель сетевого взаимодействия TCP/IP.

### Терминология

Для облегчения понимания содержимого этой главы, приведем основные термины (табл. 1.1).

*Таблица 1.1. Базовые сетевые термины*

| Термин                                          | Определение                                                                                                                 |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Датаграмма                                      | Пакет данных. Обозначает единицу информации при сетевом обмене                                                              |
| DNS (Domain Name Service, служба доменных имен) | Специально выделенные компьютеры, которые производят поиск соответствия символического имени хоста и цифрового адреса хоста |

Таблица 1.1 (продолжение)

| Термин                                                                                         | Определение                                                                                                   |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Интернет                                                                                       | Глобальная компьютерная сеть, основанная на семействе протоколов TCP/IP                                       |
| FTP (File Transfer Protocol, протокол передачи файлов)                                         | Протокол используется для приема и передачи файлов между двумя компьютерами                                   |
| IP (Internet Protocol, протокол Интернет)                                                      | Основа семейства протоколов TCP/IP. Практически любой протокол из этого семейства базируется на протоколе IP  |
| ICMP (Internet Control Message Protocol, протокол управляющих сообщений в стеке протоколов IP) | Используется для передачи управляющих сообщений протокола IP                                                  |
| NFS (Network File System, сетевая файловая система)                                            | Система виртуальных дисков, позволяющая клиентским компьютерам использовать каталоги сервера в качестве диска |
| NIC (Network Information Center, сетевой информационный центр)                                 | Организация, которая отвечает за администрирование и раздачу сетевых адресов и имен                           |
| Узел (Node, Host)                                                                              | Компьютер в сети. Название применимо как к клиенту, так и к серверу                                           |
| OSI (Open System Interconnection, взаимодействие открытых систем)                              | Модель взаимодействия открытых систем                                                                         |
| RFC (Request For Comments, запрос для пояснений)                                               | Стандарты протоколов Интернета и их взаимодействия                                                            |
| RIP (Routing Information Protocol, протокол маршрутизации информации)                          | Протокол, используемый для обмена информацией между маршрутизаторами                                          |
| SMTP (Simple Mail Transfer Protocol, простой протокол передачи электронной почты)              | Используется для обмена электронной почтой                                                                    |
| SNMP (Simple Network Management Protocol, простой протокол управления сетью)                   | Используется для управления сетевыми устройствами                                                             |
| TCP (Transmission Control Protocol, протокол управления передачей)                             | Используется для надежной передачи данных                                                                     |
| Telnet                                                                                         | Протокол, осуществляющий удаленное сетевое подключение к компьютеру, эмулирующее терминал                     |

Таблица 1.1 (окончание)

| Термин                                                            | Определение                                                         |
|-------------------------------------------------------------------|---------------------------------------------------------------------|
| UDP (User Datagram Protocol, протокол пользовательских датаграмм) | Используется для обмена блоками информации без установки соединения |

Модель взаимодействия открытых систем (OSI)

Еще в 1983 году Международная организация по стандартизации (International Organization for Standardization, ISO) разработала стандарт взаимодействия открытых систем (Open System Interconnection, OSI). В результате получилась семиуровневая модель:

- 1. Физический уровень (Physical Level).
- 2. Уровень данных (Data Link Level).
- 3. Сетевой уровень (Network Level).
- 4. Транспортный уровень (Transport Level).
- 5. Уровень сессии (Session Level).
- 6. Уровень представления (Presentation Level).
- 7. Уровень приложения (Application Level).

Первый уровень самый "приземленный", последующие — все более и более абстрагируются от особенностей физической среды передачи информации.

Каждый уровень модели OSI решает свои задачи, использует сервисы, предоставляемые предыдущим уровнем и, в свою очередь, предоставляет сервисы следующему уровню. Согласно этой модели, уровни не могут "перескакивать" через соседей, например, транспортный уровень не может непосредственно пользоваться сервисом физического уровня, он обязан пройти по цепочке: Сетевой уровень → Уровень данных → Физический уровень. В табл. 1.2 приведено описание уровней сетевой модели OSI.

Таблица 1.2. Уровни сетевой модели OSI

| Уровень | Название           | Описание                                                                                                                                                    |
|---------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Физический уровень | Отвечает за физическое подключение компьютера к сети. Определяет уровни напряжения, параметры кабеля, разъемы, распайку проводов и т. п.                    |
| 2       | Уровень данных     | Физически подготавливает данные для передачи (разбивая их на кадры определенной структуры) и преобразует обратно во время приема (восстанавливая из кадров) |

**Таблица 1.2** (окончание)

| Уровень | Название              | Описание                                                                               |
|---------|-----------------------|----------------------------------------------------------------------------------------|
| 3       | Сетевой уровень       | Маршрутизирует данные в сети                                                           |
| 4       | Транспортный уровень  | Обеспечивает последовательность и целостность передачи данных                          |
| 5       | Уровень сессии        | Устанавливает и завершает коммуникационные сессии                                      |
| 6       | Уровень представления | Выполняет преобразование данных и обеспечивает передачу данных в универсальном формате |
| 7       | Уровень приложения    | Осуществляет интерфейс между приложением и процессом сетевого взаимодействия           |

На каждом уровне блоки информации имеют собственное название (табл. 1.3).

**Таблица 1.3.** Название блока информации в модели

| Уровень | Название уровня      | Название блока информации |
|---------|----------------------|---------------------------|
| 1       | Физический уровень   | Бит                       |
| 2       | Уровень данных       | Кадр (пакет)              |
| 3       | Сетевой уровень      | Датаграмма                |
| 4       | Транспортный уровень | Сегмент                   |
| 5, 6, 7 | Уровень приложения   | Сообщение                 |

Несмотря на то, что OSI является международным стандартом и на его основе правительство США выпустило спецификации GOSIP (Government Open Systems Interconnection Profile, Государственный регламент взаимодействия открытых систем), у производителей программного обеспечения стандарт OSI широкой поддержки не получил. Это объясняется несколькими причинами:

- ☐ волокита в принятии стандарта;
- ☐ его "оторванность" от реалий;
- ☐ наличие большого числа уровней трудно для реализации и приводит к потере производительности;
- ☐ широчайшее распространение протокола TCP/IP, и нежелание потребителей отказываться от него.

В результате, спецификации OSI сегодня — это, в основном, страницы в учебнике, в реальной жизни они не применяются.

## Модель сетевого взаимодействия TCP/IP

Архитектура семейства протоколов TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/интернет-протокол) основана на представлении, что коммуникационная инфраструктура содержит три вида объектов: процессы, хосты и сети.

Основываясь на этих трех объектах, разработчики выбрали четырехуровневую модель:

- 1. Уровень сетевого интерфейса (Network Interface Layer).
- 2. Уровень межсетевого интерфейса — Интернета (Internet Layer).
- 3. Транспортный уровень (Host-to-Host Layer).
- 4. Уровень приложений/процессов (Application/Process Layer).

## Сопоставление сетевых моделей OSI и TCP/IP

Нетрудно заметить, что модель TCP/IP отличается от модели OSI. В табл. 1.4 показано соответствие модели TCP/IP и модели OSI.

Таблица 1.4. Соответствие модели TCP/IP и модели OSI

| TCP/IP                        | OSI                   |
|-------------------------------|-----------------------|
| Уровень приложений            | Уровень приложений    |
|                               | Уровень представления |
|                               | Уровень сеанса        |
| Транспортный уровень          | Транспортный уровень  |
| Межсетевой уровень (Интернет) | Сетевой уровень       |
| Уровень сетевого интерфейса   | Уровень канала данных |
|                               | Физический уровень    |

Как видно из таблицы, уровень сетевого интерфейса модели TCP/IP соответствует сразу двум уровням модели OSI, а уровень приложений модели TCP/IP — трем уровням модели OSI.

## Сетевые протоколы

В данном разделе мы рассмотрим различные сетевые протоколы, используемые в современной компьютерной индустрии. Пожалуй, это основная часть сетевых моделей (аппаратная часть все-таки не настолько важна для функционирования сети). Также здесь будут рассмотрены протоколы транспортного уровня, на которые опираются протоколы уровня приложений.