

**АЛЕКСЕЙ СТАРОВОЙТОВ**

# **СЕТЬ НА LINUX**

## **ПРОЕКТИРОВАНИЕ, ПРОКЛАДКА, ЭКСПЛУАТАЦИЯ**

**Основы функционирования  
сетей**

**Принципы работы сетевой  
аппаратуры**

**Организация локальной сети  
с нуля**

**Генерация сервера на основе  
ASPLinux (Red Hat)**

**СИ СА Д МИ Н  
СИСТЕМНЫЙ  
АДМИНИСТРАТОР**

УДК 681.3.06  
ББК 32.973.202  
С77

**Старовойтов А. А.**

**С77** Сеть на Linux: проектирование, прокладка, эксплуатация. —  
СПб.: БХВ-Петербург, 2005. — 288 с.: ил.

ISBN 5-94157-687-0

Рассмотрены практические вопросы по прокладке сети, организации сервера (Apache, Samba, DNS, DHCP) на основе операционной системы Linux и интеграции этого сервера в сетях Windows. Большое внимание уделено повседневной эксплуатации сети. Излагаются основы функционирования сетей и сетевой аппаратуры. Даются практические рекомендации по проектированию и прокладке сетей, проверке и поиску неисправностей. Приводится пример построения локальной сети небольшой фирмы и методика поиска неисправностей без использования специального оборудования. Рассмотрены вопросы антивирусной защиты сервера. Описанная технология может быть использована не только при прокладке и сопровождении сети небольшой фирмы на основе Linux-сервера, но и для организации домашних сетей.

*Для системных администраторов и опытных пользователей*

УДК 681.3.06  
ББК 32.973.202

**Группа подготовки издания:**

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Григорий Добин</i>
Редактор	<i>Елена Кошлакова</i>
Компьютерная верстка	<i>Татьяны Олоновой</i>
Корректор	<i>Татьяна Кошелева</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 20.10.05.

Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 23,22.

Тираж 3000 экз. Заказ №

"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию  
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой  
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов  
в ОАО "Техническая книга"

190005, Санкт-Петербург, Измайловский пр., 29

ISBN 5-94157-687-0

© Старовойтов А. А., 2006  
© Оформление, издательство "БХВ-Петербург", 2006

# Оглавление

<b>Введение .....</b>	<b>1</b>
О чем эта книга .....	1
Для кого эта книга .....	1
Какова структура книги .....	2
Как связаться с автором .....	2
 <b>ЧАСТЬ I. КРАТКИЕ ОСНОВЫ ФУНКЦИОНИРОВАНИЯ СЕТЕЙ .....</b>	<b>3</b>
<b>Глава 1. Характеристика протокола TCP/IP .....</b>	<b>5</b>
1.1. Модель OSI .....	5
1.2. Стек TCP/IP .....	7
 <b>Глава 2. Технологии локальных сетей .....</b>	<b>11</b>
2.1. Кабели, используемые в локальных сетях .....	11
Коаксиальный кабель .....	12
Кабель на основе неэкранированной витой пары .....	12
Кабель на основе экранированной витой пары .....	13
Волоконно-оптический кабель .....	14
2.2. Стандарты сетей .....	14
2.3. Технология Ethernet .....	16
2.4. Технология Fast Ethernet .....	21
2.5. Методика расчета сетей Fast Ethernet на повторителях .....	23
2.6. Технология Gigabit Ethernet .....	25
 <b>ЧАСТЬ II. ПРОКЛАДКА КАБЕЛЬНОЙ СИСТЕМЫ .....</b>	<b>29</b>
<b>Глава 3. Аппаратура локальных сетей .....</b>	<b>31</b>
3.1. Сетевые карты и концентраторы .....	31
Сетевые адаптеры .....	31
Концентраторы .....	32
3.2. Необходимость структуризации сети .....	33
3.3. Принципы работы мостов (коммутаторов) .....	35
Прозрачный мост .....	36
Петли при использовании мостов .....	37

3.4. Полнодуплексный и полудуплексный протоколы .....	38
Управление при полудуплексной работе .....	40
Управление при полнодуплексной работе .....	40
3.5. Проблема полосы пропускания .....	41
3.6. Технологии коммутации.....	43
Коммутация второго уровня.....	43
Коммутация третьего уровня.....	44
Коммутация четвертого уровня.....	44
3.7. Техническая реализация коммутаторов.....	45
Коммутаторы с разделяемой памятью .....	45
Коммутатор с общей шиной .....	46
Коммутатор на основе коммутационной матрицы.....	47
3.8. Основные характеристики коммутаторов .....	47
Основные характеристики .....	47
3.9. Дополнительные функции коммутаторов.....	49
Расширенная фильтрация трафика .....	50
Поддержка алгоритма Spanning Tree .....	50
Возможность создания виртуальных сетей.....	51
3.10. Методика оценки необходимой производительности коммутатора.....	52
<b>Глава 4. Проектирование кабельной системы .....</b>	<b>54</b>
4.1. Логическая структуризация сети и кабельная система .....	54
Необходимость логической структуризации сети .....	54
Структурированная кабельная система.....	55
4.2. Активное оборудование локальных сетей и его связь с СКС .....	57
Горизонтальная система .....	57
Система здания.....	57
Система городка .....	57
4.3. Выбор общей концепции сети .....	58
4.4. Сбор информации о будущей сети .....	59
4.5. Выбор типа кабеля.....	62
Коаксиальные кабели.....	62
Витая пара .....	62
Оптический кабель.....	63
Эксплуатационные характеристики витой пары .....	63
4.6. Расширение пропускной способности сети .....	63
Сеть 100Base-TX с одним сервером на основе концентраторов.....	64
Сеть с несколькими серверами по технологии 100Base-TX на основе коммутаторов.....	65
4.7. Проект сети.....	67
Общие вопросы.....	67
Проектирование топологии сети .....	67
Выбор сетевого оборудования.....	72
Подготовка проектной документации.....	73

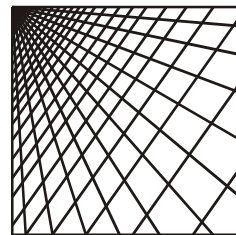
<b>Глава 5. Прокладка сети.....</b>	<b>74</b>
5.1. Техника безопасности и правила монтажа .....	74
Техника безопасности.....	74
Правила монтажа.....	75
5.2. Используемый инструмент .....	76
5.3. Монтажные шкафы. Типы шкафов. Подготовка и установка монтажного шкафа.....	78
5.4. Кабельный канал, углы, Т-примыкания, заглушки .....	80
5.5. Подготовка и установка розеток .....	82
5.6. Прокладка кабеля.....	83
Последовательность прокладки кабеля через отверстия в стенах .....	84
Прокладка кабеля за потолочными панелями .....	86
5.7. Разделка розеток и патч-панели .....	86
Разделка розетки.....	87
Разделка патч-панели.....	88
5.8. Монтаж патч-кордов.....	90
5.9. Прокладка кабеля по воздуху .....	92
<b>Глава 6. Сборка сервера .....</b>	<b>94</b>
6.1. Система клиент-сервер.....	94
6.2. Материнская плата .....	94
6.3. Процессор .....	96
6.3. Оперативная память.....	97
6.4. Жесткие диски и RAID .....	98
IDE/ATA .....	99
SCSI.....	100
SATA.....	100
RAID .....	100
6.5. Подбор конфигурации сервера.....	101
6.6. Источники бесперебойного питания.....	102
6.7. Сборка сервера .....	103
<b>Глава 7. Тестирование сети и поиск неисправностей .....</b>	<b>108</b>
7.1. Причины плохой работы сети .....	108
7.2. Как правильно тестировать сеть .....	109
7.3. Проверка правильности разделки контактов.....	110
7.4. Проверка надежности соединения в контактах .....	111
7.5. Проверка методом исключения.....	112
Поочередное отключение узлов от сети .....	112
Прокачка через сетевую карту большого объема информации .....	113
7.6. Поиск неисправного порта коммутатора .....	114
7.7. Мониторинг сети .....	115

<b>ЧАСТЬ III. LINUX-СЕРВЕР СВОИМИ РУКАМИ.....</b>	<b>117</b>
<b>Глава 8. Установка сервера.....</b>	<b>119</b>
8.1. Выбор дистрибутива .....	119
8.2. Установка сервера .....	121
8.3. Первый вход в систему и настройка графического режима при помощи утилиты xvidtune .....	138
Если все сложнее, чем вы думали .....	141
<b>Глава 9. Основы администрирования Linux.....</b>	<b>142</b>
9.1. Загрузка системы.....	142
9.2. Пользователи, группы, учетные записи .....	147
9.3. Управление учетными записями .....	153
Добавление нового пользователя.....	153
Модификация существующего пользователя .....	158
Удаление пользователя .....	160
9.3. Процессы. Управление процессами. Останов системы.....	162
Общая характеристика процессов .....	162
Получение информации о процессах.....	163
Управление приоритетом процессов.....	166
Уничтожение процессов .....	167
Останов системы .....	168
9.4. Файловая система. Структура каталогов. Работа с файлами .....	169
Понятие файловой системы.....	169
Монтирование и демонтирование файловой системы .....	170
Соглашение об именовании устройств.....	172
Структура каталогов файловой системы.....	172
Просмотр информации о файле .....	173
Типы файлов .....	175
Права доступа.....	176
Изменение прав доступа.....	177
Изменение владельца и группы .....	178
Установка режима создания файла .....	178
9.5. Текстовый редактор vi .....	179
9.6. Файловый менеджер Midnight Commander.....	181
Настройка прав доступа.....	182
Настройка владельца и группы.....	184
9.7. Средства аудита .....	184
9.8. Действия в случае аварии.....	189
Составление плана действий на случай аварии .....	189
Создание аварийной загрузочной дискеты .....	190
Резервное копирование и восстановление в Linux .....	191
Создание резервной копии .....	193
Восстановление данных из копии .....	193

<b>Глава 10. Настройка Samba .....</b>	<b>194</b>
10.1. Общие сведения о Samba .....	194
10.2. Одноранговая сеть. Основной файл конфигурации Samba /etc/smb.conf.....	196
10.3. Samba в качестве PDC .....	199
10.4. Настройка входа в домен для Windows 98.....	202
Настройка входа .....	202
Устранение проблем в Windows 98 .....	207
10.5. Настройка входа в домен для Windows NT/2000.....	207
Создание учетных записей вручную .....	209
Настройка входа .....	209
10.6. Первый запуск Swat .....	216
10.7. Некоторые переменные Samba .....	219
10.8. Автоматический запуск Samba .....	219
<b>Глава 11. Службы DNS и DHCP.....</b>	<b>221</b>
11.1. Краткая характеристика DNS.....	221
11.2. Как работает служба DNS.....	222
11.3. Пакет BIND и его компоненты.....	223
Утилита nslookup.....	224
Утилита dig .....	224
Утилита host .....	225
11.4. Как читать файл настроек BIND .....	225
Файл named.conf.....	225
Файлы баз данных зон.....	227
Запись SOA.....	227
Запись NS.....	229
Запись A.....	229
Запись PTR.....	229
Запись MX.....	230
Запись CNAME.....	230
Запись SRV.....	230
Запись TXT.....	230
11.5. Простой пример собственного домена.....	231
Проверка.....	233
11.6. Краткая характеристика DHCP.....	234
11.7. Файл настроек dhcpd и их параметры .....	235
Глобальные параметры .....	236
Опция subnet .....	237
Опция shared network .....	237
11.8. Установка DHCP-сервера. Связь DNS и DHCP.....	238
11.9. Запуск служб DNS и DHCP .....	240
11.10. Настройка клиентской части Windows 98 .....	241
11.11. Настройка клиентской части Windows 2000.....	242

<b>Глава 12. Запуск Apache и Webmin .....</b>	<b>244</b>
12.1. Почему Apache .....	244
12.2. Основы конфигурирования Apache .....	245
12.3. Базовые параметры, используемые при настройке Apache .....	245
12.4. Коды ошибок, выдаваемых сервером .....	247
12.5. Регистрация ошибок сервера .....	247
12.6. Настройка автоматического запуска Apache .....	249
12.7. Самый простой способ организовать Web-сервер в организации .....	250
Настройка Apache .....	251
Настройка клиентов .....	252
Создание информационного наполнения сервера .....	253
12.8. Краткие сведения о Webmin и запуск .....	254
12.9. Настройка Webmin .....	257
<b>Глава 13. Антивирусная защита .....</b>	<b>261</b>
13.1. Установка drwebd и настройка скрипта запуска .....	262
13.2. Проверка работоспособности drwebd .....	263
13.3. Установка Samba Spider .....	264
13.4. Настройка действия антивируса на Samba .....	265
<b>Заключение .....</b>	<b>267</b>
<b>ПРИЛОЖЕНИЯ .....</b>	<b>269</b>
<b>Приложение 1. Полезные сочетания клавиш и некоторые команды .....</b>	<b>271</b>
<b>Приложение 2. Аналоги Linux и Windows-программ .....</b>	<b>274</b>
Постановка задачи .....	275
Поиск аналогов используемых программ для Linux .....	275
Установка программного обеспечения и обучение работе .....	275
<b>Приложение 3. Источники информации о Linux .....</b>	<b>276</b>
Русскоязычные источники .....	276
Англоязычные ресурсы .....	276
<b>Предметный указатель .....</b>	<b>277</b>





## Глава 1

# Характеристика протокола TCP/IP

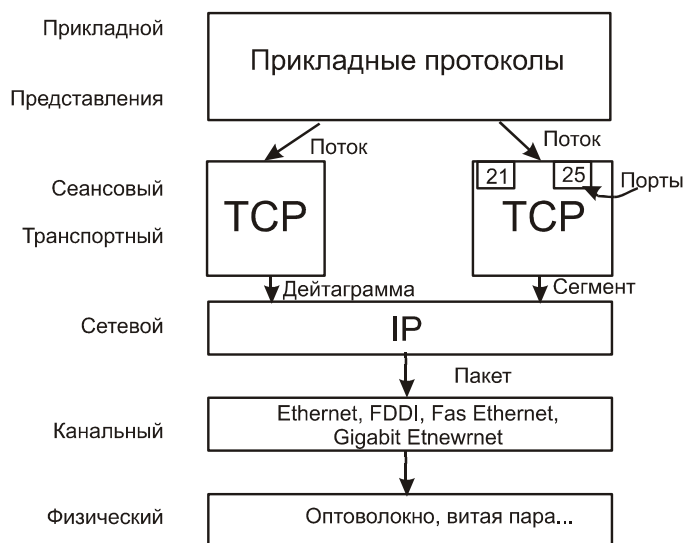
### 1.1. Модель OSI

На основании опыта, полученного при создании сетей, в середине 1980 гг. прошлого века была разработана модель, которая сыграла важную роль в развитии сетевых технологий. Речь идет о модели OSI (Open System Interconnection — взаимодействие открытых систем). Модель OSI определяет стандартные уровни взаимодействия систем и функции каждого из уровней. Иными словами, модель OSI является многоуровневым набором протоколов. При развитии программных или аппаратных средств переписывается не весь протокол заново, а лишь необходимая часть.

Модели OSI разделяет средства взаимодействия на семь уровней: прикладной (его еще называют уровнем приложений, строго говоря, не совсем корректно), представления, сеансовый, транспортный, сетевой, канальный и физический (рис. 1.1).

Каждый уровень выполняет определенные функции и обеспечивает связь со смежным уровнем (представляет вышестоящему уровню определенный сервис и может запросить у нижестоящего уровня сервис для себя). Это позволяет обеспечить независимость высоких уровней от технических деталей более низких.

- ❑ Прикладной уровень позволяет пользователям или приложениям получать доступ к сетевым ресурсам: файлам, web-страницам, принтерам, электронной почте.
- ❑ Уровень представления обеспечивает интерпретацию данных и их подготовку для прикладного уровня (на принимающем компьютере), а также прием данных от прикладного уровня в формат сеансового уровня (на передающем компьютере). Этот уровень имеет дело с представлением данных, не меняя их сути. Этот уровень также осуществляет защиту данных в сети (шифрование, например SSL) и сжатие данных.



**Рис. 1.1.** Стек TCP/IP и модель OSI

- ❑ Сеансовый уровень устанавливает соединение между двумя компьютерами. Управляет этим соединением, восстанавливает и завершает его при необходимости. Этот уровень также отвечает за синхронизацию и содержит дополнительные функции управления.
- ❑ Транспортный уровень обеспечивает вышестоящим уровням передачу данных с необходимой степенью надежности. Он отвечает за распознавание и коррекцию ошибок. Также он определяет класс сервиса: срочность, надежность, возможность восстановления. Самый низкий класс сервиса 0, самый высокий 4.
- ❑ Сетевой уровень. Функции сетевого уровня достаточно разнообразны, фактически он образует единую систему, объединяющую сети с различными принципами передачи сообщений.

Прикладной, уровень представления, сеансовый, транспортный и сетевой уровни реализуются программно.

- ❑ Канальный уровень реализует связь между сетевым и физическим уровнем, выполняет функции проверки доступности среды, проверяет корректность передачи кадров. Функции канального уровня реализуются сетевыми адаптерами и их драйверами.
- ❑ Физический уровень определяет электрические, оптические, механические и другие параметры взаимодействия в сети. Он регламентирует тип физической среды передачи, метод кодирования, скорость передачи. Физический уровень реализуется сетевым адаптером и средой передачи (витая пара, оптоволокно).

## 1.2. Стек TCP/IP

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — Протокол управления передачей/Межсетевой протокол) был разработан более двадцати лет назад по инициативе Министерства обороны США и внедрен в сети ARPANET и MILNET. Из объединения этих сетей и родился Интернет. Большую роль в популяризации TCP/IP сыграла его реализация в ОС UNIX. Сегодня протокол TCP/IP реализован во всех распространенных операционных системах: MS Windows, Novell, Linux.

Соответствие стека протоколов TCP/IP и модели OSI приведено на рис. 1.1. Набор протоколов TCP/IP захватывает транспортный сетевой и сеансовый уровни. Поверх TCP/IP работают протоколы более высокого уровня: Telnet, SNMP, FTP, HTTP.

Протокол TCP примерно соответствует сеансовому и транспортному уровням модели OSI, с его помощью реализуется сеанс связи между двумя компьютерами. Протокол TCP формирует из потока данных сегменты и контролирует прохождение сегмента по сети. К его функциям относится исправление ошибок и отслеживание прохождения пакетов по сети. При необходимости протокол организует повторную передачу потерянных или поврежденных сегментов. Таким способом достигается необходимая надежность, поскольку протокол IP не отвечает за доставку сообщений. При прохождении данных протокол TCP добавляет к ним свою служебную информацию.

Протокол IP (Межсетевой протокол) отвечает за маршрутизацию сегментов TCP. В его функции входит формирование IP-пакетов из данных на его входе, а также межсетевая адресация. По сути, протокол TCP использует IP-протокол в качестве транспортного средства. При прохождении IP пакета между сетями он упаковывается в соответствующие каждой конкретной сети средства транспортировки. Очень важно, что протокол IP рассматривает каждый IP-пакет как независимую единицу. Здесь нет средств контроля доставки пакетов. Если узел передал IP-пакет, то судьба этого пакета его уже не интересует. Все вопросы обеспечения надежности обеспечивает протокол TCP. Именно он организует повторную передачу, если какой-то из IP-пакетов потерялся. Протокол IP, как и протокол TCP, добавляет к данным служебную информацию своего уровня. Затем пакет продвигается по канальному и физическому уровню, где к нему добавляется соответствующая служебная информация.

Полезно будет вспомнить терминологию, применяемую в этой области.

*Поток* — данные, поступающие на вход протоколов TCP (и UDP). *Сегмент* — единица данных протокола TCP. *Дейтограмма* — единица протокола UDP. Единица данных протокола IP называется *пакетом*. *Порт* — уникальный идентификационный номер, который протокол TCP присваивает

приложению, использующему его в качестве транспорта. Все порты с номером меньше 1024 используют определенные приложения. Номера портов больше 1024 могут использоваться пользователем произвольно. В табл. 1.1 приведены номера портов некоторых известных служб. Номер порта и IP-адрес образуют *гнездо* (socket).

**Таблица 1.1.** Номера некоторых стандартных портов

Номер	Служба	Примечание
20	FTP-DATA	Протокол передачи данных FTP, данные
21	FTP	Протокол передачи данных FTP, управление
23	TELNET	Telnet
25	SMTP	Простой протокол передачи сообщений (Передача почты)
53	DNS	Службы доменных имен
69	TFTP	Упрощенный протокол передачи данных
70	GOPHER	Gopher
80	HTTP	Протокол передачи гипертекста
110	POP3	Post Office Protocol (Получение почты)
156	SQL	Служба SQL

Чтобы различать узлы, входящие в сеть, существует специальная система адресов. Адреса бывают трех типов:

Локальный адрес — адрес, определяемый технологией данной сети. Если речь идет о локальной сети, то это MAC-адрес (адрес, присвоенный производителем сетевой карте или порту маршрутизатора). Этот адрес уникальный, он назначается сетевой карте производителем. Адрес содержит 6 байтов: 3 байта выделяется централизованно под номер производителя, 3 байта назначается самим производителем под уникальный номер изделия. Локальный адрес имеет следующий вид: A7-B8-C4-11-D5-1F.

IP — это адрес, на основании которого протокол IP осуществляет доставку пакетов. Это адрес представляет собой 4 байта. Поскольку оперировать с двоичными цифрами человеку сложнее, то записывается IP-адрес в десятичной системе с разделением байтов точками. Например, адрес компьютера в локальной сети может выглядеть так: 192.168.10.12, на самом деле это 11000000 10101000 00001010 00001100.

Символьное или доменное имя. Поскольку человеку достаточно сложно запоминать комбинации из четырех групп цифр, то в соответствие IP-адресам

были поставлены символьные имена. С таким типом адресов вы сталкиваетесь в Интернете. Подробнее об этом мы поговорим, когда речь пойдет о службе DNS.

Теперь поговорим об IP-адресах подробнее. Собственно IP-адрес состоит из двух частей: номера сети и номера узла в этой сети. IP назначается во время установки или настройки оборудования администратором сети. Для назначения IP-адресов существуют определенные правила. В сети Интернет выдачей IP-адресов заведуют специальные службы (NIC), и выбирать произвольный адрес нельзя. В локальных сетях все немного проще, в принципе вы можете присваивать любые адреса. Однако если локальная сеть подключена к Интернету (или в обозримом будущем подключение произойдет), то при назначении адресов узлов в локальной сети необходимо придерживаться определенных правил. Для того чтобы их лучше понять, рассмотрим классы IP-адресов.

Как вы знаете, одна часть IP-адреса — это номер сети, а другая — номер узла. То, какая часть относится к номеру сети, а какая к номеру узла, определяется по первым битам в IP-адресе. Существуют 5 классов IP сетей (рис. 1.2).

Класс	1 байт	2 байт	3 байт	4 байт	Наименьш. номер сети	Наибольш. номер сети	Число узлов в сети
A	0				1.0.0.0	126.0.0.0	$2^{24}$
B	10				128.0.0.0	191.255.0.0	$2^{16}$
C	110				192.0.1.0	223.255.255.0	$2^8$
D	11110	Адрес группы Multicast			224.0.0.0	239.255.255.255	
E	111110	Зарезервирован			240.0.0.0	247.255.255.255	

Обозначения:

Адрес сети
Адрес узла

Рис. 1.2. Структура IP-адреса и классы IP сетей

Особыми являются класс D и класс E. Класс D начинается с последовательности 1110 и является групповым адресом — *multicast*. Сообщение, которое содержит адрес класса D, получают все узлы с этим адресом. Класс E начинается с последовательности 11110 и зарезервирован для будущего.

Помимо этих классов, существуют еще так называемые специальные IP-адреса:

- ☐ Адрес, состоящий из двоичных нулей, означает адрес узла сгенерировавшего пакет.
- ☐ Если в номере сети стоят нули, то считается, что узел назначения принадлежит к той же сети, что и узел, отправивший пакет.
- ☐ Пакет, состоящий из одних единиц, рассылается всем узлам в той сети, где находится источник сообщения.

- ❑ Если в поле номера узла стоят единицы, такой пакет рассылается всем узлам с указанным номером сети.
- ❑ Адрес, начинающийся с 127, предназначен для организации тестирования программ и взаимодействия процессов в рамках одной машины без передачи пакетов в сеть. Этот адрес имеет имя `loopback` (петля).

Помимо этих ограничений, для назначения IP-адресов в локальной сети существуют еще несколько правил. Для локальных сетей зарезервированы специальные диапазоны адресов:

- ❑ в классе А это диапазон 10.0.0.0 — 10.255.255.255;
- ❑ в классе В это диапазон 172.16.0.0 — 172.31.0.0;
- ❑ в классе С это диапазон 192.168.0.0 — 192.168.225.0.

Для разделения номера узла и номера сети может использоваться маска. Маска — это двоичное число, оно содержит единицы в тех разрядах, которые относятся к адресу сети. Для системы адресации, основанной на классах, маски такие: А — 255.0.0.0, В — 255.255.0.0, С — 255.255.255.0. Используя маски, можно добиться более гибкой системы адресации.

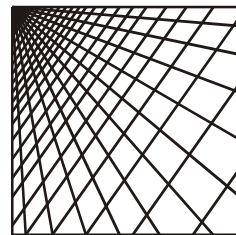
Теперь обратим внимание на то, что у нас есть два объекта: IP-адрес и MAC-адрес (локальный адрес). Эти два адреса не связаны между собой. Для того чтобы IP-пакет попал на нужный локальный узел, необходимо этот пакет перед отправкой в сеть снабдить MAC-адресом, соответствующим IP-адресу назначения. При отсутствии этого адреса у отправителя на помощь приходит ARP-протокол (Address Resolution Protocol — протокол разрешения адреса).

Узел формирует широковещательный ARP-запрос, и все узлы получают его. Затем они сравнивают IP-адрес со своим адресом, при совпадении формируется ответ, в который вкладывается искомый MAC-адрес.

Существует протокол, выполняющий обратную функцию: RARP (Reverse Address Resolution Protocol — протокол обратного разрешения адреса).

С начала 1990-гг. прошлого века началось бурное развитие Интернета, что в конечном итоге привело к дефициту IP-адресов. Одним из выходов из создавшегося положения является внедрение протокола IPv6, в котором для адресации используется уже не  $8 \times 4 = 32$  бита, а 128 битов. Также увеличено и число уровней иерархии. Введена двухуровневая иерархия провайдеров и трехуровневая — для абонентов. Это резко повышает количество доступных адресов и должно снять проблему нехватки свободных адресов.

Совместимость с текущей IPv4-версией обеспечивается ведением специального типа адресов — IPv4 compatible, где в старших 96 разрядах содержатся нули, а младшие 32 соответствуют адресу IPv4. Кроме этого, в протоколе IPv6 реализуются новые технологии защиты.



## Глава 2

# Технологии локальных сетей

## 2.1. Кабели, используемые в локальных сетях

В локальных сетях небольших предприятий на сегодняшний день наиболее используемым стал кабель на основе неэкранированной витой пары UTP. Однако это далеко не единственный кабель, применяемый в современных сетях. Более того, построение сетей исторически началось на других типах кабеля. В некоторых сетях, оставшихся как наследие прошлого, используются коаксиальные кабели. Любой кабель имеет множество характеристик, определяющих возможности его использования. Наиболее важными характеристиками являются:

- ❑ активное сопротивление — сопротивление кабеля по постоянному току. Как правило, нормируется на определенную длину, поскольку с увеличением длины кабеля сопротивление растет;
- ❑ погонная емкость — это емкость между двумя проводниками или между проводником и оплеткой кабеля. Нормируется тоже на единицу длины кабеля. Погонная емкость приводит к тому, что высокочастотный сигнал затухает по мере продвижения его по кабелю. Погонная емкость является паразитным параметром, и ее стремятся снизить;
- ❑ волновое сопротивление (импеданс) представляет собой полное сопротивление кабеля. Как правило, значение сопротивления приводится для определенной частоты, поскольку с ростом частоты оно изменяется;
- ❑ затухание — параметр говорит сам за себя. Затухание измеряется в децибелах на единицу длины и частоту сигнала;
- ❑ перекрестные наводки. Суть явления в следующем. Если есть два параллельных проводника, и по одному из них идет высокочастотный сигнал, на втором кабеле образуется паразитное напряжение от первого. Величина перекрестных наводок измеряется в децибелах и нормируется на определенную частоту.

Рассмотрим основные типы кабелей, используемых в локальных сетях, и их характеристики.

## Коаксиальный кабель

Коаксиальный кабель используется в самых различных областях техники. Кабель представляет собой центральную медную жилу, которая окружена диэлектриком. Затем идет медная оплетка, которая защищает центральную жилу от внешнего излучения, а также предотвращает излучение во внешнюю среду. Наиболее известный среди обывателей коаксиальный кабель — это телевизионный кабель (волновое сопротивление 75 Ом). В компьютерных сетях применяются кабели RG-8 и RG-11 (так называемый "толстый" коаксиальный кабель), их волновое сопротивление 50 Ом, внешний диаметр 0,5 дюйма. Также используются кабели RG-58 ("тонкий" коаксиальный кабель) — волновое сопротивление 50 Ом, внешний диаметр 0,25 дюйма (рис. 2.1, а).

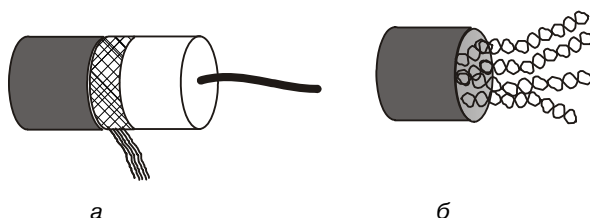


Рис. 2.1. Коаксиальный кабель и витая пара

## Кабель на основе неэкранированной витой пары

UTP (Unshielded Twisted Pair) — неэкранированная витая пара (рис. 2.1, б). Представляет собой набор из 4-х пар кабеля, скрученных попарно. Затем эти пары скручены между собой. Витая пара делится на семь категорий (UTP1 — UTP7). Кабели первой и второй категорий сегодня применяются только для телефонных сетей. Кабели третьей, четвертой и пятой категорий широко используются для построений компьютерных сетей. Кабель третьей категории был стандартизирован в 1991 г. для работы на частотах до 16 МГц. Небольшим улучшением кабеля третьей категории послужил кабель четвертой категории, который допускал работу уже на частотах до 20 МГц. Кабель пятой категории разрабатывался специально для работы сетевых высокочастотных протоколов в диапазоне до 100 МГц. Электрические характеристики кабелей UTP3—UTP5 приведены в табл. 2.1.

Таблица 2.1. Характеристики кабеля UTP3, UTP4, UTP5

Параметр	UTP3	UTP4	UTP5
Число пар	4	4	4
Волновое сопротивление	$100 \pm 15$ Ом	$100 \pm 15$ Ом	$100 \pm 15$ Ом



Таблица 2.1 (окончание)

Параметр	UTP3	UTP4	UTP5
Затухание (dB на 100 м)	4 МГц: 5.6 10 МГц: 9.8 16 МГц: 13.1	4 МГц: 4.3  10 МГц: 7.2  16 МГц: 8.9	16 МГц: 8.2 31 МГц: 11.7 100 МГц: 22
Перекрестное за- тухание не менее (dB)	4 МГц: 32 10 МГц: 26 16 МГц: 23	4 МГц: 47 10 МГц: 41 16 МГц: 38	16 МГц: 44 31 МГц: 39 100 МГц: 32

Кабели шестой и седьмой категорий работают на частотах до 200 и 600 МГц, соответственно. Их применение сдерживает относительно высокая цена.

## Кабель на основе экранированной витой пары

Shielded Twisted Pair (STP) — экранированная витая пара (рис. 2.2). Особенностью кабеля является наличие у него экрана. Это защищает его от внешних электромагнитных воздействий, а также снижает уровень излучения во внешнюю среду. Кабели на основе STP бывают девяти типов.

В локальных сетях применяется Type 1. Он представляет собой 2 пары скрученных проводов, экранированных оплеткой. По параметрам кабель Type 1 примерно соответствует кабелю UTP пятой категории. Однако его волновое сопротивление 150 Ом. Поэтому при применении его в качестве физической среды в локальных сетях необходимо обращать внимание на то, чтобы сетевое оборудование могло работать с волновым сопротивлением 150 Ом. В противном случае из-за несовпадения волнового сопротивления кабеля и активных сетевых устройств в местах их соединений будут образовываться отраженные волны. Результатом может стать непредсказуемое поведение сети и возникновение сбоев в ее работе.

Недостатком является необходимость хорошего заземления, а также более сложная по сравнению с UTP прокладка кабеля.

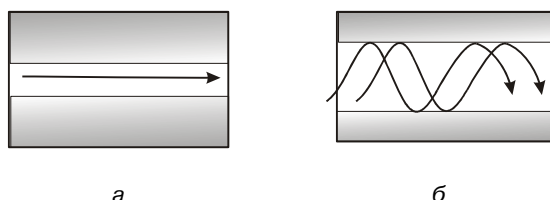


Рис. 2.2. а — одномодовый и б — многомодовый оптический кабель

## Волоконно-оптический кабель

Волоконно-оптические кабели представляют собой кабель из материала, проводящего свет. (В качестве источников излучения используются либо светодиоды, либо лазеры.) Показатели оптического преломления различны у центральной части и у внешней оболочки. В результате луч света не выходит за пределы центральной части оптического волокна. Различают многомодовые (Multi Mode Fiber — MMF) и одномодовые (Single Mode Fiber — SMF) оптические кабели (рис. 2.2). В многомодовых кабелях используется диаметр внутреннего проводника около 50 мкм. В результате внутри кабеля существует несколько световых лучей. В одномодовых кабелях диаметр внутренней части составляет менее 10 мкм. Это сравнимо с длиной волны используемого светового излучения. В результате световой пучок распространяется вдоль оптического кабеля. Одномодовые кабели имеют более широкую полосу пропускания за счет отсутствия потерь при отражении, однако так как волокно очень тонкое, монтаж одномодового волокна — чрезвычайно трудоемкая процедура, и ей должны заниматься специалисты.

Несмотря на множество преимуществ, у оптического кабеля есть один важный недостаток — более сложный монтаж сети.

## 2.2. Стандарты сетей

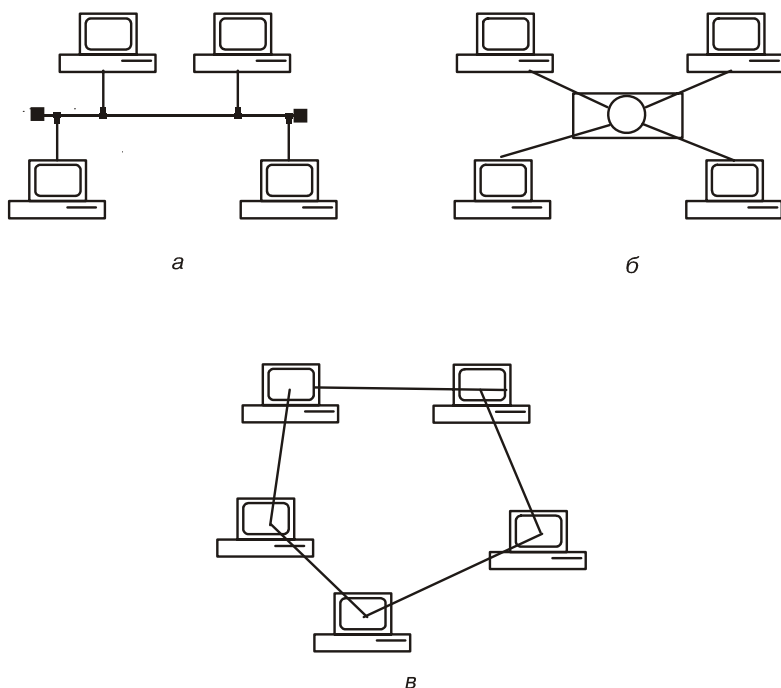
Изначально при разработке технологии локальных сетей разработчики основное внимание уделяли созданию простых, надежных и дешевых способов соединения компьютеров в локальную сеть. Поэтому одним из первых было решение об использовании единой разделяемой во времени среды передачи. С физической точки зрения сеть, объединяющая несколько компьютеров, может иметь различную топологию. Наиболее интересны с точки зрения локальных сетей следующие варианты:

- ❑ Общая шина — компьютеры подключены к общему кабелю. Применение такой технологии удешевляет прокладку сети. Однако есть серьезный недостаток — низкая надежность. Любой дефект кабеля или разьема приводит к остановке всей сети.
- ❑ Звезда — в этом случае каждый компьютер подключается отдельным отрезком кабеля к устройству, находящемуся в центре сети. Это устройство называется концентратор. Фактически концентратор передает сигнал с одного из своих входов на все выходы, за исключением того, с которого пришел этот сигнал. Основное преимущество (по сравнению с общей шиной) — это более высокая надежность, ведь повреждение отдельного кабеля сказывается только на работе одного участка сети и не затрагивает все остальные.

- ❑ Кольцо — данные передаются по кольцу в одном направлении. Незначительным недостатком является то, что при применении кольцевой топологии приходится принимать меры по повышению надежности сети, чтобы выход из строя одного узла не повлиял на работу остальных узлов сети.

Схемы физической топологии приведены на рис. 2.3. Построение сети по принципу общей шины или кольца имеет более низкую надежность и более низкую пропускную способность. Это привело к тому, что в современных локальных сетях небольшого размера, как правило, применяется звездообразная топология. Кроме того, появление новых устройств: мостов, коммутаторов, маршрутизаторов — сняло проблему единой разделяемой среды данных.

Быстрые темпы развития сетевых технологий требовали необходимости принятия стандартов. В начале 1980-х гг. прошлого века был разработан и принят стандарт IEEE 802.x. Основой для его создания послужили существовавшие на тот момент внутрифирменные стандарты ведущих производителей компьютерной техники.



**Рис. 2.3.** Физические топологии сетей: а — шина, б — звезда, в — кольцо

Стандарты IEEE 802.x определяют технологии, касающиеся двух нижних уровней модели OSI. Состав стандартов 802.x приведен в табл. 2.2.

**Таблица 2.2.** Основные стандарты 802.x

Номер	Наименование
802.1	Internetworking, объединение сетей
802.2	Local Link Control — управление логической передачей данных
802.3	Сети Ethernet
802.4	Сети Token Bus LAN
802.5	Сети Token Ring LAN
802.6	Metropolitan Area Network — сети крупных городов
802.7	Board Technical Advisor Group — группа консультаций по широкополосной передаче
802.8	Fiber Optic Techical Advisory Group — группа консультаций по оптоволоконным сетям
802.9	Integrated Voice and data Networks — интегрированные сети передачи данных и голоса
802.10	Network Security — сетевая безопасность
802.11	Wereless LAN — беспроводные сети

С практической точки зрения наибольший интерес для нас представляют сети Ethernet (802.3) и Fast Ethernet (802.3u). На сегодняшний день это самый распространенный стандарт построения локальных сетей. Причем практически все вновь создаваемые сети строятся по технологии Fast Ethernet. Технология Fast Ethernet отличается от технологии Ethernet только на физическом уровне. Кроме того, в некоторых организациях сети Ethernet еще действуют, поэтому вначале мы рассмотрим технологию Ethernet.

## 2.3. Технология Ethernet

В зависимости от типа физической среды различают следующие виды стандартов сетей Ethernet:

- ☐ 10Base-5;
- ☐ 10Base-2;
- ☐ 10Base-T;
- ☐ 10Base-F.