Д. КОЛИСНИЧЕНКО

САМОУЧИТЕЛЬ системного администратора Linux

- Дистрибутивы Fedora 13, Mandriva 2010.1 Spring, openSUSE 11.3, Ubuntu 10
- Установка и настройка операционной системы
- Подробное рассмотрение файловой системы Linux
- Настройка сети и маршрутизации без конфигураторов
- Брандмауэры iptables и ebtables, chroot-окружение
- Настройка серверов: Web, FTP, DNS, DHCP, почтового и сервера баз данных
- Прокси-серверы Squid и SquidGuard
- Linux-сервер в Windows-сети: свой среди чужих
- Виртуальные частные сети (VPN)
- Создание LiveCD
- Сетевой сканер nmap
- Система управления доступом Tomoyo
- Защита и оптимизация Linux-сервера
- Автоматизация задач с помощью bash
- Программные RAID-массивы

СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Денис Колисниченко

САМОУЧИТЕЛЬ системного администратора Linux

Санкт-Петербург

«БХВ-Петербург»

2011

УДК 681.3.06
ББК 32.973.26-018.2
К60

Колисниченко Д. Н.

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

ISBN 978-5-9775-0639-7

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

Для администраторов Linux

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

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

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 03.11.10.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 43,86.
Тираж 1800 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12.

ISBN 978-5-9775-0639-7

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

Оглавление

Введение

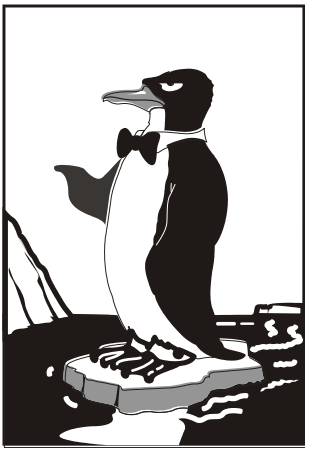
На этот раз введение не будет длинным. Тому есть две причины. Во-первых, не хочется занимать ваше драгоценное время. Во-вторых, как показывает практика, больше половины читателей считают введение чем-то скучным и вообще его не читают. Зачем же тратить время и бумагу?

Хочется сказать несколько слов об особенностях этой книги, которые выделяют ее среди других книг, посвященных системному администрированию Linux. Я старался написать ее так, чтобы она не стала "еще одной книгой по настройке Linux-сервера". В ней есть все, что нужно знать будущему системному администратору. Так, в первой части книги рассматриваются основы основ: принципы работы компьютерных сетей, адресация в сетях, монтаж сети. Все это подано настолько подробно, чтобы у будущего администратора не возникали вопросы типа "А что такое сетевая маска?" или "Как обжать витую пару?". Могу с уверенностью сказать, что благодаря этой информации вы не только настроите Linux-сервер, но сможете построить локальную сеть.

В остальных частях книги рассматривается настройка Linux (в том числе и настройка сети — как же без нее?), установка программного обеспечения, настройка сетевых служб (Apache, DNS, DHCP, ssh, Squid и т. д.). Особое внимание уделяется безопасности настраиваемого сервера — как локальной, так и безопасности в сети: подробно описываются создание шлюза (маршрутизатора), конфигурирование брандмауэра iptables, а также настройка виртуальной частной сети. Вопросам безопасности в книге действительно уделяется много внимания, а помимо всего прочего мы рассмотрим и сканер nmap — чтобы администратор мог сам просканировать свою сеть на предмет потенциальных уязвимостей.

Материал книги основан на дистрибутивах Fedora 13, Mandriva 2010.1 Spring, openSUSE 11.3, Ubuntu 10.04, Debian 5 и Slackware 13. Учитывая столь обширный список дистрибутивов, могу с уверенностью сказать, что книга подойдет большинству администраторов.

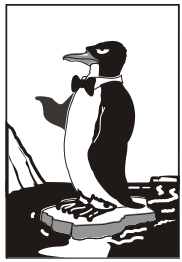
Вот теперь можно с чистой совестью приступить к чтению книги. И даже если вы не новичок, а действующий администратор, рекомендую все-таки прочитать первую часть книги — в ней вы найдете для себя много полезного.



ЧАСТЬ I

Основы администрирования

Первая часть посвящена основам администрирования. Мы рассмотрим краткую историю Linux, основы сетевого взаимодействия, познакомимся с моделью OSI, адресацией в TCP/IP-сетях, с монтажом сетей Ethernet и Wi-Fi. А в следующей части книги поговорим об установке и настройке Linux.



Глава 1

Становимся администратором

1.1. Краткая история Linux

В далеком 1969 году сотрудники фирмы Bell Labs пытались возродить ОС Multics, но превзошли сами себя, и то, что получилось, уже никак не тянуло на обычный "апгрейд" для Multics — это была совершенно новая операционная система, которую назвали UNIX. Интересно, что поначалу UNIX называлась "UNICS", но позже американцы, как они это любят делать, немного упростили название системы.

В начале 70-х годов прошлого века ОС UNIX была существенно доработана. В ее ядро добавили много новых функций, а главное — она была переписана на языке C, что обеспечило легкость переноса этой ОС на другие аппаратные платформы (первоначально UNIX была написана на ассемблере и предназначалась для компьютера PDP-7).

Важно, что с самого рождения UNIX была многопользовательской и многозадачной. Таким образом, идеи, заложенные в представленную в 1995 году Windows 95, оказались, по сути, идеями 20-летней давности — в UNIX все это уже было реализовано 20 лет назад. Да, не было красивого "фантика" — графического интерфейса, — но ведь не это главное в операционной системе.

В начале 1980-х годов появились первые персональные компьютеры фирмы IBM. Однако мощности IBM PC никак не хватало для запуска UNIX. Поэтому в мире персональных компьютеров десять лет царствовала операционная система DOS компании Microsoft. Начиная с 1990-х все изменилось — мощность "персоналок" уже позволяла запускать UNIX. К этому времени (прошло более 20 лет с момента появления первой версии UNIX) разными фирмами, университетами и отдельными энтузиастами было создано много UNIX-подобных операционных систем (IRIX, XENIX, HP-UX, BSD, Minix и др.).

Огромное значение в развитии Linux сыграла одна из UNIX-подобных операционных систем — Minix, которая не была полноценной системой, а создавалась, чтобы демонстрировать основные принципы и устройство настоящих операционных систем. Да, она не была совершенной, но зато ее исходный код (всего 12 тысяч строк) был опубликован в книге А. Таненбаума "Операционные системы". Именно эту книгу и купил Линус Торвальдс (Linus Torvalds).

В 1991 году Линус Торвальдс установил на свой компьютер ОС Minix, но та не оправдала его ожиданий, поэтому он принял решение несколько ее переработать — ведь исходные коды вместе с комментариями были под рукой. Сначала Торвальдс

просто переписал программу эмуляции терминала, а затем фактически взялся за создание собственной операционной системы.

25 августа 1991 года ОС Linux (версия 0.01) была создана. Конечно, это была не та Linux, что есть сейчас, но она уже тогда была лучше Minix, поскольку в ней запускались командный интерпретатор bash и компилятор gcc. Сообщение о создании новой операционной системы было помещено в группу новостей comp.os.minix, там же предлагалось всем желающим протестировать ее.

С этого и началось интенсивное развитие Linux, а к ее разработке в помощь Торвальдсу подключились энтузиасты со всего мира, — ведь ничто так не сокращает расстояния, как Интернет. С момента появления версии 0.01, которой практически нельзя было пользоваться, до создания версии 1.0, пригодной для обычных пользователей, а не программистов, прошло почти три года (она появилась в апреле 1994 года). И уже эта первая версия обладала поддержкой сети (поддерживался протокол TCP/IP), а также графическим интерфейсом X Window, появившимся в Linux еще в 1992 году одновременно с поддержкой TCP/IP.

Первые версии Linux распространялись на обыкновенных дискетах. Комплект состоял из двух дискет: первая содержала ядро, а вторая — корневую файловую систему и необходимые программы. Установить подобную версию Linux на компьютер мог только специалист. Чуть позже появились первые дистрибутивы, которые, помимо того же ядра и корневой файловой системы, включали также программу для установки всего этого на компьютер. Программа установки поставлялась, как правило, на отдельной дискете.

Первые дистрибутивы появились в 1992 году — тогда отдельные энтузиасты или группы энтузиастов выпускали разные дистрибутивы (каждый, естественно, под своим именем). Фактически они отличались друг от друга лишь названием и программой установки. В дальнейшем различия между дистрибутивами стали более существенными.

Самый первый дистрибутив, созданный в Манчестерском компьютерном центре (Manchester Computing Centre, MCC), появился в начале 1992 года и назывался MCC Interim Linux. Чуть позже появился дистрибутив TAMU, разработанный в Техасском университете.

Настоящий прорыв произвел дистрибутив SLS, выпущенный в октябре 1992 года, поскольку именно он содержал поддержку TCP/IP и систему X Window. Впоследствии данный дистрибутив бурно развивался и постепенно трансформировался в один из самых популярных дистрибутивов — Slackware.

Со временем дистрибутивы разрослись до таких размеров, что распространять их на дискетах стало нельзя. Вы можете себе представить дистрибутив на 50 дискетах (дистрибутивы того времени занимали 50–70 Мбайт)? А что делать, если, скажем, дискета № 47 окажется бракованной? Как раз к тому времени лазерные компакт-диски и их приводы немного подешевели, и компания Red Hat стала одной из первых, выпустивших свою разработку на компакт-диске.

Кроме получения на дискетах или компакт-диске, дистрибутив того времени (как, впрочем, и сейчас) можно было бесплатно скачать из Интернета (если не считать стоимости самого Интернета). Но далеко не все могли себе позволить Интернет в online-режиме (тогда online-режимом считалась работа с WWW, а offline — с почтой и новостями Usenet). Да и привод CD-ROM (односкоростной) стоил около

100 долларов. Поэтому в начале 1990-х основными носителями для распространения Linux все же были дискеты. А вот начиная с середины 1990-х Linux постепенно почти полностью перекочевала на компакт-диски.

О дистрибутивах можно говорить еще очень долго. Важно запомнить следующее:

- основные дистрибутивы: Red Hat, Slackware и Debian, все остальные — это производные от них. Например, Mandrake произошел от Red Hat, ALT Linux потом взял за основу Mandrake, а ASPLinux — Red Hat. Потом на смену Red Hat пришел дистрибутив Fedora Core (сейчас просто Fedora), а на смену Mandrake — Mandriva;
- номер версии дистрибутива не совпадает с номером ядра — это принципиально разные вещи.

1.2. Почему именно Linux?

А почему именно Linux? Почему бы не использовать ту же FreeBSD, у которой родства с UNIX намного больше, чем у Linux? На базе FreeBSD, как и на базе Linux, можно построить стабильный сервер. Но у Linux есть одно неоспоримое преимущество — она популярнее. А это значит, что для нее больше русскоязычной документации, на Linux уже обращают внимание производители оборудования (вы без особых проблем найдете драйвер для вашего "железа"), да и Linux более дружественна к пользователю. Да, именно к пользователю. Конечно, для администратора сервера это не столь важно, но Linux более универсальна, что позволяет ее использовать как на сервере, так и на рабочих станциях. Получается, что можно установить одну и ту же операционную систему на всех компьютерах сети — следовательно, вам будет проще обслуживать эту сеть, чем "разношерстную" сеть, где компьютеры работают под всевозможными версиями Windows, Mac OS и Linux.

1.3. Основные задачи системного администратора

Сейчас мы рассмотрим основные задачи системного администратора. У нас ведь как бывает: сисадмин и монтажом сети занимается, и обучением пользователей (далеко не все умеют "на кнопки" нажимать). Поэтому сразу скажу: далее приведен список обязанностей администратора Linux-сервера, работающего в идеальных условиях.

- **Установка и настройка программного обеспечения** — после установки самой Linux вам нужно будет установить дополнительное программное обеспечение, например, Web-сервер, FTP-сервер, а затем настроить это программное обеспечение.
- **Управление пользователями** — в обязанности администратора также входит создание, модификация и удаление учетных записей пользователей сервера. Возможно, придется ограничить место на диске, предоставляемое каждому пользователю (эта операция называется *квотированием*).
- **Инсталляция и деинсталляция аппаратных средств** — кому как не администратору подключать новые жесткие диски и подготавливать их для использо-

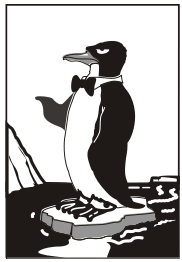
вания сервером. Причем часто бывает, что устанавливать "железо" (впрочем, как и "софт") придется не только на сервере, но и на рабочих станциях — такова уж судьба сисадмина…

- **Резервное копирование** — это одна из самых важных задач системного администратора. Часто резервное копирование, к сожалению, не выполняется или выполняется не так, как нужно. В результате — потеря данных. Да, это не интересно, да — это рутинно. Но выполнять эту задачу нужно.
- **Поиск неисправностей** — время от времени аппаратные средства выходят из строя. Иногда случаются "глюки" в программном обеспечении. Найти и устранить неисправность — задача системного администратора. Сразу предупреждаю: часто найти неисправность сложнее, чем ее устранить.
- **Защита сети.** Обеспечение безопасности сети и контроль защиты — очень важная задача, ведь вы же не хотите, чтобы ваш сервер взломали? Часто бывает, что "врага" нужно ожидать не извне, а изнутри — это могут быть любопытные либо недовольные пользователи, способные посягнуть на неприступность вашего сервера.
- **Мониторинг системы** — важно ежедневно просматривать журналы системы. В журналах можно найти много интересной и полезной информации: попытки взлома, ошибки в конфигурации системы и т. д.
- **Консультации и техническая поддержка пользователей** — чтобы не отвлекать вас от основных задач, желательно, чтобы эту задачу выполнял ваш помощник. Но если вы единственный администратор в компании, то этим придется заниматься лично вам.
- **Ведение локальной документации** — чтобы вам (или тому человеку, который, возможно, займет впоследствии ваше место) было проще в будущем, следует протоколировать все свои действия: разводку кабелей сети, инсталлируемые программные средства, изменения в конфигурации системы, изменения в схеме сети и т. д.

Вот теперь вы знаете, с чем вам придется столкнуться при выполнении своих обязанностей. Но это только базовый комплект — вполне возможно, что на практике появится еще несколько задач, которые вам придется решать.

Профессиональный праздник

Так уж получилось, что данная глава была написана в день системного администратора, поэтому не упомянуть об этом профессиональном празднике я просто не могу. День системного администратора отмечается в последнюю пятницу июля (в 2010 году это 30 июля). Основатель праздника — Тед Кекатос (Ted Kekatos), системный администратор из Чикаго. Именно он посчитал, что раз в году "бойцы невидимого фронта" должны чувствовать благодарность со стороны пользователей. Кстати, в США этот праздник называется День благодарности системному администратору (System Administrator Appreciation Day). Первый раз праздник был отмечен 28 июля 1999 года.



Глава 2

Классификация сетей

2.1. Краткая история сетей

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

2.1.1. 1941–1975 годы

Первый период развития вычислительных сетей начинается в 1941 году (тогда, если вы помните, появилась первая "большая" ЭВМ) и называется *лабораторным* — в то время сети, как впрочем и ЭВМ, не выходили за пределы лабораторий научных институтов. С самого начала ставилась задача объединения в сеть ЭВМ без привязки к конкретной аппаратуре.

Любопытно

Казалось бы, как давно это было! Но самое интересное, что мы до сих пор используем решения, разработанные в то время. Последовательный интерфейс RS-232C и параллельный интерфейс Centronics (да, тот, который служит для подключения принтеров) используются до сих пор. Интерфейс RS-232C постепенно вытесняется современными последовательными интерфейсами: USB и IEEE 1394 (FireWire), и на некоторых современных компьютерах его больше нет вообще. Однако интерфейс Centronics имеется на каждом современном стационарном компьютере, хотя большинство производителей принтеров уже практически перешло на USB. Наличие "старых" интерфейсов зависит только от производителя материнской платы — как он решит, так и будет. Мой компьютер, на котором я пишу эти строки, был куплен в феврале 2008 года. Тогда я не обратил внимания на наличие/отсутствие старых интерфейсов, но потом выяснилось, что на материнской плате отсутствует RS-232C, но имеется Centronics (LPT), а также USB, IEEE 1394, HDMI (правда, он не имеет никакого отношения к сетевым интерфейсам) и другие современные разъемы, которых не было на более старых компьютерах. С другой стороны, в продаже до сих пор имеются материнские платы с RS-232C, а также предлагаются отдельные PCI-контроллеры, добавляющие два порта RS-232C, если в них возникает острая необходимость.

Интерфейсы RS-232C и Centronics — это, в принципе, хорошо, но они годятся только для связи "точка–точка", то есть для непосредственной связи отправителя

и получателя данных. Понятно, что в сети может быть гораздо больше, чем две ЭВМ, поэтому разработчики сетей на этом не остановились, и в 1974 году компания IBM представила универсальную архитектуру вычислительных сетей: SNA (System Network Architecture). Эта архитектура, помимо всего прочего, поддерживала *адресацию узлов* сети, смысл которой в том, что каждому узлу сети присваивается уникальный адрес, по которому можно обратиться к этому узлу. Сейчас для адресации узлов преимущественно используются протоколы IPv4 и IPv6, о которых мы поговорим далее в этой главе.

2.1.2. 1976–1982 годы

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

В 1979 году был создан первый модем для персональных (!) компьютеров. Я даже догадываюсь, о чем вы сейчас подумали: какие, мол, персональные компьютеры в 1979 году? Какой модем? Да, Personal Computer (PC) от IBM появился в 1981 году, но это не означает, что до этого не было *персональных компьютеров*. Для работы с первыми ЭВМ обычно требовался целый штат специалистов, а персональный компьютер — это компьютер, предназначенный только для одного человека, для одного пользователя. И настоящие персональные компьютеры, отвечающие этому определению, появились еще до 1980 года — это были компьютеры компании Apple. А словосочетание "Personal Computer" — всего лишь название, правда, весьма удачное, продукта компании IBM. IBM первая ввела термин PC, и с того времени все компьютеры со сходной архитектурой команд считаются PC-совместимыми.

А все современные модемы являются Hayes AT-совместимыми, то есть совместимыми с набором AT-команд управления модемом, разработанным компанией Hayes. Первый модем Micromodem II был выпущен этой компанией в 1979 году. Он развивал скорость в 300 бод (бит/с) и предназначался для компьютеров Apple.

Еще в лабораторном периоде были разработаны *системы с произвольным доступом*. Впервые они были использованы в начале 1970-х годов в сети Alohanet, объединяющей Гавайские острова. Сначала эти системы считались бесперспективными, но в мае 1973 года Боб Меткалф (Bob Metcalf) усовершенствовал метод CSMA, на котором они были основаны. Усовершенствованный метод назвали CSMA/CD (Carrier-Sense Multiple Access with Collision Detection, множественный доступ с контролем несущей и обнаружением коллизий). Боб Меткалф планировал

использовать этот метод для совместного доступа к сетевым принтерам, но он позже "перерос" в то, что сейчас называется Ethernet-сетью. Тогда сеть CSMA/CD передавала данные по коаксиальному кабелю (как первые Ethernet-сети) со скоростью 2,94 Мбит/с (для того времени это была значительная скорость), а максимальное расстояние передачи данных составляло 1,5 км. В 1978 году Меткалф зарегистрировал компанию 3Com Corporation (наверное, все мы слышали название этой компании), а в 1982 году выпустил первый в мире серийный Ethernet-адаптер для компьютера Apple.

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

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

2.1.3. 1983–1989 годы

Начиная с 1983 года, в институтах и даже некоторых офисах стали появляться первые локальные сети, связывающие компьютеры толстым коаксиальным кабелем. В то время сетевой адаптер стоил очень дорого (например, для ЭВМ VAX стоимость сетевого адаптера превышала 3 тыс. долларов), поэтому локальную сеть могли себе позволить только самые крупные фирмы. Найти тогда "персоналку" с сетевым адаптером было сложно.

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

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

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

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

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

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

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

2.1.4. 1990–1995 годы

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

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

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

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

Следующим шагом в создании корпоративных сетей стало изобретение многопортового устройства — центрального коммутатора, в котором были объединены все мосты сети. Такая конфигурация получила название collapsed-backbone ("маги-

страль в точке"). Примерно в это же время родилось понятие *структурированных кабельных сетей* (СКС).

Понятно, что сети росли, и скорости 10 Мбит/с для магистрали стало недостаточно. На тот момент существовала всего одна "быстрая" технология, обеспечивающая передачу данных по оптоволоконному кабелю со скоростью 100 Мбит/с — FDDI (Fiber Distributed Data Interface, распределенный волоконный интерфейс данных). Но в 1992 году компания Grand Junction начала разработку Ethernet-сети, работающей на скорости 100 Мбит/с, и она была стандартизирована в 1995 году (стандарт IEEE 802.3u, сети 100Base-TX, 100Base-T4 и 100Base-FX). В том же 1995 году компания Grand Junction была поглощена компанией Cisco Systems: закон выживания — выживают лишь сильнейшие. После принятия стандартов 100Base-* спрос на технологию FDDI резко пошел вниз, поскольку Ethernet-сети обеспечивали ту же скорость передачи данных, но стоили намного дешевле только за счет среды передачи данных — витая пара стоит намного дешевле, чем оптоволокно. А в 1998 году появились Ethernet-сети, передающие данные со скоростью 1 Гбит/с, но об этом позже.

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

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

2.1.5. 1996–1999 годы

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

Зарождение высокоскоростного доступа произошло как раз в 1995–1999 годах, когда появились первые кабельные и ADSL-модемы. Кабельные модемы (они передают данные по сетям операторов кабельного телевидения) преимущественно применялись в США. В Европе получили большее распространение ADSL-модемы, использующие для передачи данных обычный телефонный кабель. К сожалению, в те годы в России о таких модемах только слышали, но никто их практически не видел.

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

2.1.6. 2000 — наше время

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

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

Если вы заметили, то в этой краткой истории практически ничего не было сказано о развитии беспроводных сетей. Это сделано умышлено. В *главе 6* мы поговорим о том, как данные передаются "по воздуху", рассмотрим краткую историю беспроводных сетей и существующие беспроводные стандарты.

2.2. Классификация сетей

Сети можно классифицировать по:

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

2.2.1. По занимаемой территории

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

- *локальные* (LAN, Local Area Network) — сети, занимающие небольшую территорию, например, одну комнату или одно здание;
- *региональные* (MAN, Metropolitan Area Network) — сети, охватывающие город (отсюда другое название — муниципальные) или даже область;
- *глобальные* (WAN, Wide Area Network) — такие сети охватывают территории одного или нескольких государств или даже весь мир. Пример всемирной сети — Интернет.

С локальными и глобальными сетями все понятно, разберемся с сетями региональными. Сеть MAN, как правило, объединяет в единое целое несколько сетей — например, сети двух или более зданий. При этом среда передачи данных сети MAN может быть как проводной, так и беспроводной.

Беспроводная сеть обходится намного дешевле, чем сеть на базе оптоволокна, но она менее надежна и менее безопасна. Тем не менее, беспроводные технологии очень полезны для MAN — не всегда есть возможность проложить кабель. С другой стороны, MAN часто выступает в качестве магистральной сети, поэтому производительности беспроводной сети может оказаться недостаточно.

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

2.2.2. По топологии

Существуют следующие топологии сети:

- *линейная* (рис. 2.1) — подключение по принципу гирлянды: каждый узел сети подключается к следующему узлу сети. В такой сети от узла с номером 1 до узла N будет всегда одинаковый маршрут: через узлы 2, 3, 4, …, $N - 1$. Понятно, в случае отказа одного из узлов сети, линейная сеть прекратит свое существование. В настоящее время линейные сети практически не используются (если не принимать во внимание нуль-модемное соединение);
- *кольцевая* (рис. 2.2) — каждый узел сети соединен с двумя соседними узлами, все узлы сети образуют кольцо. Кольцевая топология используется технологиями Token Ring, FDDI и некоторыми другими;
- *звездообразная* (рис. 2.3) — в такой сети есть один центральный узел, с которым связан каждый узел сети. Такие сети еще называются *централизованными*. "Падение" центрального узла означает "падение" всей сети. Обычно в качестве центрального узла используется концентратор (hub) или коммутатор (switch). Пример звездообразной сети — Ethernet на базе витой пары;
- *общая шина* (рис. 2.4) — все узлы сети подключаются к единой среде передачи данных, например, к коаксиальному кабелю. Слабое место такой сети — сама среда передачи данных: обрыв кабеля означает сбой всей сети. Пример сети на общей шине — Ethernet на базе коаксиала;
- *древовидная* (рис. 2.5) — топологию этой сети проще представить, чем описать или вникать в определение. В древовидной сети есть более двух конечных узлов и, по крайней мере, два промежуточных узла. В древовидной сети между двумя узлами есть только один путь. Чтобы вникнуть в правильное определение древовидной сети, нужно знать теорию графов, поскольку древовидная сеть — это неориентированный ациклический граф, не содержащий замкнутых путей и позволяющий соединить единственным образом пару узлов;