Red Hat Linux 9

架站实务

李蔚泽　编著

- 网络基本概念
- Apache服务器安装与设置
- FTP服务器——VSFTP
- 邮件服务器——Sendmail
- 与Windows的桥梁——SAMBA
- 高速缓存服务器——Squid
- NAT服务器与防火墙
- DNS服务器——BIND

机械工业出版社
China Machine Press

Red Hat Linux 9
架站实务

李蔚泽　编著

机械工业出版社

本书包含了 11 种常用的服务器以及网络基本概念的介绍，包括 Apache 服务器的安装与设置、多重网站与安全通信、Apache 服务器快速设置、FTP 服务器——VSFTP、邮件服务器——Sendmail、与 Windows 的桥梁——SAMBA、高速缓存服务器——Squid、NAT 服务器与防火墙、DHCP 服务器、DNS 服务器——BIND、网络磁盘驱动器——NFS、新闻服务器——INN 以及 OpenSSH 服务器等，内容丰富。

为了使读者能够融会贯通，本书在每章的开始都先说明了各类服务器的基本原理，接着再从架设开始逐步介绍，以提高读者掌握概念与实际操作的能力。为使读者能在最短的时间内轻松完成各种服务器的架站工作，在编写时舍弃了一般书籍庞杂的内容，取而代之的是核心部分的内容。

本书可以作为 Linux 短期培训、大中专院校相关专业学习的教材，同时也是广大 Linux 爱好者不可多得的一本参考书。

本书版权登记号：图字：01-2003-7228

图书在版编目（CIP）数据

Red Hat Linux 9 架站实务/李蔚泽编著.

-北京：机械工业出版社，2004.6

ISBN 7-111-13366-8

Ⅰ.R… Ⅱ.李… Ⅲ.①Linux 操作系统-基本知识 ②计算机网络-基本知识

Ⅳ.TP393.092

中国版本图书馆 CIP 数据核字（2004）第 050908 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

责任编辑：王金航 版式设计：谭奕丽

三河市宏达印刷有限公司印刷 · 新华书店北京发行所发行

2004 年 6 月第 1 版第 1 次印刷

787mm×1092mm 1/16 · 26.5 印张 · 636 千字

0001~5000 册

定价：38.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话：（010）68993821、88379646

封面无防伪标均为盗版

前　言

本书涵盖了大部分系统管理人员所需的内容，可满足一般用户入门及参考之用，这也是作者写作的初衷。

除了第 1 章的基本概念外，本书其余的章节共包含 11 种类型的服务器，这是撰写时遇到的首要难题，因为要以有限的篇幅来说明多类不同的服务器，其中有关内容的筛选，着实花费了许多时间。所幸有赖作者以往的经验，再辅以大量的参考文献，总算完成了令人满意的内容，相信读者在仔细阅读后，可以发现作者验证时的用心。

本书的第 1 章是有关网络的一些基本概念，这是所有服务器管理员所必备的基本知识，希望读者认真学习。第 2~4 章介绍了目前 Internet 上使用最多的 WWW 服务器——Apache，而第 5 章是有关 FTP 服务器的内容，因为这二者在 Internet 上的使用率相当高，所以一般企业的网络都会尽所能地在它们之上提供多样的服务，以吸引用户的访问。

第 6 章的邮件服务器也是企业网络必备的利器，因为在目前电子化的环境中，实在无法想象没有电子邮件的传递，企业是如何完成日渐繁复的商业活动的。而第 7 章介绍的 SAMBA 服务器是沟通 Windows 和 Linux 操作系统的绝佳工具，有了它，一般的用户就可轻易地通过“网上邻居”来存取 Linux 上的共享资料。

第 8 章和第 9 章主要的着眼点在于带宽使用率与安全性的提升。Proxy 服务器可以将常用的网页储存在硬盘中，以节省连接到 Internet 时消耗的带宽，而 NAT 服务器与防火墙则分别用来处理 IP 地址的不足以及保障网络安全性的解决方案。

第 10 章是有关 DHCP 服务器的内容，只要正确地使用它，就可以节省许多平时维护客户端 IP 组态的时间。而第 11 章介绍的 DNS 服务器在客户端连接 Internet 时，肩负着域名解析的工作，若没有这个机制，客户端很难顺利地连接到 Internet。

第 12 章的网络文件系统 NFS，则可利用分布式系统的概念，将网络上分散的共享资源，整合在服务器的文件系统中。第 13 章说明了新闻服务器的工作原理以及实际搭建时所需注意的内容。而最后一章是有关 OpenSSH 服务器的内容，正确地使用它，可以加强网络通信的安全性。

全书是作者花费许多研究测试的时间以及无数夜晚挑灯夜战下的成果，虽然辛劳，但只求能够满足读者的需求，同时也希望它是我们共同学习的起点。由于编者水平有限，如果本书有遗漏或不尽详细之处，恳请读者批评指正，以使本书更臻完美。

李蔚泽

jacklee1024@sinamail.com

目　录

前言

第 1 章　网络基本概念 1
1-1　TCP/IP 网络 2
1-2　OSI 七层模型 5
1-3　Linux 网络配置文件 7
1-4　系统维护常用的指令 14
1-4-1　设置网卡配置——ifconfig 指令 14
1-4-2　检测主机连接——ping 指令 17
1-4-3　显示数据包路由跟踪——traceroute 指令 18
1-5　网络管理程序 19
1-5-1　网络基本配置——netconfig 19
1-5-2　网络图形设置工具——网络配置的设置 20

第 2 章　Apache 服务器安装与设置 27
2-1　Apache 服务器简介 28
2-2　Apache 服务器的特色和新功能 29
2-3　Apache 服务器的安装与启动 31
2-4　HTTP 原理 34
2-5　客户端链接 35
2-6　Apache 服务器广域环境设置 37
2-7　Apache 主服务器设置 41

第 3 章　多重网站与安全通信 65
3-1　使用虚拟主机的优点与考虑 66
3-2　虚拟主机类型 67
3-3　虚拟主机内容选项 70
3-4　虚拟主机架设 71
3-5　什么是加密 75
3-6　SSL 与数字认证简介 77
3-7　使用 SSL 安全性通信协议 80
3-8　数字认证的申请与使用 81

3-8-1 建立加密的 Private Key 和 Public Key 82
3-8-2 建立认证要求 82
3-8-3 发送认证要求到 CA 84
3-8-4 安装与使用数字认证 86

第 4 章 Apache 服务器快速设置 91
4-1 “Apache 配置”——“主”选项卡 92
4-2 “Apache 配置”——“虚拟主机”选项卡 93
4-2-1 编辑默认设置 93
4-2-2 虚拟主机设置 97
4-3 “Apache 配置”——“服务器”选项卡 99
4-4 “Apache 配置”——“调整性能”选项卡 100

第 5 章 FTP 服务器——VSFTP 101
5-1 FTP 通信协议简介 102
5-2 VSFTP 服务器安装 104
5-3 客户端连接 107
5-3-1 以浏览器连接到 VSFTP 服务器 107
5-3-2 以 FTP 程序连接到 VSFTP 服务器 108
5-3-3 以 FTP 指令连接到 VSFTP 服务器 110
5-4 用户管理——/etc/vsftpd.ftpusers 113
5-5 VSFTP 服务器配置 114

第 6 章 邮件服务器——Sendmail 125
6-1 电子邮件系统简介 126
6-2 电子邮件传递流程 129
6-3 Sendmail 的安装及启动 132
6-4 客户端连接设置 136
6-4-1 以 mail 收发电子邮件 136
6-4-2 以 pine 收发电子邮件 140
6-4-3 以 Outlook Express 收发电子邮件 146
6-5 邮件中继功能 153
6-6 匿名邮件 156
6-7 邮箱管理 158
6-7-1 查看邮件队列配置 158
6-7-2 邮件结构 160
6-7-3 允许账号名大写 161
6-7-4 禁止电子邮件客户端登录服务器 162
6-7-5 以 IP 地址收发电子邮件 163

6-7-6 邮件大小限制 163
6-8 用户账号别名 164

第 7 章 与 Windows 的桥梁——SAMBA 171
7-1 SAM 与 SAMBA 172
7-2 SAMBA 的安装及启动 174
7-3 SAMBA 配置 177
7-3-1 设置/etc/services 文件内容 177
7-3-2 设置/etc/samba/lmhosts 文件 177
7-3-3 设置/etc/samba/smb.conf 文件内容 178
7-3-4 运行 testparm 以测试 smb.conf 配置文件 188
7-3-5 建立 SAMBA 密码文件——/etc/samba/smbpasswd 189
7-3-6 SAMBA 服务器安全性等级 191
7-4 SAMBA 相关程序 193
7-5 以浏览器管理 SAMBA——SWAT 196

第 8 章 高速缓存服务器——Squid 203
8-1 Proxy 服务器与缓存 204
8-2 Squid 服务器简介 204
8-3 Squid 服务器的组成结构 206
8-4 Squid 服务器的安装与启动 208
8-5 Squid 配置 210
8-6 客户端连接 215
8-7 自动抓取网页内容——wget 216

第 9 章 NAT 服务器与防火墙 221
9-1 浅谈 IP 222
9-1-1 IP 的定义 222
9-1-2 IP 寻址 222
9-1-3 IP 地址类别 224
9-1-4 子网掩码（Subnet Mask） 226
9-2 NAT 原理及主要功能 228
9-3 NAT 服务器的安装与使用 229
9-4 iptables 在防火墙上的运用 233
9-4-1 iptables 体系结构与处理流程 233
9-4-2 iptables 程序使用 235
9-4-3 保存 iptables 设置 239
9-5 范例练习 240
9-6 防火墙简单设置 242

9-7 iptables 配置文件参考范例 245

第 10 章 DHCP 服务器 247
10-1 DHCP 基本概念 248
10-2 DHCP 服务器的安装与客户端连接 253
10-3 DHCP 客户端租用 IP 流程 256
10-4 DHCP 配置——/etc/dhcpd.conf 258
10-5 客户端连接 262
10-6 DHCP/BOOTP 转送代理 264

第 11 章 DNS 服务器——BIND 267
11-1 DNS 起源 268
11-2 DNS 基本概念 269
11-3 DNS 运作方式 274
11-4 BIND 的安装及启动 277
11-5 BIND 服务器设置 281
11-5-1 设置/etc/named.conf 文件 281
11-5-2 设置/var/named/named.ca 文件 284
11-5-3 设置/var/named/localhost.zone 文件 287
11-5-4 设置/var/named/named.local 文件 289
11-5-5 设置/etc/resolv.conf 文件 290
11-6 DNS 资源记录介绍 292
11-7 规划 DNS 系统 295
11-8 范例研究 296
11-9 利用 nslookup 程序运行查询 299

第 12 章 网络磁盘驱动器——NFS 303
12-1 NFS 运行原理 304
12-2 NFS 服务器的安装及启动 305
12-3 NFS 配置 308
12-4 客户端连接 312
12-5 利用“NFS 服务器设置”管理 NFS 313

第 13 章 新闻服务器——INN 317
13-1 新闻服务基本概念 318
13-2 INN 服务器与文件保存方式 320
13-3 INN 服务器的安装及启动 321
13-4 INN 服务器配置 326
13-4-1 /etc/news/inn.conf 326

13-4-2 /etc/news/expire.ctl 330
13-4-3 /etc/news/readers.conf 331
13-4-4 /etc/news/storage.conf 333
13-5 新闻组管理 335
13-5-1 新闻组的新建与删除 335
13-5-2 以 ctlinnd 指令管理 INN 服务器 337
13-6 客户端连接设置 338
13-6-1 以 tin 阅读新闻 338
13-6-2 以 Outlook Express 阅读新闻 342

第 14 章 OpenSSH 服务器 347
14-1 OpenSSH 服务器简介 348
14-2 OpenSSH 服务器的安装及启动 348
14-3 OpenSSH 服务器配置 351
14-4 客户端连接 353

附录 357
附录 A Red Hat Linux 9 安装 358
附录 B Red Hat Linux 大量安装 385
附录 C Apache 服务器版权说明原文 397
附录 D Wu-ftp 服务器版权说明原文 398
附录 E 国家及地区代码 400
附录 F 名词解释 406

第1章

网络基本概念

- TCP/IP 网络
- OSI 七层模型
- Linux 网络配置文件
- 系统维护常用的指令
- 网络管理程序

自从网络和 Internet 盛行后，人们已彻底改变了生活方式以及对于信息的获取方式。例如，传统的邮件大多已被 E-mail 所取代，其中最大的原因不只是经济上的考虑，而在于其迅速和便捷；到图书馆寻找所需的数据，也考虑到时间及效率的因素，现在都倾向于直接上网来搜寻，不仅可以轻松地获取相关的信息，而且范围更是涵盖全球，但这些只是网络的部分优点，还有更多优点有待我们去研究。

身为系统管理员，在维护及架构网络的各项服务之前，首先必须建立网络的基本概念，以便在遇到不同服务类型的服务器时避免一些基础问题的发生，这也是作者在本书中所强调的一个理念。

1-1 TCP/IP 网络

“网络”一词包含的范围很广，只要两台以上的计算机，使用任何类型的介质（如电缆线或无线电波）、任何种类的通信协议（如 TCP/IP 或 NetBEUI）或任何形式的操作系统（如 Linux 或 Microsoft Windows）来连接，并且以资源共享为目的，都可称为网络。

通信协议（Protocol）是网络上建立通信及发送数据格式的标准，每一种通信协议都有一种以上的规则与定义来解决如何发送数据、如何识别目的地、如何处理错误情况和如何压缩数据等，有些通信协议则是利用其他通信协议来作为与其他计算机交换数据的规则，其本身则处理某一特定的任务。

因为目前多数的网络系统和 Internet 都是采用 TCP/IP（Transmission Control Protocol/Internet Protocol）通信协议标准，所以许多的软硬件在设计上也都以支持 TCP/IP 为目标。因此，系统管理员首先必须具备 TCP/IP 的知识，才可担任日常维护的工作，本书所介绍的各类服务器也都必须在 TCP/IP 网络上运行。

TCP/IP 的历史

TCP/IP 起源于 20 世纪 60 年代，当时美国国防部为了网络系统免于遭受核子武器的攻击，因此授权 ARPA（Advanced Research Projects Agency）研究高速的分组交换（Packet Switching）通信来连接美国不同区域内的超级计算机，以共享彼此的资源，并且在 1970 年开始使用 NCP（Network Control Protocol），这也是大家熟悉的 ARPANET。

1972 年 DARPA（Defense Advanced Research Projects Agency）取代了 ARPA 原有的工作，并且提出 Telnet 通信协议，它的标准规范在 RFC 318 之中，接着在 1973 年 RFC 454 制订了 FTP（File Transfer Protocol）标准。

ARPANET 发展到这时已相当成功，原本他们希望使用分层（Layering）的体系结构来提高网络的使用效率，但是实验的结果却是十分昂贵而且传输速度缓慢，最后宣布失败。到了 1974 年，Vinton Cerf 和 Robert Kahn 提出了 TCP（Transmission Control Protocol）通信协议标准，并且定义在 RFC 793 中，它描述了如何在网络上建立可靠的主机对主机的数据转送服务。

1980 年发展出了 UDP（User Datagram Protocol）的标准，它是一种在网络上广播使用的通信协议，目前定义在 RFC 768 中。

1981 年，在 RFC 791 中首次提出 IP（Internet Protocol）的概念，它描述了如何在相互连接的网络之间，规划寻址标准及路由数据包。同年，ICMP（Internet Control Message Protocol）加强了 IP 的内容，并且包含在 RFC 760 和 RFC 777 之中。

1982 年，TCP/IP 通信协议正式由 DCA（Defense Communications Agency）和 ARPA 提出。

1983 年 1 月 1 日，ARPANET 停止使用 NCP，并且要求所有网络传输以及基本通信都使用标准的 TCP 及 IP 通信协议，这也是日后 Internet 广为人知的开始。

1984 年，DNS（Domain Name System）提出，并加入到 RFC 1034 和 RFC 1035 标准中。

1991 年，ARPA 将负责开发 Internet 的工作移交给 NSF（National Science Foundation），因为 Internet 上扩展最快速的部分是在校园网（.edu），如图 1-1 所示。

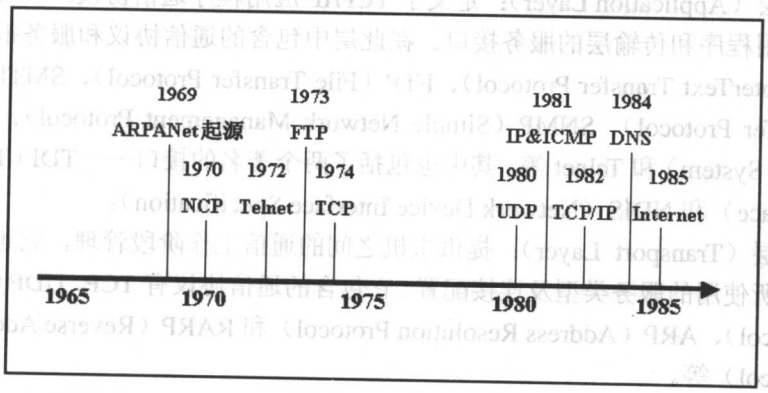

图 1-1　TCP/IP 通信协议的发展历史

注

RFC（Request For Comments）是 Internet 的前身——ARPANET 的建议评论文件，主要由网络工程师与计算机学者发布。当每一份 RFC 得到足够的支持时，它会转为 Internet 的标准、标准的一部分或者是草稿。每一份 RFC 文件都有一个编号，当一份文件被赋予编号后就不会再修改，需要改变规格时，就必须重新取得一个新编号。但并不是每一份有 RFC 编号的文件都具有意义或与网络技术有关，有些只是幽默或历史。可以到以下的网站查询 RFC 文件内容：

http://www.ietf.org/rfc.html

取代 XNS 的原因

在 TCP/IP 通信协议出现之时，XNS（Xerox Networking System）是大多数网络中使用的通信协议，而 TCP/IP 可以取代 XNS 的主要原因是：

- TCP/IP 利用一个事先定义的阶层式路径，以允许管理人员以结构化的方式维护大型网络，如 www.sina.com.cn。
- TCP/IP 地址可以进行集中式的管理，如.com、.net、.gov 和.org 等。

除了军事用途，美国国防部也将 TCP/IP 授权给一些大学使用，如 UCB（University of California at Berkeley），因此在 1983 年 UCB 开发了第一个包含 TCP/IP 的操作系统——BSD（Berkeley Software Distribution）4.2 Unix，这也是商用 Unix 的前身。

TCP/IP 四层体系结构

为了提高软、硬件和通信协议的兼容性，在 TCP/IP 中定义了层级体系结构的概念，此体系结构中共分 4 层，如图 1-2 所示。

这些层级的说明如下：

- 应用层（Application Layer）：定义了 TCP/IP 应用程序通信协议，并且提供主机之间的应用程序和传输层的服务接口。在此层中包含的通信协议和服务很多，如 HTTP（HypterText Transfer Protocol）、FTP（File Transfer Protocol）、SMTP（Simple Mail Transfer Protocol）、SNMP（Simple Network Management Protocol）、DNS（Domain Name System）和 Telnet 等，其中也包括了两个著名的接口——TDI（Transport Driver Interface）和 NDIS（Network Device Interface Specification）。
- 传输层（Transport Layer）：提供主机之间的通信工作阶段管理，它也定义了传输数据时所使用的服务类型及连接配置。它包含的通信协议有 TCP、UDP（User Datagram Protocol）、ARP（Address Resolution Protocol）和 RARP（Reverse Address Resolution Protocol）等。
- Internet 层（Internet Layer）：主要功能是将数据封装成 IP 数据报（Datagram），该数据报中记录了用来在主机及整个网络间转发数据报的来源及目的地地址信息，同时运行 IP 数据报的传递路由（Routing）。它包含的通信协议有 IP、ICMP（Internet Control Message Protocol）、IGMP（Internet Group Multicast Protocol）和 ARP 等。
- 网络接口层（Network Interface Layer）：指定如何通过网络物理地址发送数据的详细内容，这包含与网络媒体直接连接的硬件设备，如同轴电缆线（Coaxial Cable）、光纤（Optical Fiber）或双绞铜线（Twisted-Pair Copper Wire）等，以及如何将位解析为电子信号。该层包含以太网络（Ethernet）、权标环网络（Token Ring）、FDDI（Fiber Distributed Data Interface）、X.25、帧中继（Frame Relay）和 RS-232 等标准。

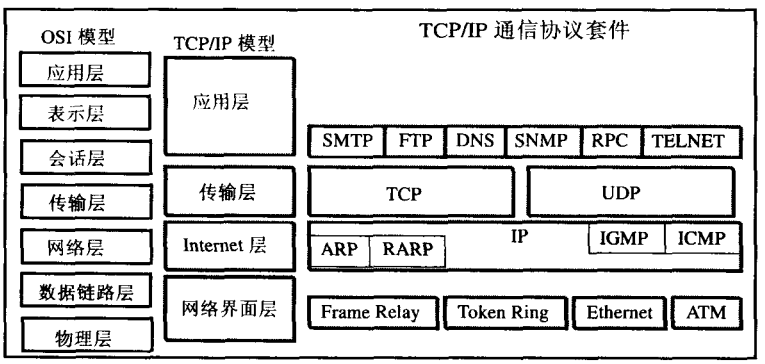

图 1-2　TCP/IP 体系结构模式

1-2 OSI 七层模型

开放系统互联模型（Open Systems Interconnection model，OSI）是国际标准组织（International Standards Organization，ISO）在 1984 年所开发的全球通用标准，它的目标是创建一个开放性的网络系统环境，来让所有的系统能相互操作，目前大部分的通信协议也都是基于 OSI 的模型来设计的。

OSI 模型由 7 个层组成，所以又称为 OSI 七层模型，因为每一层都具有特定的网络功能，因此只要软、硬件都遵循 OSI 模型的标准来设计，就可以确定所有网络组件都会具有兼容的特性。这不仅是大型网络中必备的法则，更可以节省厂商开发的时间，因为每种产品都符合特定层的标准，开发者不需考虑兼容性的问题，而将其他层的标准包含在产品中，同时这也可以简化错误故障的排除过程。OSI 七层模型如图 1-4 所示。

以下将对 OSI 模型中的每一层说明其名称及功能，帮助读者了解其中的内容，这也是网络管理员很重要的一门功课。

第 1 层：物理层（Physical Layer）

物理层定义了电缆线连接到网卡的方式，如每个连接器引角（Pin）的多少和每个 Pin 的功能。它会将数据链路层送来的数据包（Packet）转换为电子信号，也就是由 0 和 1 所组成的数据位，并通过网络介质来发送及接收，如 RS-232 和 RS-422，但它本身没有错误检测的能力。属于这一层的设备有多路复用器（Multiplexer）和中继器（Repeater）等。

第 2 层：数据链路层（Data Link Layer）

数据链路层的主要功能是将由网络层传来的数据包传递到物理层，因为物理层只会进行单纯的信号传递，并没有任何数据框架（Frame）的概念，所以数据到了数据链路层后，必须将这些位数据形成框架，并配合流量和错误的控制，如 CRC（Cyclic Redundancy Check），来确保传输时的正确性。

在数据链路层送出数据包后，它会等待来自接收端的“确认”（Acknowledgement，ACK），用来确定接收端已正确收到此数据包的信息。如果数据链路层没有收到来自接收端的 ACK，则表示在数据包发送的过程中出现了错误，因此数据链路层会再次传递此数据包，网桥（Bridge）就是使用在这个层的设备，如图 1-3 所示。

> 注
>
> IEEE 802 的标准将数据链路层分为两个子层——逻辑链路控制层（Logical Link Control，LLC）和媒体访问控制层（Media Access Control，MAC）。

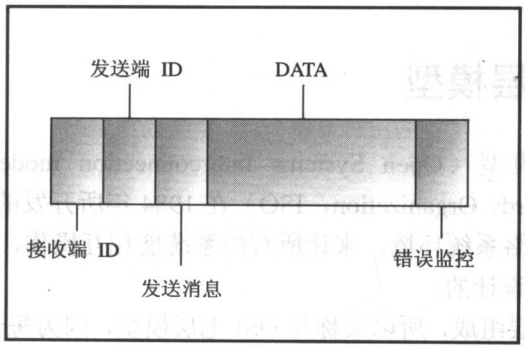

图 1-3　简单的数据包内容

第 3 层：网络层（Network Layer）

网络层负责的工作有很多，包括寻址（Addressing）、将逻辑地址（如 IP 地址）解析为物理地址（MAC 地址）、决定信息发送的路径（Route）、决定数据包发送的顺序和部分的传输控制功能，如堵塞控制，这些工作都是为了使信息的传递达到最佳化。

如果路由器中的网卡无法发送过大的数据，那么网络层会将数据分为较小的单位，而在接收端的网络层则必须重组这些数据包以得到原始的数据。作用在此层的通信协议包括 IP、IPX（Internet Package eXchange）、NWLink 和 NetBEUI（NetBIOS Extended User Interface）。另外，路由器（Router）也是符合网络层标准的设备。

第 4 层：传输层（Transport Layer）

传输层的主要功能包含分段处理（Segmentation）、数据包重新编号、流量控制和多任务处理。分段处理指将发送到传输层的数据分割成适合网络层的数据包大小，也就将一份信息分成多个数据包。重新编号是指将属于同一份信息的各个数据包重新加上序号，以便接收端能依此次序来重组原来的信息。流量控制则是协调数据发送和接收的速度，以避免发送速度太快而导致接收端来不及接收的问题。而多任务处理是指传输层连接的多任务情形，当网络层连接的速度够快，并且提供多个传输层连接使用时，可以使用多任务处理来将这些传输层连接导入一个网络层连接。作用于该层的通信协议有 NetBEUI、TCP、SPX（Sequenced Packet eXchange）和 NWLink 等。

第 5 层：会话层（Session Layer）

会话层可以允许不同计算机上的应用程序互相建立连接、使用和中止连接，这个过程就称为会话（Session），会话的主要功能是建立连接、交换数据、释放连接、对话管理和错误回复等。

会话层也支持同步（Synchronization）的工作，它是利用在数据中配置检查点（Checkpoint）来确保数据传递的正确性。如果网络出现问题，则只需重新发送最后一个检查点后的数据，

这在网络配置不稳定的情形下非常重要，因为发送端可以节省重新发送所有数据的时间。其他的功能包括用户身份验证（Authentication）、安全性和 NetBIOS 网络名称的使用等。

第 6 层：表示层（Presentation Layer）

表示层主要是担任翻译的角色，因为不同的应用程序常使用不同的语法，为了要让两端的应用程序顺利交换数据，双方必须先就传输过程中所使用的语法取得共识。所以发送端在送出数据之前其表示层必须将数据从发送端的格式（Format）转换成传输过程的格式，在到达接收端后，再由接收端的表示层转换成接收端的格式。

为了确保网络传输的安全，表示层可将发送的数据先经过加密（Encryption）处理再发送到网络上，而在到达接收端以后，再经过解密（Decryption）处理来还原原始数据。它也具有数据压缩（Compression）的能力，主要是为了减少传输的数据量，而在压缩时须以不失真为原则。因此压缩后的文字数据经过解压缩（Decompression）后必须完全地还原（Lossless），而压缩后的影像或语音数据经过解压缩后，其影像或语音的品质也要符合一定的标准。

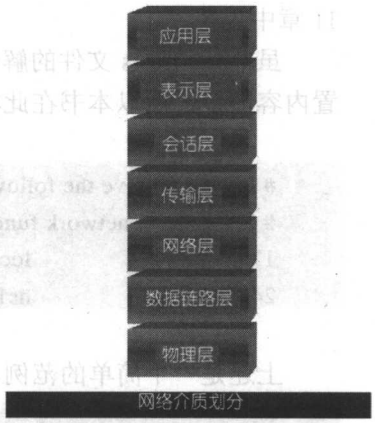

图 1-4　OSI 七层模型

第 7 层：应用层（Application Layer）

位于 OSI 七层模型的最上层是应用层，该层的功能是直接支持用户应用程序，如 FTP、E-mail 和 RPC 等。不同计算机中的应用层可以用来辨认对方计算机发送的原始数据，另外也处理一般的网络储存、流量控制和错误回复等工作。

1-3 Linux 网络配置文件

在 Linux 中，网络功能的运作必须凭借许多配置文件的内容，虽然有许多工具或程序可以用来进行这些文件的设置，但是管理员是绝对必须了解这些文件内容的。因为无法保证所有的指令或程序随时可用，如果指令或程序产生问题，就必须回到设置中手动进行修改或维护工作。因此本节选择了一些与网络管理有关而且比较重要的文件来加以说明，希望读者能确立正确的概念，以便管理工作的顺利完成。

主机地址配置文件——/etc/hosts

Linux 系统默认的通信协议为 TCP/IP，而 TCP/IP 网络上的每台主机都是以一个惟一号码来代表它的地址，这个号码就称为 IP 地址。不论主机位于局域网还是 Internet 中，只要是使用 TCP/IP 通信协议，则主机间就必须靠 IP 地址来互相辨认。目前的 IP 地址是采取 IPv4（IP 第 4 版）的标准，因此每个 IP 地址都是以 xxx.xxx.xxx.xxx 的形式组成，其中 xxx 的有效范围

为 0 ~ 255，如 24.68.10.200。因为这个地址是由 InterNIC 所指定，所以可以保证每一台主机 IP 都是惟一的，不会产生重复的问题

虽然以 IP 地址可以很准确地辨认每一台主机，但是也产生了一个问题——记忆地址的困难，因为一些数字的组合对用户来说，实在很难与特定的主机产生联系。如果采用一些便于记忆的名称，如 ns1.jschouse.com（主机名）或 ns1（别名），则可以降低用户忘记主机地址的可能性。所以在 TCP/IP 网络上就出现了一个解决方法：利用一个中介的机制来进行 IP 地址和易记名称的转换（域名解析）。

通常在 TCP/IP 网络上进行 IP 地址和易记名称的转换有两种方法：使用 DNS 服务器或 /etc/hosts 文件。DNS 服务器域名解析功能比较强大，但是由于涉及的内容很广，本书将在第 11 章中说明。

虽然/etc/hosts 文件的解析功能不如 DNS，但因为它也可以提供域名解析的功能，而且设置内容简单，所以本书在此将对它的内容加以说明。以下是一个/etc/hosts 文件的范例：

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain   localhost
24.68.32.118            ns1.jschouse.com        ns1
```

上述是一个简单的范例，其中的记录可由系统自动产生或自己加入。格式如下：

```
IP 地址        主机名        别名
```

在将 IP 地址、主机名或别名等信息输入/etc/hosts 文件后，就可以使用主机名或别名来取代原有的 IP 地址。举例来说，假设有一台 Web 服务器的 IP 地址为 24.68.32.118，而它的主机名称为 ns1.jschouse.com，别名为 ns1，则在浏览器上输入以下的任何地址都可连接到这台 Web 服务器：

- http://24.68.32.118（可在局域网和 Internet 中使用）
- http://ns1.jschouse.com（可在局域网和 Internet 中使用）
- http://ns1（仅限于局域网中使用）

网络服务数据文件——/etc/services

/etc/services 是记录各种不同网络服务的数据文件，在此文件中的每一条记录都表示一种 Internet 服务，它的格式如下：

```
服务名称    连接端口号码/通信协议名称  [别名]    [注释]
```

它允许使用“连接端口号码/通信协议名称”来对应特定的服务名称，而有些程序必须使用这个文件以运行特定的功能。例如，xinetd 是一个功能强大的程序，它专门管理 Internet 上连接的请求，而当用户请求远程登录以及文件传输协议时，它会自动检查/etc/services 文件，并且找出对应的程序，以满足用户的请求。