

Js49/10

操作系统系列丛书

Linux网络应用技术

国防科学技术大学

张银福 陈曙晖 赵振宇 等编著



机械工业出版社
China Machine Press

本书全面系统地讲解了Linux网络应用技术的各种问题。全书以实用性为指导原则，在讲述网络基本知识的基础上，重点对各种应用技术，尤其是近几年来发展起来的新技术进行了剖析，可满足网络业界人士的各种需求。

作者首先从Linux网络技术的发展入手，介绍了网络技术基础，包括如何建立WWW服务器、FTP服务器、邮件服务器和域名服务器，还介绍了在不同网络间如何实现资源共享、提高网络的安全性、管理网络、在Linux与Windows之间进行互操作以及网络编程等内容。

本书内容新颖详实、条理清晰、深入浅出，是计算机网络入门和提高者难得的参考书。本书适用于企事业单位的计算机使用人员、大专院校相关专业的广大师生以及网络的开发设计人员。

本书中文简体字版由机械工业出版社出版。未经出版者书面许可，不得以任何方式复制或抄袭本书的任何部分。

版权所有，翻印必究。

图书在版编目(CIP)数据

Linux 网络应用技术 / 张银福等编著. -北京: 机械工业出版社, 1999.5

(操作系统系列丛书)

ISBN 7-111-07211-1

I. L… II. 张… III. 操作系统, Linux IV. TP316

中国版本图书馆CIP数据核字(1999)第10881号

出版人: 马九荣 (北京市百万庄大街22号 邮政编码 100037)

责任编辑: 吴 怡

北京市南方印刷厂印刷 · 新华书店北京发行所发行

1999年5月第1版第1次印刷

787mm × 1092mm 1/16 · 18.5印张

印数: 0 001-8000册

定价: 30.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

前 言

一年前，我们课题组要进行一个网络方面的实验，采用的操作系统为Linux。虽然Linux是一个开放性非常好的操作系统，但却找不到相关的中文参考书籍。我们花费了很多时间阅读各种英文资料，以便进行网络安装和管理。这使我们下定决心要写一本Linux网络方面的书。通过半年时间的资料收集和半年时间的编写，这本书终于与读者见面了。

如今的Linux再也不是一年以前的Linux了，1999年来临之际，Dell、Compaq、SGI和HP等公司相继宣布在其高端服务器上开始支持Linux，这意味着Linux已经完全进入高端服务器市场，成为网络世界又一强劲的操作系统。

为了使本书能够在读者使用Linux网络时给予较大的帮助，全书在讲述网络基本知识的基础上，重点对各种应用技术，尤其是近几年来发展起来的新技术进行了剖析。我们从Linux网络技术的发展入手，分别介绍了网络技术基础；如何建立WWW服务器、FTP服务器、邮件服务器和域名服务器；在不同网络间如何实现资源共享；如何提高网络的安全性；如何管理网络、如何在Linux与Windows之间进行互操作以及网络编程等内容。

Linux近两年来已经开始在国内流行，但相关书籍，尤其是专门介绍Linux网络技术的书却不多。希望本书能满足广大Linux使用者、企事业单位的计算机使用人员、大专院校相关专业的广大师生以及网络的开发设计人员的需求。

本书由张银福、陈曙晖、赵振宇进行了主要的编著工作，此外，陈彦海、孔桂兰、卿华、李志、张巧莉、李林、赵军锁、龚波、邓波、叶玉、张涛、王良启、李节节、郑少雄、郑波、肖云、胡平等同志参加了本书部分章节的编写以及审校工作。由于作者水平和时间有限，书中难免有不妥之处，请读者批评指正。

作 者

1999年2月

目 录

前言

第1章 Linux 网络概述	1
1.1 了解Linux	1
1.2 网络常用术语	4
1.3 网络协议	6
1.4 Internet / Intranet 解决方案	8
1.5 文件与打印共享	9
1.6 Linux 网络的安全问题	10
1.7 Linux 网络管理工作	10
1.8 网络技术的演变	11
1.9 小结	11
第2章 理解TCP/IP	12
2.1 TCP/IP 的历史	12
2.2 TCP/IP 通信基础	12
2.2.1 TCP/IP 协议体系结构	12
2.2.2 TCP/IP 数据封装	15
2.2.3 网络访问层	16
2.2.4 IP 层	16
2.2.5 主机到主机传输层	29
2.2.6 名字服务	30
2.3 TCP/IP 配置文件	33
第3章 建立Internet站点	38
3.1 准备工作	38
3.2 选择接入方式	39
3.3 安装E-mail软件	41
3.3.1 Linux 邮件软件	41
3.3.2 电子邮件结构	43
3.3.3 配置sendmail	44
3.3.4 配置邮件程序	50
3.3.5 运行邮件列表	54
3.4 安装WWW服务	60
3.4.1 安装Web服务器软件	60
3.4.2 建立Web站点	65
3.5 安装FTP服务器软件	67

3.5.1 编译FTP服务器	67
3.5.2 安装和启动FTP服务器	69
3.5.3 检查FTP服务器的工作状况	71
第4章 网络应用程序与网络文件系统	74
4.1 网络应用程序	74
4.1.1 inetd超级服务器	74
4.1.2 tcpd访问控制机制	75
4.1.3 services和protocols文件	76
4.1.4 远程过程调用	77
4.1.5 配置远程命令	78
4.2 网络文件系统	79
4.2.1 准备网络文件系统	80
4.2.2 安装NFS卷	81
4.2.3 NFS守护进程	82
4.2.4 exports文件	83
4.3 NIS	84
4.3.1 什么是NIS	84
4.3.2 安装NIS	85
4.4 小结	86
第5章 Windows与Linux的互操作性	87
5.1 互操作方法简介	87
5.1.1 FTP	87
5.1.2 telnet	88
5.1.3 web方式	88
5.1.4 在Linux上运行Windows	89
5.1.5 命令仿真	89
5.1.6 文件与打印共享	90
5.2 Linux提供NT文件服务	91
5.2.1 SMB	91
5.2.2 Samba	91
5.2.3 编译和安装Samba	92
5.2.4 创建Samba	93
5.2.5 配置Samba	93
5.2.6 特殊段	94

5.2.7 共享文件系统	95	7.1.1 网络管理的需求	162
5.2.8 Samba用户的认证	96	7.1.2 网络管理的功能	163
5.2.9 Samba打印	96	7.1.3 网络管理的标准化	164
5.2.10 在 Windows打印机上打印	97	7.2 网络管理系统	165
5.2.11 运行Samba	98	7.2.1 网络管理系统的基本构成	165
5.2.12 使用smbclient	99	7.2.2 网络管理模型	168
5.3 NT提供Linux文件服务	100	7.2.3 网络管理平台及产品	168
5.3.1 文件许可	100	7.2.4 远程网络监控	174
5.3.2 文件映射	101	7.2.5 新型网络管理模式	177
5.3.3 NFS文件命名问题	102	7.3 规划网络管理系统	181
5.3.4 NFS软件	102	7.4 Linux网络管理	183
5.4 小结	103	7.4.1 Linux系统网络管理命令和工具	183
第6章 网络安全	104	7.4.2 Linux相关网络管理工具	196
6.1 概述	104	7.4.3 安装SNMP软件	202
6.2 主要安全问题	105	第8章 远程通信	207
6.2.1 物理安全	106	8.1 SLIP	207
6.2.2 帐号安全	108	8.1.1 SLIP配置	207
6.2.3 网络应用安全	112	8.1.2 把Linux 配置成一个SLIP服务器	211
6.2.4 文件系统安全	118	8.2 PPP	215
6.3 监视系统安全	124	8.2.1 PPP简介	215
6.3.1 帐号安全	124	8.2.2 Linux 系统配置PPP	218
6.3.2 网络应用安全	126	8.2.3 建立连接	235
6.3.3 文件系统安全	127	8.2.4 运行连接	243
6.3.4 了解系统	131	8.2.5 连接之后的工作	248
6.4 系统安全评估和监测工具	131	8.2.6 建立PPP服务器	251
6.4.1 Sniffer	132	第9章 网络编程	254
6.4.2 系统安全扫描程序	133	9.1 Linux 编程概述	254
6.4.3 日志工具	136	9.1.1 C语言及其调试	254
6.4.4 口令破解工具	138	9.1.2 其它编程工具	255
6.5 防火墙	141	9.2 网络编程	256
6.5.1 防火墙概述	141	9.2.1 端口和套接口	256
6.5.2 防火墙构件	144	9.2.2 连接方式socket编程	257
6.5.3 设计防火墙系统	148	9.2.3 无连接方式socket编程	263
6.5.4 防火墙实例	150	9.3 记录和文件加锁	266
6.5.5 安装防火墙	152	9.4 进程间通信	267
6.6 如何应付入侵者攻击	159	9.5 小结	267
第7章 网络管理	162	附录 Linux 常用命令	268
7.1 概述	162		

第1章 Linux 网络概述

近年来“信息高速公路”技术取得了很大进展，许多被认为是未来的网络技术今天已经成为现实。在信息传输的过程中，通信通路虽然十分重要，但我们也不能忽视端系统的性能和功能，端系统的性能和功能很大程度上是由端系统所采用的操作系统所决定的。Linux操作系统与其它操作系统显著不同的一点就在于Linux中的网络是操作系统本身所固有的，Linux系统从其初期的发布版本开始就包含了相对完整的网络功能。而许多其它操作系统中的网络则是附加在操作系统之上的，也就是说Linux系统中网络与操作系统的结合关系更为紧密。

用户可以通过网络获得大量的计算机和信息资源，也可以与同事共享数据、发送邮件，甚至与分布在世界各地的朋友共同玩电子游戏等等。本章将介绍Linux网络技术的发展过程及基本技术。

1.1 了解Linux

1. UNIX的发展

20世纪60年代中期，AT&T贝尔实验室组织开发了一个名为Multics的操作系统。Multics的主要设计目标是支持大规模的计算工具，后来参加Multics开发的贝尔实验室的许多人员都参加了UNIX的开发工作。

1969年，由于贝尔实验室从Multics的计划中撤出，科学计算研究中心（Computing Science Research Center）的成员没有了计算环境，Ken Thompson、Dennis Ritchie和其他一些研究人员开发了一个基本的文件系统，该系统后来演化成了UNIX文件系统。系统最初的版本是在PDP-7机器上开发的。

AT&T专利部门将UNIX用于文本处理使UNIX获得了成功，UNIX也因短小精巧而闻名天下。后来为UNIX开发出C语言后，UNIX便使用C语言来实现。这一实现也是UNIX转变成开放式系统的重要原因。

由于UNIX无法进入计算机市场，AT&T无法将UNIX作为商品出售，因此只能自己使用和发放到大学的科研机构中供研究使用。直到1977年UNIX才得到商业使用的许可，第一家UNIX销售商——交互式系统公司（Interactive System Corporation），开始为办公自动化业务销售UNIX系统。

AT&T（后来的UNIX系统实验室，现在为Novell公司所有）开发了UNIX的后续版本，如系统Ⅲ以及系统V的一些版本。系统V的两个最新版本——系统V版本3（SVR3.2）和系统V版本4（SVR4，SVR4的最新版本为SVR4.2）在计算机操作系统中一直很流行。

如果使用由AT&T发展而来的所有UNIX版本，都要首先从UNIX系统实验室得到许可权。

1978年UNIX研究小组将UNIX的发布工作交给了UNIX支持组（USG，UNIX Support Group），该组织在1978年就发布了一个叫程序员工作台（Programmer's Workbench）的UNIX内部版本。1982年，在集中了几个内部版本对UNIX改动的基础上，USG发布了系统Ⅲ，

1983年USG又发布了系统V, 随着AT&T的*解体, 系统V又走上了市场。在许多UNIX不同版本发展的基础上(包括USG的内部版本和BSD), UNIX又出现了许多后续版本。

在AT&T(通过UNIX研究小组和USG)发展UNIX的同时, 许多大学也在研究UNIX。Berkeley的California大学计算机科学研究组(Computer Science Research Group)开发了UNIX的BSD版本, 该组织首先在PDP-11上开发了1BSD和2BSD, 然后又在DEC的VAX计算机上开发了3BSD, 后来发展为4.0BSD、4.1BSD、4.2BSD和4.3BSD, 其中(尤其是4.2BSD和4.3BSD)的许多特色(包括一些源代码)被应用到商业产品中。

2. UNIX的特点

UNIX是一个功能强大的多任务、多用户的操作系统。与其它操作系统不同的是UNIX具有许多变体, 这些变体具有不同的功能, 有一些是针对某类机器由计算机销售商开发的, 还有一些被专门开发成共享的或免费的软件。尽管各种UNIX变体之间有差别, 但它们都有基本相同的运行环境。这些环境都支持awk、grep、Bourne Shell和make等命令, 不同的是各变体在此环境上向开发人员提供的通用工具、应用程序和编程语言不同。

UNIX的显著特点是它的可扩展性和开放性。可扩展性是指可以方便地定义一些供其它程序调用或终端用户使用的命令。由于UNIX内核只定义了程序间通信的基本接口和方法, 因此可扩展性在UNIX环境中是很有意义的。UNIX不仅仅是一个严格的操作系统, 除了包括传统操作系统模块以外, 一个标准的UNIX还包括一组库和应用。在硬件之上是文件系统和进程控制模块, 接着是一组库, 在最顶端是应用。用户可以访问到库和应用, 这两部分组成了UNIX的用户界面, 它们就是用户眼中的UNIX。

电器电子工程师协会(IEEE, Institute of Electrical and Electronic Engineers)为制定“基于UNIX操作系统的工业使用的操作系统接口标准”产生了一系列的标准委员会。其中两个委员会的工作对用户和开发者来说比较重要: POSIX.1委员会为编写UNIX程序定义了标准的C库接口, POSIX.2委员会定义了用户使用的UNIX命令的标准。

UNIX的各种版本, 如Solaris、HP/UX、SCO, 都非常昂贵。而Linux属于UNIX的一种, 是由全世界一些志愿者书写的操作系统。

3. Linux的发展

Linux是基于Intel PC的操作系统, 它是由分布在全世界的数以百计的程序员设计和实现的。目的是创建一个脱离需付版权费用才可购买的UNIX产品, 使得全世界的人都能免费使用。

1991年, 芬兰赫尔辛基大学的Linus Torvalds开始开发Linux, 该系统在当时已经能够运行bash和gcc。Linus Torvalds后来在一个新闻组上对其进行的工作进行了阐述。于是, 其开发工作立即得到了遍布于Internet上的UNIX程序员和爱好者的帮助。许多志愿者参加了这项工作, 这些人或多或少地参加了核心程序的开发。经过几年之后, Linux成为了正式发行的操作系统。

4. Linux免费的原因

Linux系统在很大程度上得益于支持GNU项目的自由软件基金会(Free Software Foundation)。这些人为Linux系统准备了一整套软件, 而且大部分都比商业版本开发人员开发得更好、更强壮、更快, 并且它们是免费的。如果Linux没有GNU工具的话, 它就仅仅是一个内核、一些磁盘访问代码和很少的几个软件, 甚至标准文件工具(如ls, mv, cp和rm等)都是GNU实用工具包的一部分。

在Linux用户群中, 经常会见到许多“免费”的软件。免费(free)并不意味着它不花钱,

尽管通常情况下是这样的，免费意味着可自由得到或可自由再发行，也就是说没有什么条款能限制用户得到它，或者说如果想得到源代码，就能毫不费力地得到。用户可以修改它，或借用其部分代码，改进这些代码等等。用户可以在免费软件上做任何想做的工作。

如果想知道更多的有关自由软件基金会的信息，可以访问它们的FTP站点：
<ftp://prep.ai.mit.edu>。

尽管Linux从GNU中得到了许多益处，但GNU和Linux是不同的实体，许多实用工具都是GNU的，Linux的大部分代码都是在GNU的公共许可证下发行的，而且如果Linux没有依靠数百个GNU/NSF的程序员，就会有很大的不同。然而Linux还是Linux，不是GNU。

5. Linux的特点

现在国外使用Linux的用户正在逐年增加，只要花上几十美元，就能从Red Hat公司购买到一套Linux。某些人总是认为免费的东西能好到哪里去呢？事实上，Linux与其它UNIX相比具有价格低的优势（其实卖Linux的公司仅仅收取一些光盘的工本费），而与Microsoft公司的操作系统相比，Linux相对稳定，而且对机器的配置要求比较低。国外许多老牌公司的IT部门都开始将Linux用于文件服务器、Web服务器和打印服务器等，其主要原因是Linux的低成本、高可靠性和很好的可缩性。Linux现在的主要问题是客户支持十分有限，Red Hat公司可以为购买RedHat Linux的客户提供30天的免费电话支持，此后，用户可以借助Internet和Linux上的随机手册来解决问题。

Linux最大的特点，不是先进的功能，而是全新的软件开发模式。Linux成功之前，人人都认为操作系统是很复杂的软件，非要靠一个开发团队密切合作、互相协调与分工才有可能写出来。事实上，到1993年底，Linux就已经发展成熟，能与商业UNIX一较高下，渐渐有商业应用软件移植到Linux上来，许多小的UNIX商家因此失去了很多市场。

6. Linux的发行版本问题

虽然从许多Internet匿名站点上，可以免费得到Linux大部分发行版本的完整拷贝。我们还是建议到当地零售商处购买一个CD-ROM的拷贝，以节省在Internet上传输大量数据的时间和烦恼。

目前主要有以下四种Linux发行版本：

Caldera是一个高质量的商业版本，它包括许多增值特性。它是在早期的Redhat版本中建造起来的，但与当时相比，已经变化了许多，它的开放性和可扩展性没有Redhat发行版本高，但它却带有一些商业软件，读者可以访问<http://www.caldera.com>来获取更多的信息。

Debian“家族”的开发人员一直在积极工作，而且已组织了一个好而稳定，并且功能齐全的发行版本，以在功能、多样化和普及等方面与Redhat一比高下。在懂技术的用户中，它很受欢迎，而且也不会出问题。但对于不懂技术的用户来说，会有一点不方便，这是因为它在安装配置方面相对要复杂。访问<http://www.debian.org>可以找到有关Debian的更多信息。

Slackware是最好的发行版本之一，我国的用户普遍使用Slackware。但由于Debian和Redhat功能强大而使得Slackware的国外用户相对少一些。可以从Walnut Creek CD-ROM包所在的站点<http://www.cdrom.com>处得到有关Slackware的更多信息。

Redhat提供了一个稳定的包系统rpm，这样就可以用一个简单的命令来安装、升级或移去软件的整个包。每个版本都经过了完整的测试，而且包含了大量软件的最好和最新版本。而且，许多志愿者把他们喜欢的，而发行版中又不包含的软件打包起来，使得rpm可以使用它们。

另外, Redhat还出售一些打过包的流行商业软件, 并且也安装到系统之中, 可以访问<http://www.redhat.com>来获取该发行版本的更多信息。Redhat在国外使用得最多。

1.2 网络常用术语

在介绍完Linux之后, 下面介绍Linux网络技术, 首先介绍一些经常要使用的术语, 这样对后面的阐述将有所帮助。

1. 服务器

服务器 (Server) 是为用户提供文件、资源和服务的机器。事实上, 在客户机/服务器系统中, 一个机器 (客户机) 从另外一个机器 (服务器) 处请求某种服务。通常, 一台机器既可以是客户机, 也可以是服务器。

对服务器最初的定义是在局域网上, 服务器就是一台放置大量文件和应用程序的高性能机器, 而其它的机器通过网络访问服务器上的文件。在这种类型的网络中, 一般只有一台机器作为服务器, 而其它的机器都是客户机。

大的基于服务器的网络有专用目的的服务器。例如, 有的服务器可能用来放置文件 (称为文件服务器); 有的服务器则用来处理打印需求 (称为打印服务器); 有的服务器可能用来处理连接外部 (广域网) 的服务 (称为通信服务器); 而在广域网或者局域网中, 都可能采用HTTP提供WWW服务的服务器 (称为WWW服务器) 等等。有些特殊的应用可能还需要特殊的服务器, 如有些大的软件, 为了保证软件不被盗版使用, 可能设置Licence服务器, 每个使用其应用程序的机器, 在使用前都必须通过Licence服务器进行验证, 以保证软件不被盗版使用。

重要的是, 服务器是与所使用的网络和所请求的服务密切相关的。简单地说, 服务器就是对某些请求提供服务的机器。

2. 客户机

从服务器的定义中可以看出, 客户机 (Client) 是请求服务器进行服务的机器。通常意义上的客户机是指服务器为之提供文件和处理能力的机器, 每一个这样的机器都称为客户机。典型情况下, 在有10个PC机的局域网中, 可能有一个大的服务器, 提供对大量文件和数据库的服务, 而其它连接其上的机器称为客户机。

人们经常提到客户机/服务器模式, 客户机就是向服务器发请求的机器。在TCP/IP的网络中, 经常使用客户机/服务器模式。

3. 节点

小的网络中通常会包含一台服务器和一定数量的PC机或者Macintosh机器。每一个位于网络上的机器都称为一个节点 (Node)。节点是指连接到网络上的设备, 这些设备在网络上有独一无二的名字 (地址)。读者可能听到术语“节点名称”和“节点号”。在大的网络中, 可能包含上千个节点, 这些节点可能是计算机、打印机或者网络设备 (如后面要介绍的路由器) 等。

4. 本地和远程资源

本地资源 (Local Resource) 是指直接连接到自己机器上的设备, 如打印机、调制解调器、扫描仪以及硬盘等。机器访问本地设备无须通过网络, 这样的设备称为本地设备或者本地资源。

同样, 如果要访问一个设备, 必须通过网络, 这样的设备就称为远程资源 (Remote Resource)。例如, 对一般用户而言, 那些连接到服务器上的设备就是远程资源。直接连接在

网络上的网络打印机也可称为远程资源。

5. 网络操作系统

网络操作系统 (Network Operating System) 缩写为NOS, 是控制网络上的所有机器进行交互的系统。NOS负责控制网络媒体中信息的发送和接收方式。它处理诸如下面的事务: 来自一台机器的报文如何到达另一台机器, 如果多个机器同时发送报文如何处理等。NOS还要负责对共享外设 (如网络上的打印机、扫描仪等) 进行控制, 因为这些外设要被网上的用户共同使用, 不可避免地存在资源的分配问题。

在只有一个服务器和几个客户机的小型局域网中, NOS位于服务器上, 如Novell的Netware网络就是采用这样的处理方式, 其NOS的主要部分驻留在服务器上, 而每个客户机中只有很小的客户软件。

对于拥有超过一台服务器的大网络, 例如运行TCP/IP的Linux, NOS是每个机器中软件的一部分。Linux有一些用于建造TCP/IP网络的代码, 集成在操作系统的内核中。任何想连上TCP/IP网络的PC机都要安装TCP/IP协议。

有些网络, 如Microsoft Windows 95, Artisoft的LANtastic等, 并没有单个的主服务器 (当然, 它们也可以使用单个服务器的方式)。这样的网络中, 每台机器都拥有NOS中用来与其它机器进行通信的功能。

6. 网络协议

共享计算机的资源, 以及在網上交换信息, 都需要不同系统的实体之间进行通信。两个实体 (实体间对等的应用程序等) 要成功地通信, 就必须具有同样的语言。交流什么、怎样交流及何时交流, 都必须遵从有关实体间某种相互能接受的规则。这些规则的集合称为协议 (Protocol), 它可以定义为两实体间控制数据交换的规则集合。协议的关键部分包括: 语法 (数据格式、编码及信号电平等)、语义 (包括用于协调和进行差错处理的控制信息)、定时 (包括速度匹配和排序)。

由于不同系统中实体间通信的任务十分复杂, 相互不可能作为一个整体来处理, 否则任何小部分的改变, 就要修改整个软件包。一种替代的方法是使用结构式的设计和实现技术, 用分层或层次结构的协议集合。有关协议理论的详细叙述, 请读者参见有关的书籍。

在UNIX系统中, TCP/IP (Transmission Control Protocol/Internet Protocol) 是最为通用的网络协议。事实上, TCP/IP是一个协议的集合 (称为协议族), 第2章有详细的叙述。而Novell Netware则使用IPX协议 (InterPacket Exchange)。

7. 网络接口卡

网络接口卡 (Network Interface Card, NIC), 简称网卡, 是插在PC机的I/O槽上的一种适配器。有些NIC可能插在并口或者SCSI口上, 这样的NIC适合于笔记本等移动式PC机。

网卡一般处理的是协议族的底层协议, 底层协议是与网络介质直接相关的, 如FDDI网络有FDDI (Fibre Distributed Data Interface, 光纤分布式数据接口) 的网卡, 以太网有以太网的网卡, ATM (Asynchronous Transfer Mode, 异步传输模式) 有ATM的网卡等。

8. 桥、路由器

读者可能经常听说桥 (Bridge, 或者称为网桥) 和路由器 (Router)。网桥和路由器二者都是用于互连局域网 (LAN) 的专门设备, 它们是把不同的LAN或LAN分段连接在一起的设备。许多机构都有一些建在地理位置相隔较远的场点上的LAN, 路由器最初的设计是使用户

能够通过广域网把这些远程LAN连接起来,网桥也可用于这一目的。把路由器或者网桥放在两个不同地点的LAN上,再通过广域网或远程通信把它们连起来,一个LAN上的用户就可以访问另一个LAN上的资源,就好像这些资源是在本地一样。

网桥比较简单,它能在网络传递过程中接收到的每一个数据包作出简单的转发/不转发决定,在LAN之间过滤数据包。过滤是根据数据包的目的地址来执行的,如果包的目的地址是发送点所在网段上的一个站,就不进行转发;如果其目的地是另一个LAN上的一个站,它就被连接到不同的网桥端口,并转发到该端口。当前许多网桥过滤和转发数据包只有很小的延迟,故适用于大的流量。

路由器是更为复杂的网络互连设备,通常要比网桥昂贵。它利用每个数据包中的“网络层协议信息”,把数据从一个LAN传送到另一个LAN。这意味着路由器必须能够识别与之连接的各个网络上可能使用的各种不同的网络层协议。这就是术语“多协议路由器”的由来——一种可以使用许多不同协议进行路由的设备。路由器之间互相通信并共享信息,使它们能决定通过连接许多LAN的复杂互连网络的最佳路由。

进行网络连接的设备有很多,而且不同的网络有不同的连接设备,这方面的知识请读者参见计算机连网方面的书籍。

9. Intranet

Intranet是指在组织和企业内部采用Internet相似技术实现的网络,其主要目的是以Internet的方式在组织和企业内部发布信息。Linux支持的Internet/Intranet服务包括电子邮件、新闻、WWW服务等。

1.3 网络协议

对某些用户而言,UNIX或者Linux的网络似乎就是TCP/IP,由此可见TCP/IP对于UNIX用户的重要性。TCP/IP从20世纪70年代发展到现在已经经过了20多年,它日趋成熟,已经成为了网络界事实上的标准。图1-1是使用TCP/IP的机器的协议结构图。

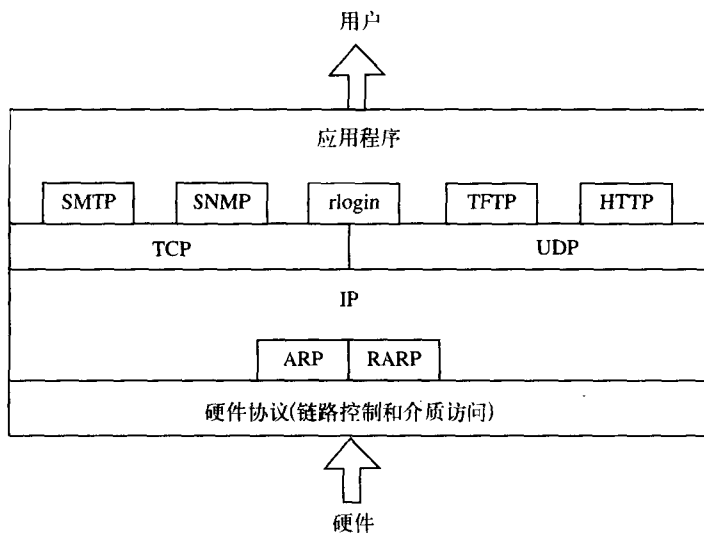


图1-1 TCP/IP协议结构图

网络所涉及的基本分层结构、报文封装、网络拓扑结构等内容属于网络的基本知识，我们不在本书中讲述。读者可以在书店里找到几十本这样的书籍，挑选其中一两本进行阅读，以对网络知识有一个基本的了解。

对于TCP/IP协议和相关的应用，我们将进行详细的阐述。第2章重点介绍作为全书基础知识的TCP/IP。

Linux最初的版本就包含了TCP/IP，TCP/IP是Linux中最为稳定可靠、效率也极高的协议之一，但Linux还支持其它很多的协议，如：

1. IPv6

IPv6，有时称为IPng (IP Next Generation)，是对IPv4协议（原来的IP）的升级。其目的主要是为了解决现行IPv4中存在的三个问题：IP地址短缺、缺乏传输时间敏感性流量的支持、网络安全问题。

IPv6通过扩展地址位数来解决IPv4中最迫切需要解决的问题——地址空间问题，当然这种扩展对路由的性能会有一定的影响。Linux上已经存在Beta版的IPv6，可以运行在2.2.0的Linux核上。读者要了解IPv6的有关知识，可以访问以下网址：

<http://www.terra.net/ipv6/linux-ipv6.faq.html>

<http://playground.sun.com/pub/ipng/html/ipng-main.html>

2. IPX/SPX

IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange) 是Novell公司开发的基于Xerox网络系统(XNS)协议的专用协议栈。20世纪80年代，Novell公司的Netware表现得十分突出，成为了第一代局域网事实上的标准。Novell在其NOS中实现了面向业务的应用套件和客户方连接工具。

Linux拥有非常完整的IPX/SPX实现。Linux可以配置成IPX路由器、IPX桥、NCP客户机或NCP服务器（用于共享文件）、Novell打印的客户端、Novell打印服务器，以及PPP之上的IPX，IPX之上的IP等。

而且，Caldera还为在Linux上运行Novell Netware提供了商用的版本。有关Linux对IPX/SPX的支持，请访问以下网址：

<http://sunsite.unc.edu/mdw/HOWTO/IPX-HOWTO.html>

3. AppleTalk协议

AppleTalk是Apple公司的互连网络协议栈的名称。该协议通过点到点的网络模式提供基本的文件和打印共享。每个机器可以同时作为客户机和服务器，其所需的软硬件在每个Apple计算机中都已包含，而Linux能够提供完全的Appletalk实现。

4. 广域网 (X.25, 帧中继)

许多第三方的厂家为Linux提供T-1、T-3、X.25和帧中继的产品，一般进行此类连接需要一些专用的硬件。提供硬件的厂商也提供相应的协议资源。读者要了解Linux与广域网的相关问题，请访问以下网址：

<http://www.secretagent.com/networking/wan.html>

5. ISDN

Linux内核中具有内置的ISDN功能，Isdn4linux系统可以控制ISDN的PC卡，并能通过实现Hayes命令集（“AT”命令）来仿真调制解调器。这样，Linux既可以作为终端程序使用

HDLC连接，也可以使用PPP进行Internet连接。有关Isdn4linux，读者可以访问<http://tsikora.tiac.net/i4l-faq/eng-i4l-faq.html>。

6. PPP、SLIP与PLIP

Linux内核内置支持PPP (Point to Point Protocol)、SLIP (Serial Line PPP) 和PLIP (Parallel Line IP)。PPP是用户连接其ISP (Internet服务提供者) 最为常用的方法。PLIP提供两台机器之间花费很小的连接，使用并行接口或者某些专用的接口，速度从10kbps到20kbps。有关PPP和SLIP的知识在第8章中进行介绍。

7 ATM

当Linux还处于测试阶段时，就包含了对ATM的支持，有许多相关的服务都可以在Linux上运行，这些服务和协议目前一般还处在实验阶段，读者可以访问<http://lrcwww.epfl.ch/atml>以了解详细的知识。

1.4 Internet/Intranet解决方案

一些企业的分公司或部门的小型销售集团希望能有一种办法，使他们的十几名销售和支持人员共享文件、定期观看更新的本地HTML文档并能方便地连到WWW，这就需要建立Intranet。但不幸的是，使用商业工具创建Intranet，即便只需要支持少量用户，也要花费数千美元。而Linux已使许多企业都能便宜地建立Intranet，利用旧的486、某些网卡，并花几小时时间就能建立一个Intranet，把Web接入本地HTTP服务、电子邮件、文件共享，甚至新闻和交谈组组合在一起，其现金投资可忽略不计。使用Linux、Apache和其它免费工具建起来的小型Intranet，总开支不到50美元，而且还是购买软件，不是免费下载。

当然用这种方法建立起来的小型Intranet存在问题。虽然有越来越多的供应商、增值零售商和咨询商提供Linux支持服务，但Linux用户还没有发现像Microsoft或IBM这样规模的公司能在出现故障时给予帮助。在某些情况下，Linux技术支持还仅仅是通过电子邮件从供应商处获得。此外，Linux用户也通过新闻组和邮寄清单构造信息支持网络。安装Linux软件也可能常常要涉及编译源码的问题，这是使用Windows NT程序时不会出现的情况。有鉴于此，某些IT厂商对于是否支持Linux还举棋不定，至少不愿表示公开支持。但是不管怎样，对Linux的支持现在处于飞速发展的过程。如现在的Oracle、Sysbase、Informix和IBM等公司都开发出了支持Linux的系列产品。

Linux支持全面的Internet/Intranet解决方案，包括以下几种服务：

1. 邮件

邮件服务器 Sendmail是在UNIX平台上事实上的标准邮件服务器程序。它拥有极高的可靠性、可伸缩性，并且能毫不费力地处理几千个用户的邮件服务。当然还有很多其它的服务器程序，如smail、qmail等。邮件服务在第3章进行介绍。

远程访问邮件 在单位或ISP中，用户通常要从桌面远程访问邮件。对于Linux而言，有很多可以选择的方案，如POP(Post Office Protocol，邮局协议)、IMAP (Internet Message Access Protocol，Internet消息访问协议)。POP一般用来在服务器和客户机之间传输邮件，而IMAP用来在服务器之间传输邮件。

邮件用户代理 在Linux上有大量的邮件用户代理 (MUA) 可供使用，有些是图形方式的，有些是文本方式的，最为常用的有Pine、mutt、elm和Netscape。

Fetchmail 还有一个非常有用的邮件工具: **Fetchmail**。**Fetchmail**是一个免费的、高可靠性的、文档组织很好的远程邮件检索与传递工具。它支持很多流行的远程邮件协议, 并且支持IPv6。

Fetchmail从远程邮件服务器上检索邮件, 使用SMTP进行邮件传递, 它可以被通常的邮件用户代理, 如**mutt**、**elm**、**BSD Mail**等, 所读取。

上述所有与邮件相关的服务都将在第3章进行介绍。

2. Web服务器

许多Linux的发布中包含了**Apache Web**服务器。**Apache**或者其派生的服务器占Internet上所有服务器数量的一半以上。**Apache**的优势在于其模块化设计、性能稳定和速度快。只要有好的硬件, 并且配置得当的话, 它可以支持很高的流量。**Yahoo**、**Altavista**、**GeoCities**、**Hotmail**等都使用这种服务器的定制版本。

要在该服务器上支持SSL(**Security Socket Layer**)的话, 还有其它一些工作要做, 读者可以参见第3章。

3. Web浏览器

Linux平台上存在大量的浏览器。**Netscape Navigator**就是其中很好的选择, 而**Mozilla**也有Linux版本。还有一个比较流行的基于文本的浏览器是**lynx**, 该浏览器的速度极快, 可惜不支持图形显示。

4. FTP服务器和客户

FTP表示文件传输服务协议(**File Transport Protocol**)。**FTP**服务器可以让客户程序与其进行连接, 并为客户提供检索(下载)文件的服务。Linux上有许多**FTP**服务器和客户程序, 基于文本方式的和基于图形方式的都有, 这些软件一般都可通过[http:// sunsite.unc.edu/pub/Linux/system/network/file-transfer](http://sunsite.unc.edu/pub/Linux/system/network/file-transfer)找到。

5. 新闻服务

Usenet (或称为**news**)是一个大的公告牌系统, 其中包括各种各样的主题, 采用层次方式的组织结构。网络上的计算机通过**NNTP**协议在**Usenet**上交换文章。在Linux上也有很多这种软件实现。

6. 域名服务

DNS服务器的工作是将容易读取的名称转换成IP地址。**DNS**服务器并不可能知道Internet上所有机器的IP地址, 对于不知道的地址, 它会请求其它的服务器进行帮助。如果该地址存在的话, **DNS**将告诉客户端正确的IP地址, 否则会反馈一个找不到该地址的消息。

UNIX上域名服务程序都称为**named**。有关这些知识将在第2章和第3章介绍。

7. 其他服务

Linux还支持很多其他的Internet/Intranet服务和协议, 如**DHCP**与**bootp**、**NIS**等, 这些服务和协议构成了Linux Internet/Intranet全面解决方案的庞大体系。

1.5 文件与打印共享

总的来说, 网络应用的目的是提供资源共享(包括程序、数据、信息)和网络用户的合作, 其中最为主要的就是资源共享。所谓资源共享是指: 要使得网络中的所有程序、数据和各种资源能被用户使用, 而用户不必(或者不用花很大的精力)考虑自己在网络中的位置和

资源在网络中的位置。

文件共享与打印共享可能是用户最为需要的资源共享方式。

FTP（第2章和第3章进行阐述）就是这样一种支持文件共享的协议和应用程序。但FTP的文件共享是不透明和非实时的，不是一种多用户共享的方式。第4章讲述的网络文件系统（NFS）是一种真正共享的方式。第4章将讲述网络信息服务（NIS），这是一种分布式的访问控制系统。

有些方式的资源共享是可以跨平台的，如WEB共享，而有些方式的共享在跨平台时还要费一番精力，比如在Windows和Linux之间进行打印机共享等。有些资源的共享需要运行其它的第三方软件，另一些则可能要进行正确的配置。第5章重点剖析Linux与Windows的集成。

1.6 Linux网络的安全问题

随着Internet的普及，网络安全问题越来越引起人们的重视。1996年初，美国国防部宣布其计算机系统在前一年中遭到25万次进攻，更令人不安的是，大多数进攻未被察觉。这些进攻给美国国家安全带来的影响程度还未确定，但多数已发现的进攻是针对计算机系统中存放的敏感数据和分类信息，其中2/3的进攻被认为是成功的，入侵者（黑客）获取、修改或破坏了系统中的数据。

只要一谈到安全，人们总是要说防火墙，防火墙是内部网络安全的有力保证，但它只是安全策略的一个部分。安全需要一整套完善的立体防御体系来保证。第6章将详细介绍网络安全，使网络用户可以充分地认识和了解可能面临的危险，以便采取切实有效的措施，保证网络运行正常。另外还介绍了一些在Linux上使用的安全工具软件（包括防火墙等）。

1.7 Linux网络管理工作

只要将几个Linux机器（或者其它机器）连到一起，就会有网络管理工作，就应该有一个特定的网络管理员。网络管理员需要一些专门的知识来确定系统如何连接、所需的安全级别和共享资源（打印机、磁盘等）的分配。另外，网络管理员还需要维护系统成员，网络地址和用户接口的列表，并始终保证网络的正常运行。只要耐心地学习，任何人都可以胜任一个网络管理员的工作。在大多数情况下，网络管理员和系统管理员是同一个人。

1. 硬件与软件的问题

作为网络管理员，如果要求为自己控制的计算机选择网络软件和硬件，需要考虑以下一些情况。如果在同一个建筑物内连接网络，当然要选择局域网方式连网，可以采用各种各样的网络层协议，如果没有特殊的要求，就可以选择TCP/IP。

在长距离连接中，可以使用调制解调器进行低速传输。用点到点协议（PPP）或串行线路接口协议（SLIP）都能提供异步的TCP/IP连接。UUCP软件也可以用于邮件、新闻和文件传输，但它具有一些局限性，所以本书没有对其进行重点描述。

在购买软件方面，一般不要买旧的连网软件。Linux所支持的网卡等驱动程序都会在HOWTO文件中说明，因此在购买网卡时，要确认选择了系统支持的网卡。

2. Linux网络管理

网络管理涉及网络资源和活动的规划、组织、监视、计费和控制，在OSI网络管理模型中，基本的网络管理功能被划分成五个功能域。这五个功能域通过与其它开放系统交换管理信息

分别完成不同的网络管理功能，它们分别是：故障管理（Fault Management），配置管理（Configuration Management），性能管理（Performance Management），计费管理（Accounting Management）和安全管理（Security Management）。

Linux带有一整套的网管命令，这些命令可以诊断很多网络故障，如果要进行高级的网络监控，如远程主机的负载情况，是否有人非法访问等，可以使用一些免费的软件。此外，Linux还支持SNMP（简单网络管理协议），可以在其上安装SNMP软件。

详细内容将在第7章介绍。

1.8 网络技术的演变

网络最初的雏形是两个计算机通过串口或并口进行通信，显然这样的方式只能传输简单的文件，网络基本上不具有可扩展性。直到9600bps的双绞线出现，这种情况才有了很大的改变。当前，100Mbps到桌面的网络传输速率已经随处可见。90年代的网络技术主要体现在改进网络结构、传输技术、交换技术、网络管理以及增进网络安全等方面。这些技术中的任何一种，都可以用一本书来进行讲述，它们是网络研究人员的工作，本书的第6章和第7章分别对网络管理和网络安全进行了简单阐述，而第8章讲述远程电话线连接。

近几年来网络技术的发展可谓日新月异，一会儿是ATM，一会儿是IP Switch，一会儿是交换代替路由，一会儿又是多层交换，这就使得网络工程师和网络构造者无所适从，感到很困惑。其实网络技术的发展，总的目的是提高网络的服务质量，即让网络提供尽可能高的带宽，尽可能少的出错率，尽可能小的延迟。人们在关注网络硬环境的同时，也越来越关注网络的软环境。硬环境是指网络的物理和底层设备，软环境则是在物理网络上运行的协议、管理配置工具、应用程序等。只有软硬环境的结合，才能提供安全性强、可伸缩性好，性能卓越的网络。

对于终端用户而言，情况却不同。虽然网络用户在选择网络层协议时，有IPX、ATM、IP等，但实际上现在的终端用户使用IP的占绝大多数。各种网络应用：Telnet、FTP、USENET、WWW都是以IP为基础的。因此终端用户对网络的学习要从TCP/IP开始。

1.9 小结

从前面的阐述可以看出，Linux有其固有的优点：开放性，价格极其便宜，网络支持性能高，各种免费软件应有尽有等等。但是，使用Linux与使用Windows是不同的，Linux需要各种各样的配置和设置，需要使用者对所使用的功能有一定的了解。因此，必须学习如何使用和管理Linux。与DOS、Windows和OS/2不同，Linux需要管理。管理者通常被称为系统管理员，他们负责维护系统并担负增加和删除用户帐户，在固定的基础上备份系统，安装新软件，配置系统，修改错误等任务。即使是商用UNIX，也同样要经常面对这些问题。但是Linux的用户却没有商用UNIX用户那么全面的技术支持。

读者似乎有些害怕Linux了，其实，现在的情况正在一步步地好转。随同Linux一同发布的有许多Howto文件和readme文件。这些文件对使用Linux提供第一手的帮助。而在Internet上也有上千个讨论组和站点（国内就有几十个，而且这些站点都在慢慢地完善）提供各种各样的疑难解答。我们编写本书的目的也是为了让读者对Linux网络系统的使用、管理有一个全面的了解。只要努力，一定能够成为Linux网络方面的专家！

第2章 理解TCP/IP

TCP/IP是当今最成熟、应用最广泛的互联网技术，它拥有一整套数据协议。按照TCP/IP建立的、世界最大的网间网——Internet覆盖了全世界的许多大学、科研机构、政府及军事部门，它已成为世界上许多人工作环境中不可或缺的一部分。

TCP/IP是一项从实践中诞生的、并在实践中不断得到发展和完善的网络技术。现在，TCP/IP技术成为业界普遍接受的网络标准，TCP/IP网络也逐渐进入科研、教育、工商业、政府机关等部门，成为一种信息基础设施。因此，在介绍Linux网络技术之前，首先要介绍一下TCP/IP网络技术。

2.1 TCP/IP的历史

TCP/IP的起源要追溯到20世纪70年代中期，当时ARPA（Advanced Research Project Agency，即DARPA——Defense Advanced Research Project Agency的前身）为了实现异种网之间的互连（Interconnection）和互通（Intercommunication），大力资助网间网技术的研究开发，于1977年到1979年间推出了目前形式的TCP/IP体系结构和协议规范。

到了1979年，越来越多的研究开发人员投入到TCP/IP的研究开发之中，于是DARPA组织了Internet组织与配置委员会（Internet Control and Configuration Board，ICCB）来协调各方面的工作。

1980年前后，DARPA开始将ARPANET上的所有机器转向TCP/IP协议，并以ARPANET为主干建立了Internet（又叫互联网间网，Connected Internet）。

1983年1月，ARPANET到TCP/IP的转换全部结束，美国国防部命令联入远程网的所有计算机都必须采用TCP/IP协议。

为推广TCP/IP协议，DARPA以低价出售TCP/IP，并资助BBN（Bolt Beranek and Newman Inc.）实现其UNIX的TCP/IP协议，还资助加州大学伯克利分校将TCP/IP协议融入BSD UNIX（Berkeley Software Distribution UNIX），促成TCP/IP与当时多数大学中流行的BSD UNIX的结合。

到今天，TCP/IP技术以及Internet已经为广大计算机工作者、计算机厂商和计算机用户所接受，成为许多人工作环境的一部分。作为一种事实上的并日益进化的工业标准，TCP/IP技术方兴未艾。

2.2 TCP/IP通信基础

TCP/IP的核心思想是把千差万别的网络的最下面两层（物理层和数据链路层）硬件连接为物理网络，而在传输层和网络层上建立一个统一的虚拟的“逻辑网络”，屏蔽或隔离所有物理网络的硬件差异，从而实现普遍的“连通性”。

2.2.1 TCP/IP协议体系结构

TCP/IP协议是按照模块化的思想设计的。它将通信协议分为不同的层次，每个层次的协