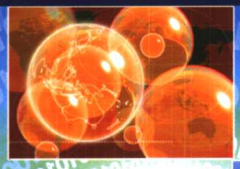
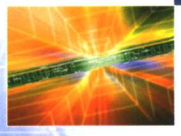
HZ BOOKS

Fedora Core 5 Linux 架站与网管





李蔚泽 著

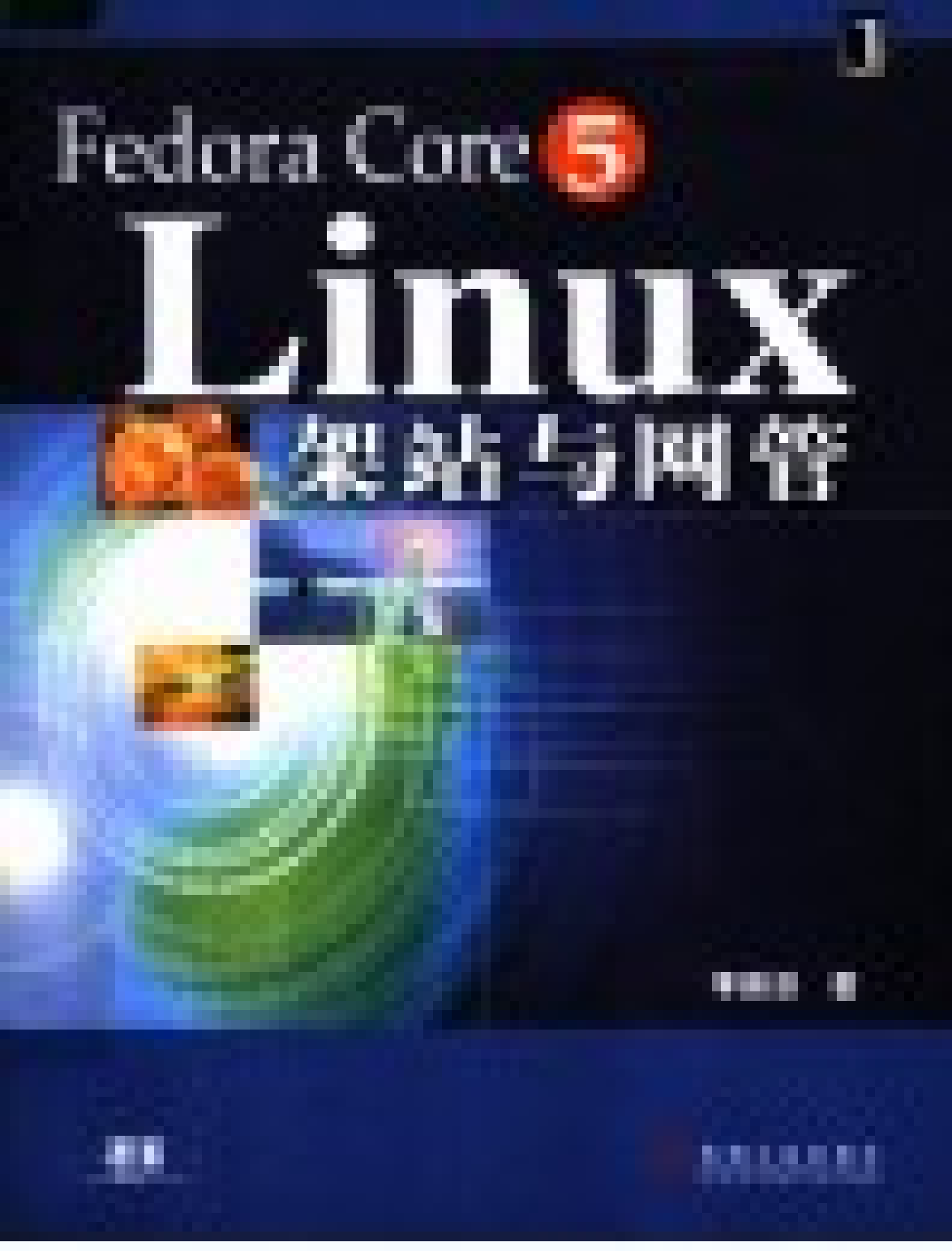
碁峰
www.gotop.com.tw

机械工业出版社
China Machine Press

Fedora Core 5

Linux

架站与网管



Fedora Core 5 Linux 架站与网管

李蔚泽 著

机械工业出版社
China Machine Press

本书系统讲解Fedora Core 5 Linux的使用方法，涉及服务器与网络管理两大领域的内容。主要内容包括：网络基本概念、Apache服务器、多重网站与安全通信、Apache图形设置工具、各种服务器设置方式、ARP与RARP、IPv4静态路由、动态路由、ICMP与IGMP、TCP与UDP、应用程序层和故障排除与系统监视等。本书采用理论阐述、命令操作以及图形工具使用并重的方式，讲解翔实，生动实用。对于广大的Linux专业人员来说，是一本不可或缺的参考书籍。

本书版权登记号：图字：01-2006-4283

图书在版编目（CIP）数据

Fedora Core 5 Linux架站与网管/李蔚泽著. －北京：机械工业出版社，2006.9
ISBN 7-111-19870-0

Ⅰ.F… Ⅱ.李… Ⅲ.Linux操作系统 Ⅳ.TP316.89

中国版本图书馆CIP数据核字（2006）第106913号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：李南丰
北京中兴印刷有限公司印刷 · 新华书店北京发行所发行
2006年9月第1版第1次印刷
186mm × 240mm · 27.75印张
定价：49.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

前　言

本书特别采用Fedora Core 5为说明的平台，其内容可涵盖大部分系统管理人员的需要，虽不敢自比为经典之作，但足以满足一般用户入门时的参考，这也是笔者撰写此书的初衷。

为了兼顾实用性与理论基础知识，本书收集了服务器与网络管理两大领域的主题，在开宗明义的第1章中，我们谈到有关网络的基本概念，这是管理人员在维护网站与各项服务前，理应熟悉的内容。

除此之外，本书的其余章节共包含10种各类型的服务器。这也是笔者撰写本书时遭遇的首要难题，因为要以有限的篇幅来说明如此繁多的服务器主题，势必要取其精华的部分，所以有关内容的筛选，着实花费笔者许多时间。

从第14章开始，是属于网络管理的范畴，因为基本上都是遵循OSI与TCP/IP的分层架构，由下而上逐层介绍，因此，建议读者按照章节顺序阅读，以保持学习的连贯性。

全书是笔者花费许多研究测试的时间，以及无数夜晚挑灯夜战的成果，虽然辛劳，但只求能满足读者的需求，同时也希望它是我们共同学习的起点。笔者才疏学浅，如果本书有遗漏或是不尽详细之处，还请各位读者不吝给予指教与提携，以使本书更臻完美。

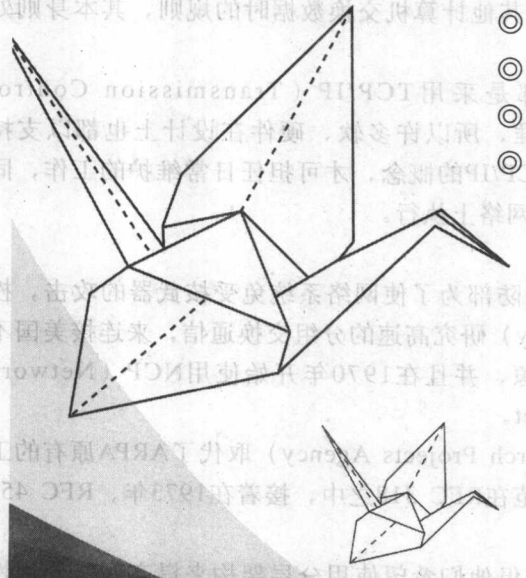
李蔚泽
jacklee1024@hotmail.com
2006年4月

目　录

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
◎ 常用的系统维护命令
◎ 网络管理程序



自从Internet出现以来，人们已经彻底改变了生活的方式以及对于信息的取得。举例来说，传统邮件目前大多数已经由E-Mail所取代，其中主要的原因不仅是经济上的考虑，更大的好处在于它的迅速与便捷；现在人们要查找所需的资料，也都因为时间及性能的原因，倾向于直接上网查找，不仅相关的信息容易取得，范围更可涵盖全球。

身为系统管理员，在维护及架构网络的各项服务前，必须建立基本的网络概念，以避免基础问题的发生，这也是笔者在每本书中所强调的概念。顺便提一下，本书所有提到的Linux平台，都是以Fedora Core 5为主，如果与读者使用的平台有所不同，本书的内容仍极具参考价值。

1.1 TCP/IP网络

所谓的“网络”一词包含的范围很广，凡是两台以上的计算机，使用任何类型的介质（例如电缆或无线电波）、任何类型的通信协议（例如TCP/IP或NetBEUI），或是任何形式的操作系统（例如Linux或Windows）来进行连接，同时以资源共享为目的，都可称为网络。

通信协议是网络上建立通信及传送数据时的标准，每一种通信协议都会利用一种以上的规则来定义如何传送数据、如何识别目的、如何处理错误情况以及如何压缩数据等内容，而有些通信协议会利用其他通信协议来作为与其他计算机交换数据时的规则，其本身则处理某一特别的任务。

因为目前多数的网络系统与Internet都是采用TCP/IP（Transmission Control Protocol/Internet Protocol）为通信协议标准，所以许多软、硬件在设计上也都以支持TCP/IP为目标。因此，系统管理员必须具备TCP/IP的概念，才可担任日常维护的工作，同时本书所介绍的各类服务器也都必须在TCP/IP网络上执行。

TCP/IP历史

TCP/IP起源于20世纪60年代，当时美国国防部为了使网络系统免受核武器的攻击，授权ARPA（Advanced Research Projects Agency）研究高速的分组交换通信，来连接美国不同区域内的超级计算机，以共享彼此间的资源，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定义了FTP（File Transfer Protocol）的标准。

ARPANet发展至此原本一切都相当成功，但他们希望使用分层架构来提高网络使用性能的构想却在实验后证明不可行，因为结果十分昂贵且传输速度缓慢，因此最后宣告失败。

1974年，Vinton Cerf和Robert Kahn提出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及主机对主机的数据转发服务。

1980年发展出UDP（User Datagram Protocol）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分组。同年ICMP（Internet Control Message Protocol）也加强了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将负责发展Internet的工作移交给NSF（National Science Foundation），因为Internet上扩展最快速的部分都是在学校网络（.edu）。图1-1中给出了TCP/IP通信协议的发展历史。

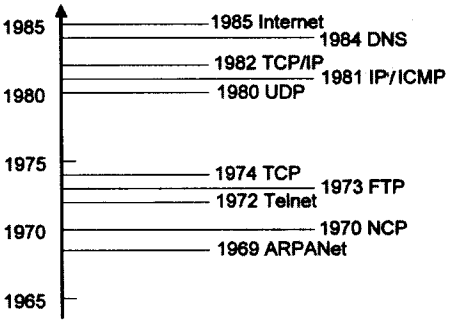


图1-1 TCP/IP通信协议发展历史

以上提到的RFC（Request For Comments），原来是Internet前身——ARPANET所提供的建议评论文件，主要由网络工程师与计算机学者共同发表。当每一份RFC得到足够的支持时，它会转为Internet标准、标准的一部分或是草稿。

而每一份RFC文件也都会有一个编号，当一份文件被赋予编号后就不会再修改，需要变动规范时，必须重新取得一个新编号。但并不是每一份有RFC编号的文件都有意义或与网络技术有关，有些只是幽默或历史。您可以到以下的网站查询每个RFC文件的内容：

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

取代XNS的原因

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

- 在TCP/IP中，它利用一个事先定义的层次式路径，允许管理人员以结构化的方式来维护大型网络，例如www.sina.com.cn。
- TCP/IP地址可以进行集中式的管理，例如.com、.net、.gov和.org等。

除了军事上的用途外，美国国防部还将TCP/IP授权给一些大学使用，例如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四层架构

为了提高软、硬件和通信协议的兼容性，在TCP/IP中也定义了层架构的概念，在这个架构中共分为四层：应用层、传输层、网络层与网络接口层等，如图1-2所示。以下是这些层的说明：

- 应用层

应用层定义了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，因此一般直接支持用户的程序都包含在此。

这个层包含的通信协议和服务有很多，例如HTTP（HyperText 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

传输层提供主机之间的通信工作阶段的管理，它也定义了传输数据时所使用的服务级别及连接状态，此层包含的通信协议有：TCP、UDP、ARP（Address Resolution Protocol）和RARP（Reverse Address Resolution Protocol）等。

• 网络层

网络层主要的功能是将数据封装成IP数据包，其中记录了主机及整个网络间转寄数据包的来源及目的地址信息，同时执行IP数据包的传递路由。

此层包含的通信协议有：IP、ICMP（Internet Control Message Protocol）、IGMP（Internet Group Multicast Protocol）以及ARP等。

• 网络接口层

网络接口层定义了如何通过网络物理地传送数据的详细内容，包含与网络介质直接连接的硬件设备，例如同轴电缆、光纤或双绞线等，以及如何将位转换为电信号。

这层中包含以太网络（Ethernet）、令牌环网络（Token Ring）、FDDI（Fiber Distributed Data Interface）、X.25、帧中继（Frame Relay）和RS-232标准等。

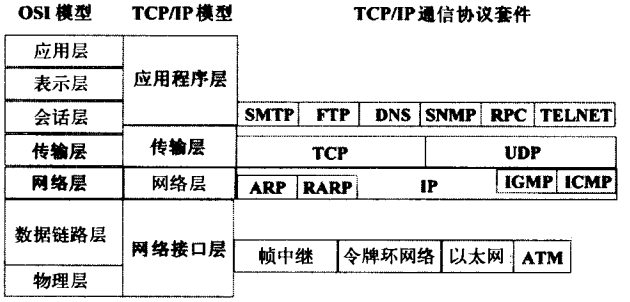


图1-2 TCP/IP架构模式

1.2 OSI七层模型

开放系统互连模型（Open Systems Interconnection model，OSI）是国际标准化组织（International Standards Organization，ISO）在1984年发展的全球通用标准，它的目标是创造一个开放性的网络系统环境，来让所有的系统能够相互运行，目前大部分通信协议也都是基于OSI模型来设计的。

由于OSI模型是由7个层所组成：应用层、表示层、会话层、传输层、网络层、数据链路层与物理层，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，所以只要软、

硬件都遵循OSI模型的标准来设计，则可确定所有网络组件都会具有兼容的特性。

这不仅是在大型网络中必备的法则，更可节省厂商开发的时间，因为如果每种产品都能符合特定层的标准，开发者就不需为了考虑兼容性的问题，而将其他层的标准包含在产品中，这同时也可简化错误产生时的故障排除过程。

接下来我们将针对OSI模型中的每一层说明其名称及功能，以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

由于网络架构必须包含不同的物理传输介质，所以在OSI中使用物理层来定义接口的物理特性，例如电气规格和信号处理的方式。它主要是利用电信号通过传输介质传送最基本的0或1信息，因此也可说物理层是由一些通信用的电子设备所组成。

著名的物理层接口有EIA RE-232、RS-449等，而常见的局域网络有以太网络、令牌环、分布式光纤数据接口、CCITT X.25分封网络、综合业务数字网与同步光纤网络等。以下是物理层定义的范围内容：

• 连接方式

指信号传送端和接收端之间的连接方式，其中包括点对点和多点连接等。

• 物理拓扑

网络使用的拓扑类型也就是网络的实际架构。

• 数字信号解译

所谓的信号解译是指规定如何将0与1的物理电信号传送到远方，也就是采用数字的方式。而以数字方式传送的好处是，数字通信设备较为简单而且抗干扰能力强，但主要的缺点则是信号较易衰减，一般广泛应用于局域网络。

• 模拟信号解译

将原本计算机内部的数字信号先转换为模拟信号再进行传送，而以模拟方式传送信息的最大好处是，可以使用多路复用器来增加带宽的使用，同时信号也较不易衰减。但它主要的缺点是，容易受噪声或外界的信号所干扰，一般广泛使用于广域网络。

• 位同步

为了使接收端正确读取发送端的信息，双方必须通过同步的方式进行。一般同步的方式有两种：异步传输和同步传输。

• 带宽使用

在带宽的使用上有两种方式：基频和宽频。

• 多任务器

为了有效利用带宽，因此产生了多任务的概念。一般最常用的方式有：Frequency-Division Multiplexing（FDM）、Time-Division Multiplexing（TDM）和Statistical Time-Division Multiplexing（StatTDM）等。

第2层：数据链路层

数据链路层的主要功能是，定义各节点对传输介质的使用方法，并处理信号传输所产生的错误，再将上一层（网络层）传来的分组传递到物理层。因为物理层只负责单纯的信

号传递，而没有任何数据帧的概念。

所以数据到了数据链路层后，必须将这些位数据形成帧，并配合流量和错误的控制，例如CRC（Cyclic Redundancy Check），来确保传输的正确性。

在数据链路层送出分组后，它会等待来自接收端所发出的确认信息，这可确定接收端已正确收到此分组。如果数据链路层没有收到来自接收端的ACK，则表示分组传送的过程出现问题，因此数据链路层会再次传递此分组，网桥便是在这个层使用的设备。

IEEE将数据链路层再细分为两个子层：介质访问控制（Media Access Control，MAC）和逻辑链路控制（Logical Link Control，LLC）。MAC是较低的层，它定义传输介质访问的方式，如CSMA/CD、Token Ring等。而LCC则为不同的网络类型提供数据传输的方法，它将数据重新包装、加上新的报头，并在数据链路层中加入链接的功能，以提供网络模块化的能力。

目前常见的位于数据链路层的通信协议为高级数据链路控制（High-level Data Link Control，HDLC），因为HDLC属于面向位，所以它的传输是由二进制数据组成，没有任何特殊句柄，但是数据帧内的信息存放着控制与恢复命令。图1-3中是一个简单的分组结构。

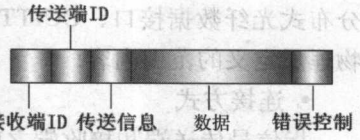


图1-3 简单的分组内容

第3层：网络层

为了使不在同一条传输介质上的节点能通过中间其他节点进行通信，OSI定义了网络层来规范数据在网络中的路由功能，以便分组能根据最短的路径传送到目的。如果数据可移动的路径不只一种，则网络层便可从中找出并决定一条最佳路径，路由器便是在此层中运行的设备。

网络层负责查看分组地址，如果目的在局域网络中，则进行直接传递，但如果目的属于其他网络段，则先将分组送到路由设备，再由路由设备传递到另一网络。

另外，网络层也提供将逻辑地址（例如IP地址）解析为硬件地址（MAC地址）、决定信息传送的路径、决定分组传送顺序与部分传输控制功能，例如拥塞控制，这些工作都是为了使信息传递达到最优化。

如果路由器上的网卡无法传送过大的数据，网络层会将此数据划分为较小的单位，而在接收端的网络层则必须重组这些划分后的分组，以得到原始数据内容。作用于此层的通信协议包括：X.25、IP、IPX、NWLink和NetBEUI等，另外路由器也是符合网络层标准的设备。

第4层：传输层

虽然网络层可将数据传输到目的，但由于它只负责相连节点间的数据传递，所以并不能保证分组能以正确的顺序抵达，也无法找出在传输过程中所产生的错误，因此传输层便负责控制数据在起始点和目的节点之间可靠无误的传输。

传输层的主要功能包含：分段处理、分组重新编号、流量管制和多路复用处理等。分段处理是指将传送到传输层的数据划分成适合网络层的分组大小，也就是将一份信息分封成多个分组。重新编号是指将同属一份信息的所有分组重新加上序号，以便接收端能按照

这个次序重组原来的信息。流量管制是协调数据在传送和接收时的速度，以避免传送速度太快而导致接收端来不及接收的问题。多路复用处理是指传输层连接的多任务情形，当网络层连接的速度足够快，且提供多个传输层连接使用时，可以经由多路复用处理来将这些传输层连接导入同一个网络层连接，作用于此层的通信协议有：NetBEUI、TCP、SPX和NWLink等。

由于服务需求的不同，传输层发展了以下5种不同级别的标准及相关通信协议：

• 级别0（TP0）——简单级别

具备最基本的传送连接功能，其流量控制、连接释放依赖于网络层的协助，但并不提供紧急数据的处理。

• 级别1（TP1）——基本错误恢复级别

除了具备级别0的功能外，TP1能根据网络层的错误反馈或连接释放作一些简单的错误恢复。如果网络层提供紧急数据传送的功能，级别1亦可让用户有传送紧急数据的选择。

• 级别2（TP2）——多路复用级别

提供多路复用的功能，数条传送连接的数据可以由一条网络连接传送。并具备扩充性编号，使用较大的接收窗口来进行数据量的控制和错误恢复。

• 级别3（TP3）——错误恢复多路复用级别

TP3表示级别1与级别2功能的总合，因此所负责的工作也较多。

• 级别4（TP4）——错误检测和恢复级别

TP4可说是功能最强的一个级别，除了具备级别3所具有的功能外，还能检测出数据的丢失、重复、乱序，进而完成恢复的工作。

第5层：会话层

会话层可允许不同计算机上的应用程序互相建立连接、使用或终止连接，这个过程就称为会话，通过会话的进行，可使系统建立会话、交换数据、释放会话、会话管理和错误恢复等。

会话层也支持同步的工作，它是利用在数据中设置检查点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之后的数据，这在网络状态不稳定的情形下非常重要，因为传送端不需重新传送所有的数据，所以可节省大量的时间。以下为会话层的主要功能：

• 令牌管理

令牌的使用主要是为了让用户具有公平传送信息的机会（非竞争式），其中规定拥有令牌的用户才具有传送信息的权利。为了使令牌使用权平均分配，令牌管理的机制应运而生，此机制可定义令牌的取得、转让与放弃等功能。

• 活动管理

活动属于会话连接中的一部分，一般是利用数据的性质来区分活动的范围，而会话服务有权控制活动单元的取消、中断、转移等管理工作。

• 对话控制

通常一个活动可由多个对话组成，而对话控制的主要适用范围在事务管理（Transaction

Management)。

• 异常报告

数据进行传递时可能会出现许多错误的情形，如果错误还未严重到中断传输，会话层可以利用异常报告服务向目的提供异常状况，再由用户判断采取的措施以使会话恢复正常。

第6层：表示层

表示层主要担任翻译的角色，因为不同的应用程序常使用不同的语法，而为了使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。所以传送端在送出数据之前，其表示层必须将数据从传送端的格式转换成传输过程的格式，而在到达接收端后，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，表示层可将传送的数据先经过加密处理再传送到网络上，而在到达接收端以后，再经过解密的处理还原原始数据内容，同时它也具有数据压缩的能力，以减少传输时的数据量。

注意： 压缩时需以不失真为原则，在压缩后的文字数据经过解压缩后必须完全还原，而压缩后的影像或语音数据，经过解压缩后其影像或语音也要符合一定的品质。

第7层：应用层

位于OSI模型的最上层是应用层，它的功能是直接支持用户应用程序，例如FTP、EMAIL和RPC等。不同计算机中的应用层可用来识别对方计算机传送的原始数据，同时也处理一般的网络访问、流量控制和错误恢复等工作。图1-4中是OSI七层模型。

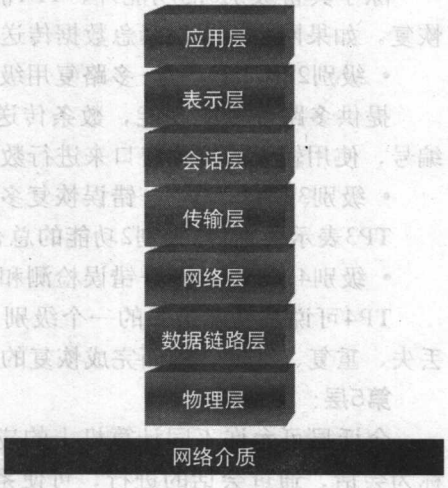


图1-4 OSI七层模型

注意： 有关OSI七层模型的详细说明，可参考以下的网页内容：http://lips.lis.ntu.edu.tw/ytchiang/study/others/tcpip/OSI.htm。

1.3 Linux网络配置文件

在Linux系统中，网络功能的运行必须借助许多配置文件的内容，虽然目前有许多工具或程序可用来针对这些文件的内容进行设置，但是站在系统维护的角度上，了解这些文件的内容是绝对必须的。

因为无法保证所有的命令或程序随时可用，如果命令或程序的执行产生问题时，就必须回到原始的配置文件中手动进行修改或维护。因此在这个小节中，笔者选择了与网络管理有关，且较为重要的网络配置文件来加以说明，希望读者能了解每个配置文件的功能及使用时机，以利管理工作的顺利进行。

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的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络或是Internet中，只要是使用TCP/IP作为通信时的协议，主机间就必须依靠IP地址来互相识别。

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，例如192.168.0.1。因为这个地址是由InterNIC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。

IP地址虽然可以准确地识别每一台主机，但是它也产生了一个问题——地址记忆的困难，因为对用户来说，一些数字的组合实在很难与特定的主机产生联想。

如果采用一些一般人较为易记的名称，例如ns1.fc5linux.com（主机名称）或ns1（别名），应该可以降低用户忘记主机地址的机会。因此，在TCP/IP网络上出现了一个解决方法——利用一个中介机制进行IP地址和易记名称的转换（名称解析）。

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服务器或是/etc/hosts文件。DNS服务器在名称解析的功能上较为强大，但是因为牵涉的内容很广，所以本书将在第11章中讨论。

虽然/etc/hosts文件的解析功能不如DNS，但因为它也可以提供名称解析的功能，而且设置内容简单，所以本书在此将针对它的内容加以说明。以下是一个/etc/hosts文件的示例：

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1         localhost.localdomain          localhost
192.168.0.1               ns1.fc5linux.com       ns1
```

上述是一个简单的示例，其中的记录可由系统自动产生，或是自行加入。这些记录的格式如下：

```
IP地址    主机名称    别名
```

在将IP地址、主机名称或别名等信息输入/etc/hosts文件后，就可以使用主机名称或别名来取代原有的IP地址。举例来说，假设一台Web服务器的IP地址为192.168.0.1，而它的主机名称为www.fc5linux.com，别名为www，则在本机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://192.168.0.1（局域网络和Internet中使用）
- http://www.fc5linux.com（局域网络和Internet中使用）
- http://www（仅限于局域网络中使用）

网络服务信息文件/etc/services

/etc/services是记录各种不同网络服务的信息文件，在这个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/通信协议名称    [别名]    [批注]
```

这个文件允许使用连接端口号/通信协议名称的格式来对应特定的服务名称，而有些程