Fedora Core 3 Linux 架站实务

李蔚泽 编著

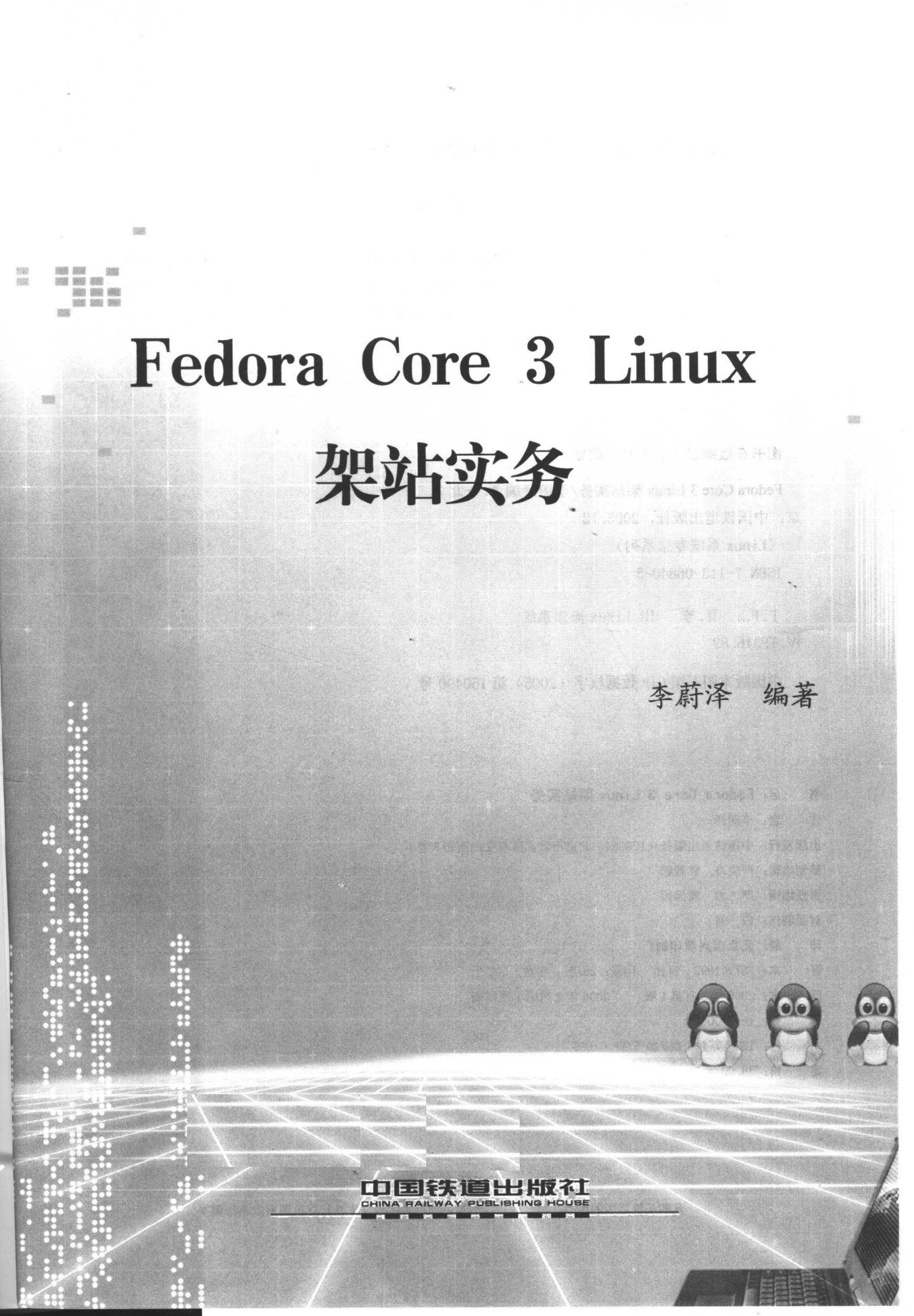
- 本书精心收录了11种最常用的服务器架设方法。
- 在开宗明义的第1章讲解了入门者所需的网络基本概念。
- 为使读者对每一类服务器融会贯通，在每章开始均先说明各类服务器的运行原理。
- 舍弃了市面上一般书籍庞杂的内容，取而代之对核心部分的剖析。
- 兼具了理论与实践两方面。
- 将帮助读者在最短的时间内由零开始轻松的完成服务器架设。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

Fedora Core 3 Linux

架站实务

李蔚泽　编著



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

北京市版权局著作权合同登记　图字：01-2005-4564 号

版　权　声　明

图书在版编目（CIP）数据

Fedora Core 3 Linux 架站实务/李蔚泽编著. —北京：中国铁道出版社，2005.12
（Linux 系统专家系列）
ISBN 7-113-06840-5

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（2005）第 150490 号

书　　名：Fedora Core 3 Linux 架站实务
作　　者：李蔚泽
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
策划编辑：严晓舟　郭毅鹏
责任编辑：严　力　黄园园
封面制作：白　雪
印　　刷：北京市兴顺印刷厂
开　　本：787×1092　1/16　印张：26.5　字数：607 千
版　　本：2006 年 2 月第 1 版　　2006 年 2 月第 1 次印刷
印　　数：1～4 000 册
书　　号：ISBN 7-113-06840-5/TP・1695
定　　价：38.00 元

出 版 说 明

近十年 Linux 在全球信息界创造了奇迹，它已经可与微软的崛起相提并论。Linux 的构思源自 Andrew Tanenbaum 所开发的 Minix，起初的发展是以 386（486）为设计目标，但是目前支持的平台增加了许多，例如 Compaq Alpha AXP、Sun SPARC、PowerPC、IBM S/390、HP PA-RISC 与 AMD 等机器目前都可执行 Linux。由于 Linux 以 GPL（General Public License）的方式来发布，所以允许使用任何形式来复制与分发 Linux。而随着投入研究和开发的人数激增，Linux 的功能也愈趋完善，到目前为止，它已可和微软操作系统相抗衡。

Linux 最大的优点——经济，因为不需花费可观的版权费用，就可使用功能强大的操作系统及其内置的软件包。除了经济的好处外，Linux 还包括以下的优点：

（1）在 Linux 上同时执行多个程序（多任务），支持多种文件系统；

（2）与现今的 System V 以及 BSD 等主流 UNIX 系统均可兼容，原本在 UNIX 系统下可以执行的程序，几乎可以完全移植到 Linux 上；

（3）可采用多种图形管理程序（例如 GNOME 和 KDE）来改变不同的桌面图案或功能菜单；

（4）目前可以执行 Linux 的平台有很多，并不只限于 Intel 计算机，而且可以使用多个处理器来执行服务器工作，这更增加 Linux 在系统或服务器管理上的能力；

（5）与 UNIX 系统一样，Linux 使用 TCP/IP 为默认的网络通信协议，除此之外，它还内置许多服务器级的软件，例如 Apache（Web 服务器）、Sendmail（邮件服务器）、VSFTP（FTP 服务器），或 Squid（代理服务器）等，所以您不需额外购买其他的软件，即可直接利用 Linux 来担任全方位的网络服务器。

由于互联网的迅速发展，学习 Linux 成为形势所趋。为满足广大读者的学习需要，我社从台湾碁峰资讯股份有限公司引进了优秀的 Linux 专业书籍，以飨读者。本书由聂雪军整稿，作者李蔚泽老师也为本书简体版的改编作了大量的工作，在此一并表示感谢。

2005 年 10 月

前　言

本书采用最新版的 Fedora Core 3 平台，内容可涵盖网管人员平日的需求，虽不敢自比经典之作，但足以担任一般用户架设网站时的入门书，这也是笔者撰写时的初衷。

第 1 章介绍了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，首先要熟悉的内容。除此之外，在本书的其余章节，共包含 11 种类型的服务器，这也是笔者在撰写时遭遇的首要难题，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。所幸有赖以往的经验，再辅以大量的参考文献，总算完成令人满意的内容，相信读者在细心阅读后，必可发现笔者求证时的用心。

第 2～4 章可说是本书最大的重点所在，介绍了目前 Internet 上占有率最多的 Web 服务器——Apache，它也是企业急于树立形象与拓展商机的最佳选择，无论如何都建议您仔细地阅读。

第 5 章是有关 FTP（File Transfer Protocol）服务器的运行，顾名思义，它是提供客户端与服务器间文件交换时的平台，因此一般企业网站都会竭尽所能提供此项服务，以吸引用户访问。

第 6 章介绍的邮件服务器也是现今企业网络必备的利器，因为在目前电子信息数据充斥的环境中，早已跳离传统的纸张文件，笔者实在无法想像如果没有借助电子邮件的传递，企业如何完成日渐复杂的商业活动。

第 7 章说明的 SAMBA 服务器是沟通 Windows 和 Linux 操作系统的绝佳工具，有了它，一般用户就可轻易通过“网上邻居”来访问 Linux 上的共享数据，这对信息的集成实在是举足轻重。

第 8 章与第 9 章主要着眼点在于带宽使用率与数据安全的提升，利用代理（Proxy）服务器可以将常用的网页内容保存在硬盘中，以避免重复连接至相同网页时消耗的带宽。而 NAT 服务器与防火墙在目前已是企业网络不可或缺的机制，它们可分别用来作为 IP 地址不足，以及保障信息交换安全性的解决方案。

第 10 章是有关 DHCP 服务器的内容，正确地使用 DHCP，可以节省许多平时维护客户端 IP 配置的时间。

第 11 章介绍的 DNS 服务器在客户端连接 Internet 时，肩负着名字解析的工作，如果没有这个机制，客户端可能很难顺利地连接到 Internet。

第 12 章的网络文件系统——NFS，则是利用分布式系统的概念，将网络上原本分散的共享资源，集成在服务器的文件系统中。

第 13 章说明了新闻服务器——INN 的运行原理，以及实际构建时所需注意的问题。

最后一章是有关 OpenSSH 服务器的内容，它可强化网络通信时的安全性。

由于笔者才疏学浅，如果本书有遗漏或不尽详细之处，还请各位不吝指教与提携，以使本书更臻完美。

李蔚泽
jacklee1024@hotmail.com

目 录

CHAPTER 1

网络基本概念

本章重点

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

自从 Internet 出现后，人们已彻底改变了生活的方式以及对于信息的取得方式。而作为系统管理员，在维护及架构网络的各项服务之前，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 3 为主，如果与读者使用的平台有所不同，本书的内容仍然具有很大的参考价值。

1-1 TCP/IP 网络

“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（例如缆线或无线电波），任何类型的通信协议（例如 TCP/IP 或 NetBEUI），或是任何类型的操作系统（例如 Linux 或 Windows）来进行连接，同时以资源共享（Sharing）为目的，都可称为网络。

而通信协议（Protocol）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、如何处理错误情况与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于遭受核武器的攻击，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，如图 1-1 所示。

1972 年，DARPA 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 制定了 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（Layering）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。

到了 1974 年由 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数据包。同年 ICMP（Internet Control Message

Fedora™ Core 3 为 Fedora™ Project 的产品。

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 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）。

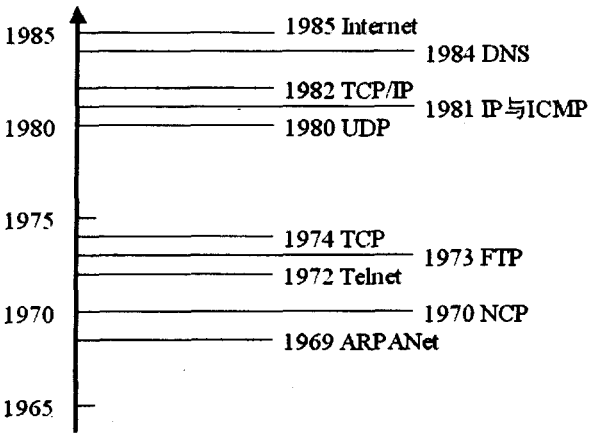


图 1-1　TCP/IP 通信协议发展历史

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，需要变动规格时，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 通信协议出现时，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。
- TCP/IP 地址可以进行集中式的管理，例如.com、.net、.gov 和.org 等。

而除了军事上的用途外，美国国防部也将 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 四层结构

为了提高软、硬件和通信协议的兼容性，在 TCP/IP 中也定义了层结构的概念，在这个结构中共分为 4 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（Application Layer）**
  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，其中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。
- **传输层（Transport Layer）**
  传输层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等级及连接状态，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（Internet Layer）**
  网络层主要的功能是将数据封装（Encapsulate）成 IP 数据报（Datagram），其中记录了主机及整个网络间转发数据报的源及目的地址信息，同时执行 IP 数据报的路由转发（Routing）。在此包含的通信协议有：IP、ICMP（Internet Control Message Protocol）、IGMP（Internet Group Multicast Protocol）以及 ARP 等。
- **网络接口层（Network Interface Layer）**
  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，这包含与网络介质直接连接的硬件设备，例如同轴电缆（Coaxial Cable）、光纤（Optical Fiber）或双绞线（Twisted-Pair Copper Wire）等，以及如何将位转换为电子信号。在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 等标准。

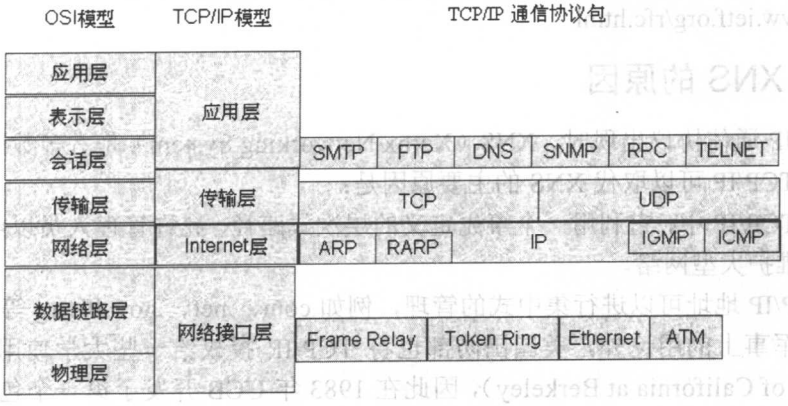


图 1-2 TCP/IP 架构模型

1-2 OSI 七层模型

开放式系统互联模型（Open Systems Interconnection model，OSI）是国际标准化组织（International Standards Organization，ISO）在 1984 年所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，来让所有系统能够相互运行，目前大部分的通信协议也都是基于 OSI 的模型来设计。

由于 OSI 模型是由 7 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等，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，如图 1-3 所示。

图 1-3　OSI 七层模型

这不仅是在大型网络中必备的规则，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，则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（Physical Layer）

由于网络结构必须包含不同物理的传输介质，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。它主要是利用电子信号通过传输介质，以传送最基本的“0”或“1”信息，因此也可说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 RS-232、RS-449 等，而常见的局域网则有以太网、令牌环、分布式光纤数据接口、CCITT X.25 分组网络、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**

  指信号发送端和接收端之间的连接方式，其中包括点对点（Point-to-Point）和多点连接（Multipoint Connection）等。

- **物理拓扑**
  网络使用的拓扑（Topology）类型，也就是网络的实际结构。
- **数字信号解译**
  所谓的信号解译是指规定如何将“0”与“1”的物理电子信号发送到远方，也就是采用“数字”的方式。
  而以数字方式发送的好处是，数字传输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，一般广泛使用于局域网。
- **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发送，而以模拟方式发送信息最大的好处是，可以使用多路复用器（Multiplexer）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。
- **位同步（Bit Synchronization）**
  为了使接收端正确解译发送端的信息，双方必须通过同步（Synchronization）的方式进行，一般同步的方式有两种：异步（Asynchronous）传输和同步（Synchronous）传输。
- **带宽使用**
  在带宽的使用上主要分为两种方式：基带（Baseband）和宽带（Broadband）。
- **多路复用**
  为了有效利用带宽，因此产生了“多路复用”（Multitasking）的概念，一般最常用的方式有频分多路复用（Frequency-Division Multiplexing，FDM）、时分多路复用（Time-Division Multiplexing，TDM）和统计时分多路复用（Statistical Time-Division Multiplexing，StatTDM）等。

➤➤ 第 2 层：数据链路层（Data Link Layer）

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）传来的数据包传递到物理层，如图 1-4 所示。

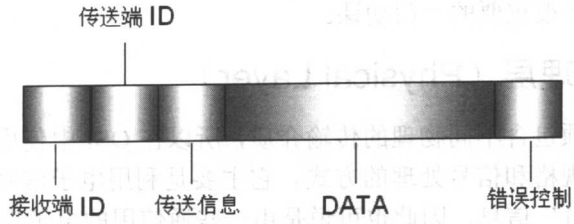


图 1-4　简单的数据包内容

因为物理层只负责单纯的信号传递，同时没有任何数据帧（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帧，并配合流量和错误的控制，例如 CRC，来确保传输的正确性。

在数据链路层送出数据包后，它会等待来自接收端所发出的确认（Acknowledgement，

ACK）信息，这可确定接收端已正确收到此数据包。如果数据链路层没有收到来自接收端的 ACK，则表示在数据包传送的过程出现问题，因此数据链路层会再次传递此数据包，网桥（Bridge）便是使用在这个层的设备。

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）等。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 LLC 则为不同的网络类型提供数据传输的方法，它会将数据重新封装、加上新的报头（Header），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（Bit-Oriented）的协议，所以它的传输是由二进制数据所组成，并没有任何特殊句柄，但是数据帧内的信息存放着控制与恢复命令。

➤➤ 第 3 层：网络层（Network Layer）

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，因此 OSI 定义了网络层来规范数据在网络中的路由功能，以让分组能按照最短的路径传送到目的。如果数据可移动的路径不止一种，则网络层便可从中找出并决定一条最佳路径，路由器（Router）便是在此层中运行的设备。

网络层负责查看数据包地址，如果目的在局域网中，则进行直接传递，但如果目的属于其他网络段，则会先将数据包送到路由设备，再由此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、决定数据包传送顺序与部分的传输控制功能，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（Transport Layer）

虽然网络层可将数据传输到目的地，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节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（Segmentation）、分组重新编号、流量控制和多任务处理等。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，也就将一份信息分成多个数据包，而重新编号是指将同属一份信息的所有数据包重新加上序号，以便接收端能按照这个次序来重组原来的信息。

流量控制则是协调数据在发送和接收时的速度，以避免发送速度太快而导致接收端来不及接收的问题，多任务处理则是指传输层连接的多任务情况，当网络层连接的速度够快，且提供多个传输层连接使用时，可以经过多任务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 种不同等级的标准及相关通信协议：

- **等级 0（TP0）——简单等级（Simple Class）**
  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。
- **等级 1（TP1）——基本错误恢复等级（Basic Error Recovery Class）**
  除了具备等级 0 的功能外，TP1 还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，等级 1 也可让用户有传送紧急数据的选择。
- **等级 2（TP2）——多路复用等级（Multiplexing Class）**
  提供多路复用的功能，数条运送连接的数据可以经过一条网络连接传送。并具备扩充性编号（Extended Numbering），使用较大的接收窗口（Receive Window）来进行数据量的控制和错误恢复。
- **等级 3（TP3）——错误恢复多路复用等级（Error Recovery and Multiplexing Class）**
  TP3 表示等级 1 与等级 2 功能的总和，因此所负责的工作也较多。
- **等级 4（TP4）——错误检测和恢复等级（Error Detection and Recovery Class）**
  TP4 可说是功能最强的一个等级，除了具备等级 3 的功能外，并能检测数据的流失、重复、失序等情况，而做恢复的工作。

➤➤ 第 5 层：会话层（Session Layer）

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

它也支持同步的工作，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，则只需重送最后一个检查点之后的数据，这在网络状态不稳定的情况下非常重要，因为传送端不需重新传送所有的数据。以下为会话层的主要功能：

- **令牌管理（Token Management）**
  使用令牌（Token）主要是为了使传送信息的机会较为公平（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。而为了使令牌使用权平均分配，令牌管理的机制便因此产生，此机制可定义令牌的取得、转让与放弃等功能。
- **活动管理（Activity Management）**
  活动是属于会话连接中的一部分，一般都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（Dialogue Control）**
  通常一个活动可由多个对话（Dialogue）所组成，而对话控制主要的适用范围则在事务管理（Transaction Management）时。
- **异常报告（Exception Reporting）**
  数据进行传递时可能会出现许多错误的情况，如果错误还未严重到中断传输时，会话层可以利用异常报告服务来向目的提供异常情况，再由用户判断采取的措施以使会话恢复正常。