普通高等教育“十一五”规划教材

网络工程教程

鲍 蓉 主 编
宋子强 孟凡立 副主编

中国电力出版社
www.infopower.com.cn

普通高等教育“[illegible]”规划教材

网络工程教程

鲍 蓉 主 编
宋子强 孟凡立 副主编
谢 俊 殷 丽 朱永红 参 编

中国电力出版社
www.infopower.com.cn

内容提要

本书为普通高等教育“十一五”规划教材。针对本科计算机网络工作课程教学要求，本书介绍了网络的传输介质、网络互连设备、网络调试、网络应用服务器的搭建、局域网技术及应用、虚拟局域网的建立和互连、无线局域网、Internet 的接入、路由和交换技术、访问控制列表、NAT 与 VPN 技术、网络安全与管理基础等内容。全书共 15 章，附录给出了常见的端口协议一览表、子网掩码速查表及各章节用到的命令，以便于学习使用。

本书的特点是紧贴本科教学需求、图文并茂，从教学需要和工程实践两个角度出发，既重视实践又兼顾原理，深度和难度相适宜。

本书主要供高等院校网络工程专业和计算机相关专业高年级本科生作为教材使用，同时也可供计算机网络技术人员、开发人员及管理人员参考。

图书在版编目（CIP）数据

网络工程教程 / 鲍蓉主编. —北京：中国电力出版社，2008

普通高等教育“十一五”规划教材

ISBN 978-7-5083-6377-6

Ⅰ. 网… Ⅱ. 鲍… Ⅲ. 计算机网络－高等学校－教材 Ⅳ. TP393

中国版本图书馆 CIP 数据核字（2007）第 184570 号

丛 书 名：普通高等教育“十一五”规划教材

书　　名：网络工程教程

出版发行：中国电力出版社

地　　址：北京市三里河路 6 号　　邮政编码：100044

电　　话：（010）68362602　　传　　真：（010）68316497，88383619

服务电话：（010）58383411　　传　　真：（010）58383267

E-mail：infopower@cepp.com.cn

印　　刷：航远印刷有限公司

开本尺寸：185mm×260mm　　印　　张：18　　字　　数：424 千字

书　　号：ISBN 978-7-5083-6377-6

版　　次：2008 年 2 月北京第 1 版

印　　次：2008 年 2 月第 1 次印刷

印　　数：0001—4000 册

定　　价：27.00 元

前　言

只是不到20年的发展，以Internet为主要特征的计算机网络技术的快速发展已经从根本上改变了人们的生活，工作、学习、娱乐无一能够离开网络。打好网络技术基础已成为当代大学生学习专业核心技术的必经之路。

计算机网络工程是针对“网络工程”专业方向学生开设的一门实践性非常强的课程，知识体系综合交叉、技术难度较大。目前的各种网络工程教材大多注重理论而缺少实践，有些又只注重设备的使用而与原理脱节。教材难选、课程难教、实验难做、学生难学已成为众多高校网络工程课程教师的共识，也是我们编写这本教材的主要原因。我们期待从教学需要和工程实践两个角度出发，编写一本既重视实践又兼顾原理，深度和难度相适宜的网络工程教程。

本书编写的一条主线是大量的案例、示例，兼顾网络在企业、学校、家庭等各种环境的应用，并从实践层次而非理论角度来安排，以利于统筹教学和实验。

本书的实验案例主要以锐捷网络设备为背景，其配置命令和使用方法与美国Cisco的设备基本兼容。

本书主要供高等院校网络工程专业和计算机专业高年级本专科学生使用，同时也可供计算机网络技术人员、开发人员及管理人员参考。读者一般应在学习了“计算机网络”课程后再学习本书，并动手实验，以获得计算机网络工程方面的知识和技能。

本书的编者队伍既有教学经验丰富的一线高校教师，又有长期从事工程实践的资深工程师和网络管理员。本书由鲍蓉主编，宋子强、孟凡立为副主编。参加编著的有鲍蓉（第1章）、宋子强（第1章、第3章）、孟凡立（第2章、第4章、第5章、第6章、第10章、第13章）、谢俊（第11章、第14章、第15章）、殷丽（第4章、第6章、第7章、第8章、第12章）、朱永红（第9章）。全书由鲍蓉统稿、定稿。另外，孙荣老师为本书部分图片的拍摄和处理做了许多工作，在此谨致谢意。

由于编者水平所限，书中难免存在一些疏漏之处，敬请广大读者批评指正。

编　者

2007年12月

目　　录

第1章 概　　述

1.1 系统集成与网络工程

政府、企事业单位、社会团体等机构和个人越来越多地建立了各种各样基于计算机网络平台的信息系统，因此涉及系统集成和网络工程的技术也越来越受重视。

1.1.1 计算机信息系统的结构

计算机信息系统简称信息系统。目前信息系统已经从早期的以单机为主的系统发展到基于计算机网络的系统，它可以随时为用户提供各种各样的信息，也能为用户间的直接信息交互提供支撑。一般地，信息系统可以分成多个模块，包括布线系统、网络连接、操作系统、应用服务软件、应用软件、系统管理和系统案例等。图 1-1 是信息系统的典型结构与各模块间关系的示意。

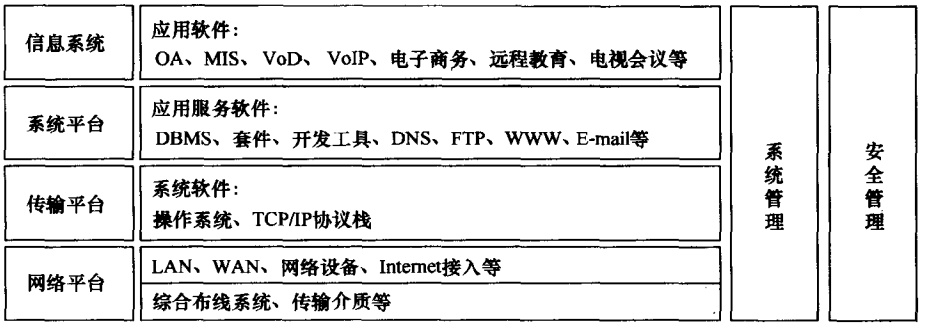

图 1-1　计算机信息系统的结构

网络平台作为信息系统的基础处于整个结构的最底层，包括综合布线和网络连接两部分，为信息系统提供通信服务。网络平台中最常用的传输介质包括双绞线、光纤、同轴电缆等，可以通过综合布线系统与各类网络设备（如交换机、路由器等）连接形成计算机网络。计算机网络可分为局域网（LAN）、城域网（MAN）、广域网（WAN）等类型。而因特网（Internet）则是全世界各种同构或异构网络互连形成的巨大网络。信息系统可以工作在某个局域网上，也可以工作在多个互连的网络上，甚至 Internet 上。

在网络平台上集成 TCP/IP 协议栈就形成了传输平台。TCP/IP 协议栈通常被包括在操作系统中。目前比较常用的有 Windows 系列（包括 2000/XP/2003/Vista 等）、Unix（如 Solaris、AIX 等）、Linux（如 Red Hat、SuSE Linux、Red Flag、FreeBSD 等）、Mac OS 等。

在传输平台上可以集成各种应用服务软件，例如基于 TCP/IP 的常规网络应用服务 DNS、FTP、WWW、E-mail 等，以及数据库管理系统（DBMS）、套件、支撑软件和开发

工具（包括程序设计语言）等。这些软件构成了系统平台。常用的 DBMS 有 Sybase、Oracle、SQL Server、DB2、Informix 等，套件则有 Lotus Notes、Exchange 等。

在系统平台上进行应用开发后形成了应用软件层，从而构成信息处理系统。常规的应用软件有办公自动化系统（OA）、管理信息系统（MIS）、辅助决策系统（DSS），以及信息发布和查询系统等。网络应用软件则包括各类网络多媒体应用（如 VoD、IP 电话、网络电视）、网络教学、电子商务等。

为了了解、维护和管理整个系统的运行，必须配置相应的软硬件进行系统管理，包括网络管理和应用管理两个部分。网络管理的对象主要是网络平台的软硬件设备，负责网络平台性能、配置和故障的管理。应用管理比较复杂，其对象是系统服务和应用服务，包括性能、配置、故障、安全和记账等 5 个方面。

安全管理日益成为人们关注的焦点。计算机信息系统内可能存放着政府、企业的机密数据或个人的隐私等，因此安全问题是不同层次用户共同关心的问题。在技术上，从底层的网络平台直到应用系统都存在安全的问题，需要配置相应的安全措施以保护重要数据的安全。这些措施包括数据加密、访问控制、身份认证、病毒防范和数据备份等。安全问题不只是技术问题，还涉及社会环境、法律、心理等方面的问题。

1.1.2 信息系统的集成

所谓集成就是把各个独立部分组合成具有全新功能的、高效和统一的整体。而系统集成（System Integration，SI）则是指在系统工程学的指导下，提出系统的解决方案，将部件或子系统综合集成，形成一个满足设计要求的自治整体的过程。系统集成是一种指导系统规划、实施的方法和策略，体现了改善系统性能的目的和手段。

网络工程领域所说的系统集成实际就是信息系统的集成，通常意味着由系统集成商向用户提供整体解决方案、整套设备和全面服务。具体来讲即是以用户的应用需要和投入资金的规模为出发点，综合应用各种计算机网络相关技术，适当选择各种软硬件设备，经过相关人员的集成设计、安装调试、应用开发等大量技术性工作和相应的管理性及商务性工作，使集成后的系统能够满足用户对实际工作的要求，并具有良好性能和适当的价格。

系统集成有以下几个显著特点：

（1）系统集成以满足用户需求为根本出发点。

（2）系统集成不是选择最好的产品的简单行为，而是要选择最适合用户的需求和投资规模的产品和技术。

（3）系统集成不是简单的设备供货，更多的是设计、调试与开发，是技术含量很高的行为。

（4）系统集成包含技术、管理和商务等各个方面，是一项综合性的系统工程。技术是系统集成工作的核心，管理和商务活动是系统集成项目成功实施的可靠保障。

（5）性价比是评价系统集成项目设计是否合理和实施成功的重要参考因素。

总而言之，系统集成的本质就是最优化的综合统筹设计，它既是一种商业行为，也是一种管理行为，更是一种技术行为。

1.1.3 网络工程

网络工程是根据用户单位的需求及具体情况，结合现代网络技术的发展水平及产品化

的程度，经过充分的需求分析和市场调研，从而确定网络建设方案，依据方案的步骤有计划实施的网络建设活动。

1. 网络工程的特点

（1）有非常明确的网络建设目标。这在工程开始之前就必须确定，在工程进行中不能轻易更改。

（2）工程有详细的规划。规划一般分为不同的层次，有的比较概括（如总体规划），有的非常具体（如实施方案）。

（3）工程要有正规的依据。例如国家标准、国际标准、军队标准、行业标准或是地方标准等。

2. 网络工程的用户需求分析

网络工程建设是一项复杂的系统工程，一般可分为网络规划和设计阶段、工程组织和实施阶段，以及系统运行维护三个阶段。

需求分析采用自顶向下的方法。经过初步调研和分析，确定建设规模、定位技术水平、预计投资总额、计划建设周期后，可具体明确如下情况：

（1）通信量：响应时间、地理布局、用户设备类型、网络服务、通信类型/通信量、容量/性能、网络现状。

（2）终端：个人计算机、主机及服务器、模拟设备。

（3）网络中心（或计算机中心）及各级设备间的位置、用户数量及其位置、任何两个用户之间的最大距离、用户群组织、特殊的需求或限制。

（4）数据库和程序共享、文件的传送和存取、用户设备之间的逻辑连接、电子邮件、网络互连、虚拟终端。

（5）通信类型：数据、视频信号、音频信号。

（6）用户要求：网络的功能、性能、运行环境、可扩充性和维护性要求。

3. 网络的总体实现目标和设计原则

（1）确定网络总体实现的目标：采用的网络技术和网络标准，分期目标、时间和进度计划等，网络实施成本、网络运行成本。

（2）总体设计原则：实用性、开放性、高可用性/可靠性、安全性、先进性、易用性、可扩展性原则。

4. 网络的拓扑结构与总体规划

影响网络拓扑结构设计与总体规划的主要因素是费用（规模）、灵活性、可靠性。

网络拓扑结构的规划设计与网络规模密切相关。一个规模较小的星型局域网没有主干网和外围网之分。规模较大的网络通常需要分层的拓扑结构。

分层设计规划的优点是可以有效地将全局通信问题分解考虑，还有助于分配和规划带宽。规模较大的网络通常可分为三层：核心层、汇聚层（分布层）、接入层（访问层）。

（1）核心层：核心交换机，高速传送数据，对数据不做任何处理。

（2）汇聚层：交换机、路由器设备，访问层的汇接点，路由数据、分割广播域/多点传送域、介质转换、安全性、远程访问的接入点。

（3）接入层：交换机、集线器设备，端接设备到网络的接入点。

5. 资源子网的规划设计

前面所述的主要是涉及通信子网的部分，资源子网设计的核心则是提供网络应用服务的服务器系统。服务器在网络中的位置直接影响网络应用的效果和网络运行效率。

服务器从服务范围看一般分为两类：

（1）为全网提供公共信息服务、文件服务和通信服务，为全网提供集中统一的数据库服务。它通常由网络中心管理维护，服务对象为网络全局，甚至是网络的外部用户，适宜放在网络中心。

（2）部门业务和网络服务结合，主要由部门管理维护、如财务部服务器等。

1.2 OSI 参考模型

计算机网络是由多台独立自治的计算机通过传输介质连接起来进行信息交换的复杂系统。互相连接和进行通信的计算机系统必须高度协调地工作，因而必须通过某种方法实现这种“协调”。计算机网络体系结构从整体角度抽象地定义计算机网络的构成及各个网络部件之间的逻辑关系和功能，通过网络协议给出协调工作的方法和必须遵守的规则。

网络发展之初，各种不同类型的网络结构不同，很难实现互连和通信。随着经济全球化的快速发展，不同网络结构的用户迫切要求能够互相交换信息，为了实现这一点，国际标准化组织（International Standard Organization，ISO）于 1977 年成立了专门机构研究该问题，并提出了一个试图使各种计算机在世界范围内互连成网的标准体系结构，即著名的开放系统互连参考模型 OSI/RM（Open Systems Interconnection Reference Model），简称 OSI。

每一种体系结构都有与之对应的参考模型，在本书中并不严格区分这两个概念。

1.2.1 OSI 的体系结构

如图 1-2 所示，OSI 把整个网络的通信工作分为 7 层：第 1～4 层是低层，与数据的传输密切相关，被认为是面向通信的；第 5～7 层是高层，包含应用程序级的数据，被认为是面向应用的。

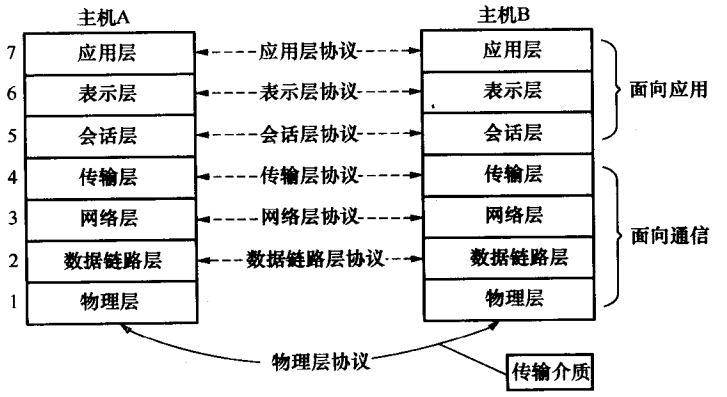

图 1-2 OSI 参考模型

在 OSI 的体系结构中，不同主机之间的相同层次称为对等层。如主机 A 的表示层和主

机B的表示层互为对等层、主机A的网络层和主机B的网络层互为对等层等。

对等层之间互相通信需要遵守一定的规则，如通信的内容、方式、时序等，这就是协议（Protocol）。

我们将某个主机上运行的某种协议的集合称为协议栈。主机正是利用这个协议栈来接收和发送数据的。

OSI参考模型通过将协议栈划分为不同的层次，从而简化问题的分析、处理过程以及网络系统设计的复杂性。

OSI参考模型的提出是为了解决不同厂商、不同结构的网络产品之间互连时遇到的互不兼容的问题，但该模型自身的复杂性阻碍了其在计算机网络领域的实际应用。事实上，工业标准的TCP/IP参考模型取代了OSI而成为目前因特网的基石。

1.2.2 OSI参考模型中各层的作用

OSI中的每一层负责一项功能、目标明确的具体工作，然后把数据向上或向下传送到相邻层。

1. *物理层*

物理层（Physical Layer）是整个OSI参考模型中的第一层，规定了激活、维持、关闭通信端点之间机械的、电气的、功能的以及过程的特性。该层为上层协议提供了一个传输数据的物理介质。在这一层，数据的单位称为比特（bit）。

属于物理层定义的典型代表包括：EIA/TIA RS-232、EIA/TIA RS-449、V.35、RJ-45等。

物理层在实际的网络工程课堂教学中经常被忽略。它实际上总是与布线、光纤、网卡和其他用于连接两个网络通信设备的东西。在实际工作中我们经常会发现网线从办公室的桌子旁或椅子边经过，有时不经意就会踢到它。事实上，由于布线不佳等原因导致的物理层故障十分常见，而排除这种故障往往需要耗费很长的时间。

需要注意的是，物理层是整个OSI的最底层，但传输介质本身并不包括在内。传输介质有时被称作体系结构的“第0层”。“网络综合布线”的课程通常更详细、系统地讲述与传输介质和物理层相关的内容。

2. *数据链路层*

数据链路层（Data Link Layer）简称链路层，是OSI模型的第二层，用以实现在不可靠的物理介质上提供可靠的传输。该层的作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错和重发等。这一层数据的单位称为帧（frame）。

数据链路层协议的代表包括：SDLC、HDLC、PPP、STP、帧中继等。

3. *网络层*

网络层（Network Layer）是OSI模型的第三层，负责对网络（或子网）间的数据包进行路由选择。此外，网络层还可以实现拥塞控制、网际互连等功能。网络层中数据的单位称为数据包（packet）。

网络层协议的代表包括：IP、IPX、RIP、OSPF等。

4. *传输层*

传输层（Transport Layer）负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的差错控制和流量控制问题。在这一层，数据的单位通

常也称为数据包（packet），但在讨论 TCP 或 UDP 等具体协议时则被称为数据段（segment）或数据报（datagram）。

传输层协议的代表包括：TCP、UDP、SPX 等。

5. 会话层

会话层（Session Layer）管理主机之间的会话进程，即负责建立、管理、终止进程之间的会话。会话层还利用在数据中插入校验点来实现数据的同步。

会话层协议的代表包括：NetBIOS、ZIP（AppleTalk 区域信息协议）等。

6. 表示层

表示层（Presentation Layer）对上层数据或信息进行变换以保证一个主机的应用层信息可以被另一个主机的应用程序理解。表示层的数据转换包括数据的加密、压缩、格式转换等。

表示层协议的代表包括：ASCII、ASN.1、JPEG、MPEG 等。

7. 应用层

应用层（Application Layer）为操作系统或网络应用程序提供访问网络服务的接口。

应用层协议的代表包括：Telnet、FTP、HTTP、SNMP 等。

OSI 模型的每一层都为其上一层提供服务以及访问接口或界面。

1.2.3 OSI 参考模型中的数据封装过程

图 1-3 描述了 OSI 参考模型中数据的封装和解封装的过程。

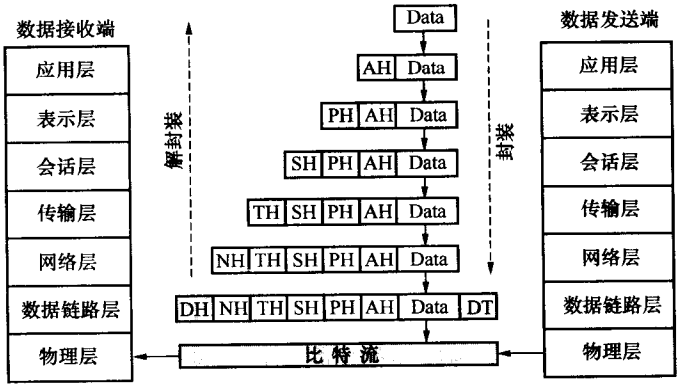

图 1-3 OSI 参考模型中的数据封装过程

1. 封装

封装发生在数据发送端。

网络中的一台主机（数据发送端）向另一台主机（数据接收端）传送用户进程的数据（Data）时，数据首先通过应用层的接口进入应用层。

在应用层，传送的数据被加上应用层的报头 AH（Application Header），形成应用层协议数据单元 PDU（Protocol Data Unit），然后按垂直方向递交到下一层——表示层。

表示层并不“关心”其上层（应用层）的数据格式而是把整个应用层递交的数据包看成是一个整体进行封装，即加上表示层的报头 PH（Presentation Header），然后再垂直向下

递交到下一层——会话层。

同样，其下的各层——会话层、传输层、网络层、数据链路层等也都要分别将上层递交下来的数据依次加上自己的报头，即：

- 会话层报头 SH（Session Header）
- 传输层报头 TH（Transport Header）
- 网络层报头 NH（Network Header）
- 数据链路层报头 DH（Data link Header）

其中，特别需要注意的是数据链路层还要给网络层递交的数据包同时再加上数据链路层报尾 DT（Data link Termination），从而形成最终的数据帧，完成了数据封装的全过程。封装完成的数据帧向下递交到物理层后就形成了比特流，并通过传输介质传送到数据传送的另一端——数据接收端。

2. 解封装

解封装发生在数据接收端。

在数据接收端，当一个数据帧通过传输介质到达该目标主机的物理层时，其物理层将把它向上递交给上层——数据链路层。数据链路层负责剥除数据帧的报头 DH 和报尾 DT，同时还要进行数据校验。如果数据没有出错，则再向上递交到上层——网络层。

同样地，沿着垂直向上的方向，网络层、传输层、会话层、表示层、应用层也要做类似的工作。最终，在剥除应用层报头 AH 后，发送端传输过来的原始数据就被完整还原，并被递交到目标主机的具体应用程序中。

这样，数据接收端就完成了一个数据包解封装的全过程。

1.3 TCP/IP 参考模型

1.3.1 TCP/IP 的体系结构

ISO 的 OSI 参考模型并没有在市场上取得成功，它太过于庞大和复杂招致了许多批评。与此同时，由技术人员自己开发的 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/网际协议）参考模型及其协议栈获得了更为广泛的应用。图 1-4 所示的是 TCP/IP 参考模型与 OSI 参考模型的对比示意图。

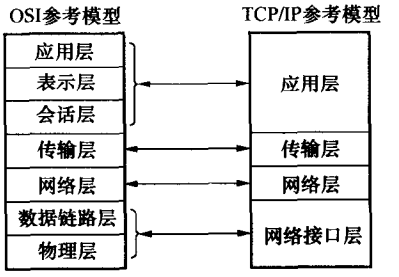

图 1-4 TCP/IP 与 OSI 参考模型结构对比

可以非常明显地发现，在 TCP/IP 参考模型中，并不存在 OSI 参考模型中的表示层和会话层，这两层的功能被合并到应用层中。同时将 OSI 参考模型中的数据链路层和物理层合并为网络接口层。这样，TCP/IP 参考模型就成为一个比较简单的 4 层体系结构，自顶向下分别为：应用层、传输层、网络层和网络接口层。由于 TCP/IP 参考模型提出时，局域网技术已比较成熟了，所以其中的网络接口层并没有进行定义，这为该体系结构提供了最大程度的灵活性，使其可以根据各种不同类型的、异构的网络而在网络接口层有不同的具体实现，或者说网

络接口层可以随不同的底层网络结构而改变。

事实上，OSI 体系结构的一大贡献就是很好地定义了物理层和数据链路层，如果将这两层纳入到 TCP/IP 体系结构的“网络接口层”，就会形成一个“新”的 5 层的 TCP/IP 体系结构，自底向上依次为：物理层、数据链路层、网络层、传输层和应用层。这更加贴切地反映了目前整个 Internet 的层次结构。

图 1-5 给出了三个参考模型的比较。从中我们可以清楚地发现不同参考模型层次间的对应关系，其中 5 层的 TCP/IP 是我们现实中最常使用的模型。目前，我们经常说的网络的“第×层”实际上都是将这个 5 层的 TCP/IP 模型按照与 OSI 层次对应的原则称呼的。这样，应用层就不被称为“第 5 层”，而是仍被称为“第 7 层”。

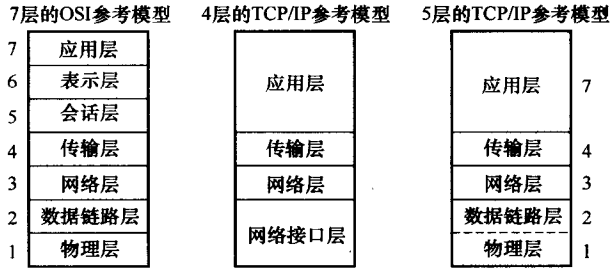

图 1-5 参考模型的比较

1.3.2 TCP/IP 参考模型中各层的作用

TCP/IP 实际上是一个协议栈的统称，或称为协议族，它包括一组协议，分布在各个层次上，而并非只是指 TCP 协议和 IP 协议。其结构类似于“沙漏”形，如图 1-6 所示。

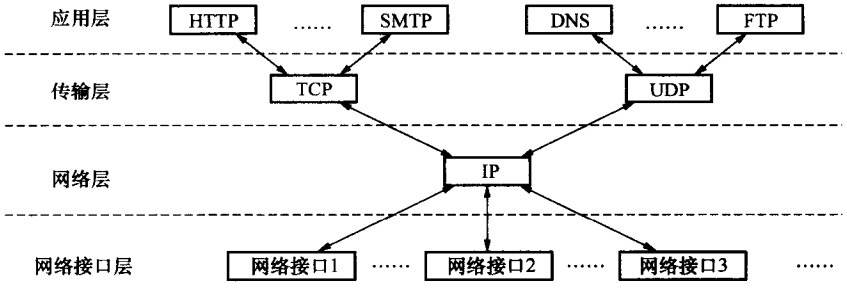

图 1-6 沙漏形的 TCP/IP 协议栈

1. 网络接口层

由于网络接口层未被定义，所以其具体实现将随着网络类型的不同而不同。只要能够向其上层——网络层提供一个访问接口，以便在其上传递 IP 分组（数据包）就可以了。

网络接口层可以分拆成物理层和数据链路层，功能与 OSI 参考模型相似。

2. 网络层

网络层也称为网际层、网络互连层等，它是整个 TCP/IP 协议栈的核心。它的功能是把分组发往目标网络或主机。同时，为了尽快地发送分组，可能需要沿不同的路径同时进行分组传递。因此，分组到达的顺序和发送的顺序可能不同，这就需要上层必须对分组进

行排序。

网络层定义了分组格式和协议，即网际协议（Internet Protocol，IP）。

网络层除了需要完成路由功能外，也可以完成将不同类型的网络（异构网）互连的任务。除此之外，网络层还需要完成拥塞控制的功能。

3. *传输层*

在 TCP/IP 模型中，传输层的功能是使源端主机和目标端主机上的对等实体可以进行会话。在传输层定义了两种服务质量不同的协议。即：TCP（Transport Control Protocol，传输控制协议）和 UDP（User Datagram Protocol，用户数据报协议）。

TCP 协议是一个面向连接的、可靠的协议。它将一台主机发出的字节流无差错地发往互连网上的其他主机。在发送端，它负责把上层传送下来的字节流分成报文段并传递给下层。在接收端，它负责把收到的报文进行重组后递交给上层。TCP 协议还要处理端到端的流量控制，以避免接收缓慢的接收方没有足够的缓冲区接收发送方发送的大量数据。

UDP 协议遵循“尽力而为”的原则，是一个不可靠的、无连接协议，主要适用于不需要对报文进行排序和流量控制的场合。

4. *应用层*

TCP/IP 模型将 OSI 参考模型中的会话层和表示层的功能合并到应用层。

应用层面向不同的网络应用引入了不同的应用层协议。其中，有基于 TCP 协议的，如文件传输协议 FTP（File Transfer Protocol）、虚拟终端协议 Telnet、超文本传输协议 HTTP（Hyper Text Transfer Protocol）；也有基于 UDP 协议的，如简单网络管理协议 SNMP（Simple Network Management Protocol）、域名解析协议 DNS（Domain Name System）等。

了解了 TCP/IP 参考模型各个层次的功能以后，我们可以大致地形成一个关于“层次”的概念地图，它描绘了 TCP/IP 参考模型各层中数据的形态、主要的技术特点，以及不同人员角色的大致分工，如图 1-7 所示。这张图有助于我们把握各种涉及网络层次的概念和关注的技术要点。

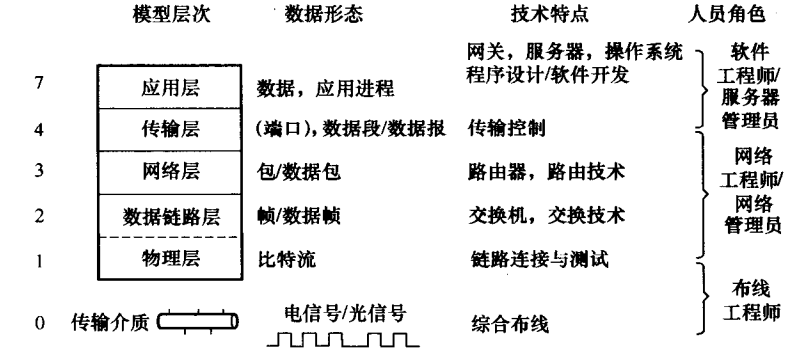

图 1-7　TCP/IP 参考模型各层次技术特点

1.3.3　TCP/IP 协议栈报文格式

一个真正的网络工程师必须熟练地掌握 TCP/IP 协议栈的报文格式，它非常有助于深入地分析一个现实的网络，以及探究在网络上究竟发生了什么。

1. IP 报文格式

IP 协议是 TCP/IP 协议族中最为核心的协议。它提供不可靠、无连接的服务，也即依赖其他层的协议进行差错控制。在局域网环境，IP 协议往往被封装在以太网帧中传送。而所有的 TCP、UDP、ICMP、IGMP 数据都被封装在 IP 数据报中传送，如图 1-8 所示。

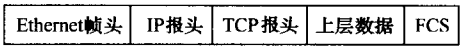

图 1-8　TCP/IP 报文封装

图 1-9 是 IP 报头格式，后面详细说明了各字段的含义。

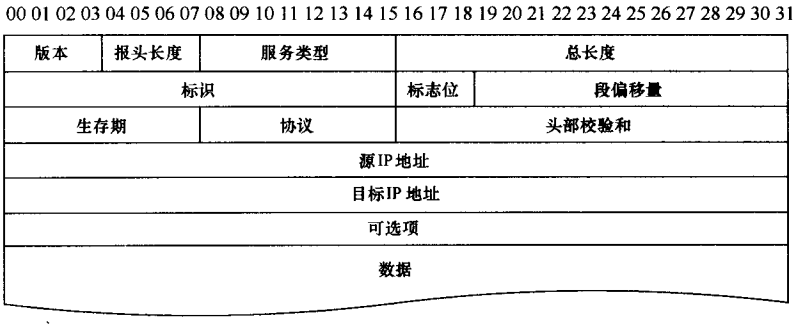

图 1-9　IP 报头格式

（1）版本（Version）字段：占 4 比特。用来表明 IP 协议实现的版本号，目前一般为 IPv4，即 0100。

（2）报头长度（Internet Header Length，IHL）字段：占 4 比特。报头长度是报头数据的长度，以 4 字节也就是 32 比特为单位。报头长度是可变的。必需的字段使用 20 字节报头，可选项字段最多有 40 个附加字节（此时报头长度为 15）。

（3）服务类型（Type of Service，TOS）字段：占 8 比特。其中前 3 比特为优先权子字段（Precedence，现已被忽略）。第 8 比特保留未用。第 4～7 比特分别代表延迟、吞吐量、可靠性和花费。当它们取值为 1 时分别代表要求最小时延、最大吞吐量、最高可靠性和最小费用。这 4 比特中同时只有 1 比特可以为 1。也可以全为 0，表示一般服务。服务类型字段声明了数据报在传输时的处理方式。例如：Telnet 协议可能要求有最小的延迟，FTP 协议（数据）可能要求有最大吞吐量，SNMP 协议可能要求有最高可靠性，NNTP（Network News Transfer Protocol，网络新闻传输协议）可能要求最小费用，而 ICMP 协议可能无特殊要求（4 比特全为 0）。实际上，大部分主机会忽略这个字段，但一些动态路由协议如 OSPF（Open Shortest Path First Protocol，开放最短路径优先协议）、IS-IS（Intermediate System to Intermediate System Protocol，内部系统间协议）可以根据这些字段的值进行路由决策。

（4）总长度：占 16 比特。指明整个数据报的长度（以字节为单位）。最大长度为 65535 字节。

（5）标识：占 16 比特。用来唯一地标识主机发送的每一份数据报。通常每发一份报文，它的值会加 1。