普通高等教育“十二五”规划教材

网络工程教程

（第二版）

鲍 蓉 主 编
谢 俊 张 慰 副主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

普通高等教育“十二五”规划

网络工程教程

（第二版）

主　编　鲍　蓉
副主编　谢　俊　张　慰
编　写　宋子强　孟凡立　徐亚峰

中国电力出版社

内 容 提 要

本书为普通高等教育“十二五”规划教材。针对本科计算机类相关专业的“网络工程”或“交换与路由”等课程教学要求，本书介绍了网络传输介质、网络互连设备、网络测试、网络应用服务器搭建、局域网和虚拟局域网技术、交换和路由技术、Internet接入、访问控制列表、NET与VPN技术等内容。全书共13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用到的命令，以便学习使用。本书的特点是紧贴当前网络工程实践，图文并茂，既重视实践又兼顾原理，深度和难度相宜。在第一版内容的基础上，根据多年教学实践和网络技术的发展，对部分内容进行了修改。增加了综合布线、网络工程实践平台和工具，以及网络工程实践方面的内容，更加强化教材的工程性和实践性。

本书主要供高等院校网络工程专业和计算机类相关专业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. —2 版. —北京：中国电力出版社，2013.8

普通高等教育“十二五”规划教材

ISBN 978-7-5123-4557-7

Ⅰ. ①网… Ⅱ. ①鲍… Ⅲ. ①计算机网络－高等学校－教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2013）第 161283 号

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）

北京市同江印刷厂印刷

各地新华书店经售

*

2008 年 2 月第一版

2013 年 8 月第二版 2013 年 8 月北京第三次印刷

787 毫米×1092 毫米 16 开本 20 印张 485 千字

定价 **36.00** 元

前　言

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。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。

本书的第一版已经在这方面做出了一些探索，也在教学过程中取得了很好的效果。基于以下原因，我们决定重新修订此教材：网络技术的发展日新月异，有的内容需要增补，有的内容需要删改；多年的教学实践使我们对网络工程领域涉及的技术有了更深入的认识和理解，适当调整章节安排能更适合教学需要；按照网络技术课程体系和教学内容分层设计的要求，网络工程教材应更着重于组网技术，减少与网络原理和网络安全课程中重复的内容；以培养学生工程技术能力为目标，增加综合布线、网络工程实践平台和工具，以及网络工程实践方面的内容，更加强化教材的工程性和实践性。

我们力图通过此次修订使教材章节结构更加合理，内容更贴近当前网络工程实践的需要。本书编写的主线是大量的案例、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，突出网络技术应用，有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思科的设备基本兼容。

读者一般应在学习了"计算机网络原理"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。

本书的编写队伍既有教学经验丰富的高校一线教师，又有长期从事网络工程实践的资深工程师和网络管理员。本书由徐州工程学院鲍蓉主编，江苏师范大学谢俊、张慰为副主编，江苏师范大学宋子强、孟凡立、徐州工程学院徐亚峰等老师参加了部分章节的编写工作。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，书中难免存在一些错漏之处，敬请广大读者批评指正。

编　者

2013 年 6 月

目　录

第1章 概 述

1.1 信息系统集成与网络工程基本概念

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。一般的，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、系统管理和安全管理等。如图 1-1 所示，是信息系统的典型结构与各模块间关系的示意图。

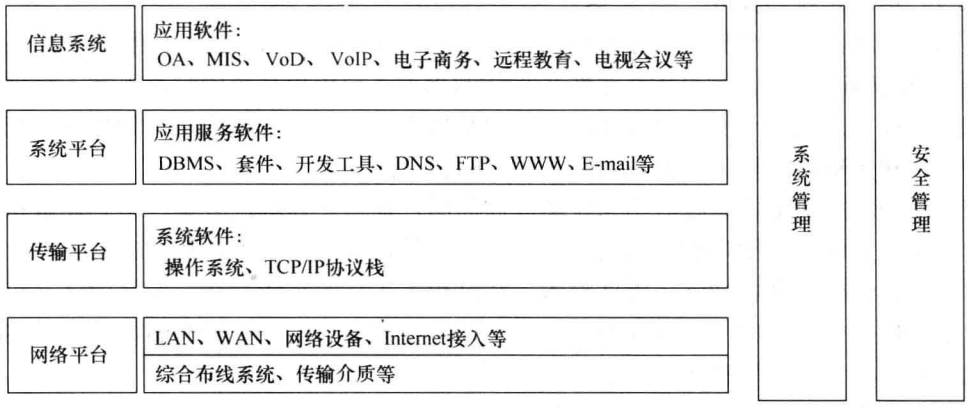

图 1-1 计算机信息系统的结构

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，甚至在 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 协议栈通常被包含在操作系统中。目前比较常用的操作系统有 Windows 系列（包括 XP、2003、WIN7、2008 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，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）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、安全和记账等五个方面。

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。

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。

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。

信息系统集成主要包括以下几个显著特点。

（1）以满足用户需求为根本出发点，选择最适合用户的需求和投资规模的产品和技术。

（2）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。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。

（3）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

网络工程是信息系统集成的重要组成部分。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。网络工程是一项复杂的系统工程，一般可分为网络规划和设计、工程组织和实施、系统运行和维护三个阶段。

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。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

需求分析是指在初步调研的基础上，确定网络建设规模、定位技术水平、预计投资总额和计划建设周期。需求分析阶段可具体明确以下情况。

（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包括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）总体设计原则包括实用性、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. 网络拓扑结构的规划设计

影响网络拓扑结构设计的主要因素是费用（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。一个规模较小的星形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核心层、汇聚层（分布层）、接入层（访问层）三层。

（1）核心层。核心交换机，高速转发数据，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 网络体系结构

计算机网络是由多台独立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”。网络体系结构从整体角度抽象、精确地定义了计算机网络及其构件所应完成的功能，通过网络协议给出协调工作的方法和必须遵守的规则。

1.2.1 OSI 的体系结构

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。

OSI 把整个网络的通信工作分为 7 层，如图 1-2 所示。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。

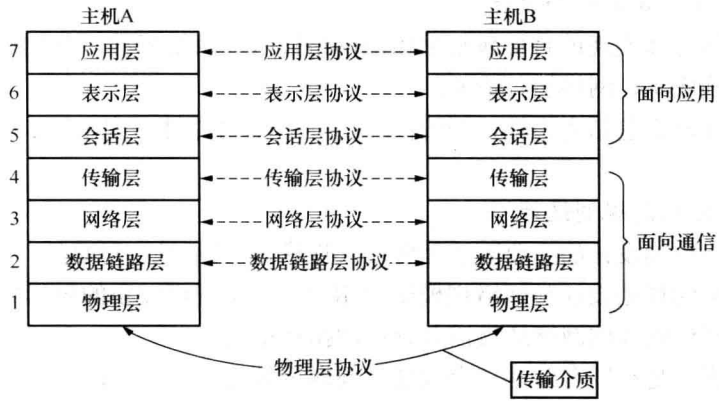

图 1-2 OSI 参考模型

OSI 参考模型将计算机网络的功能划分为不同的层次，从而简化问题的分析、处理过程及网络系统设计的复杂性。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。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）。体系结构中各层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。

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、功能的及过程的特性。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。

物理层实际上总是与传输介质、布线系统、网卡和其他用于连接两个网络通信设备的东西密切相关的。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”。

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 SSH、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及访问接口或界面。

1.2.2　TCP/IP 体系结构

事实上，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。如图 1-3 所示，是 TCP/IP 参考模型与 OSI 参考模型的对比示意图。

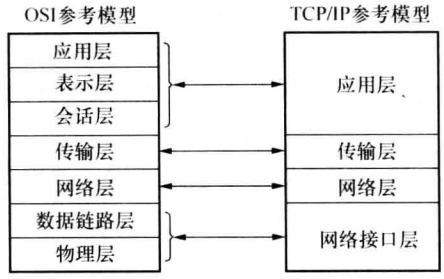

图 1-3 TCP/IP 与 OSI 参考模型结构对比

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，自上向下分别为应用层、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。

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，自下向上依次为物理层、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。

如图 1-4 所示，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“第几层”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 1-4 参考模型的比较

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 Internet 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。

TCP/IP 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 1-5 所示。

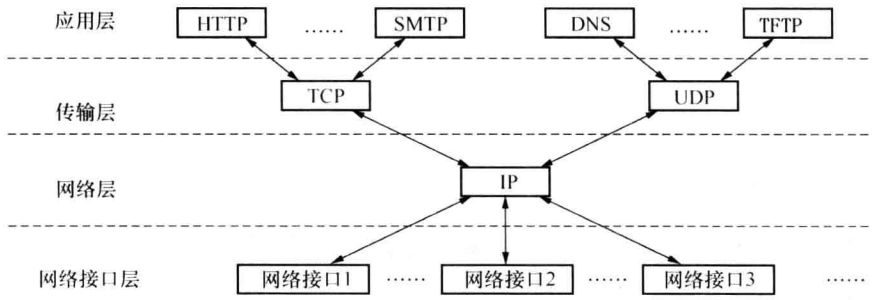

图 1-5　“沙漏”形的 TCP/IP 协议栈

通过解 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 1-6 所示。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。

1.2.3　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，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 1-7 所示。

图 1-6 TCP/IP 参考模型各层次技术特点

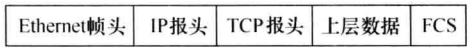

图 1-7 TCP/IP 报文封装

如图 1-8 所示，是 IPv4 报头格式，后面详细说明了各字段的含义。

图 1-8 IP 报头格式

（1）版本（Version）字段。占 4b。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 4b。报头长度是报头数据的长度，以 4B 也就是 32b 为单位。报头长度是可变的。必需的字段使用 20B 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 8b。其中前 3b 为优先权子字段（Precedence，现已被忽略）。第 8b 保留未用。第 4～7b 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 4b 中同时只有 1b 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（4b 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 16b。指明整个数据报的长度（以字节为单位）。最大长度为 65535B。

（5）标识。占 16b。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。

（6）标志位。占 3b。标志一份数据报是否要求分段。

（7）段偏移。占 13b。如果一份数据报要求分段的话，此字段指明该段偏移距原始数据报开始的位置。

（8）生存期（TTL。Time to Live）字段。占 8b。用来设置数据报最多可以经过的路由器数。由发送数据的源主机设置，通常为 32、64、128 等。每经过一个路由器，其值减 1，直到 0 时该数据报被丢弃。

（9）协议。占 8b。指明 IP 层所封装的上层协议类型，如 ICMP（1）、IGMP（2）、TCP（6）、UDP（17）等。

（10）报头校验和。占 16b。内容是根据 IP 报头计算得到的校验和码。计算方法是对报头中每个 16b 进行二进制反码求和（和 ICMP、IGMP、TCP、UDP 不同，IP 不对报头后的数据进行校验）。

（11）源 IP 地址/目标 IP 地址。各占 32b。用来标明发送 IP 数据报文的源主机地址和接收 IP 报文的目标主机地址。

（12）可选项字段。占 32b。用来定义一些任选项，如记录路径、时间戳等。这些选项很少被使用，同时并不是所有主机和路由器都支持这些选项。可选项字段的长度必须是 32b 的整数倍，如果不足，必须填充 0 以达到此长度要求。

2. TCP 报文段格式

TCP 是一种可靠的、面向连接的字节流服务。源主机在传送数据前需要先和目标主机建立连接，然后在此连接上按序收发被编号的数据段。同时，要求对每个数据段进行确认，保证了可靠性。如果在指定的时间内没有收到目标主机对所发数据段的确认，源主机将再次发送该数据段。如图 1-9 所示，为 TCP 报头结构。

图 1-9　TCP 报头结构

（1）源/目标端口号。各占 16b。TCP 协议通过使用“端口”来标识源端和目标端的应用进程。端口号可以使用 0～65535 之间的任何数字。在收到服务请求时，操作系统动态地为客户端的应用程序分配端口号。在服务器端，每种服务在“公认端口”上为用户提供服务。

（2）顺序号。占 32b。用来标识从 TCP 源端向 TCP 目标端发送的数据字节流，它表示在这个报文段中的第一个数据字节。

（3）确认号。占 32b。只有 ACK 标志为 1 时，确认号字段才有效。它包含目标端所期望收到源端的下一个数据字节。

（4）长度。占 4b。每单位为 32b。不包含可选项字段的 TCP 报头长度为 20B。TCP 扳头最多可以有 60B。

（5）标志位字段（U、A、P、R、S、F）。占 6b。各比特的含义如下。

1）URG。紧急指针有效。

2）ACK。确认序号有效。

3）PSH。接收方应该尽快将这个报文段交给应用层。

4）RST。重建连接。

5）SYN。发起一个连接。

6）FIN。释放一个连接。

（6）窗口大小。占 16b。此字段用来进行流量控制。单位为字节数，这个值是本机期望一次接收的字节数。

（7）TCP 校验和。占 16b。对整个 TCP 报文段，即 TCP 报头和 TCP 数据进行校验和计算，并由目标端进行验证。

（8）紧急指针。占 16b。它是一个偏移量，和顺序号字段中的值相加表示紧急数据最后一个字节的序号。

（9）可选项。占 32b。可能包括“窗口扩大因子”、“时间戳”等选项。

3. UDP 数据段格式

UDP 是一种不可靠的、无连接的数据报服务。源主机在传送数据前不需要和目标主机建立连接。数据被冠以源、目标端口号等 UDP 报头字段后直接发往目的主机。这时，每个数据段的可靠性依靠上层协议来保证。在传送数据较少、较小的情况下，UDP 比 TCP 更加高效。

UDP 报头结构如图 1-10 所示。

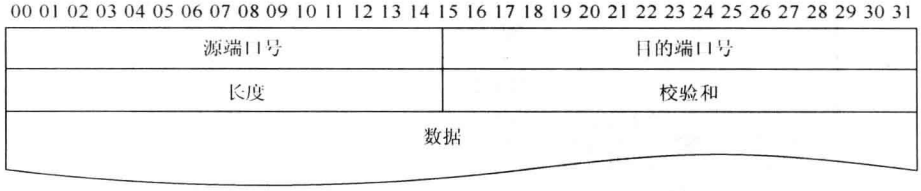

图 1-10 UDP 数据段格式

（1）源、目标端口号。各占 16b。作用与 TCP 数据段中的端口号字段相同，用来标识源端和目标端的应用进程。

（2）长度。占 16b。标明 UDP 报头和 UDP 数据的总长度字节。

（3）校验和。占 16b。用来对 UDP 报头和 UDP 数据进行校验。与 TCP 不同的是，对 UDP