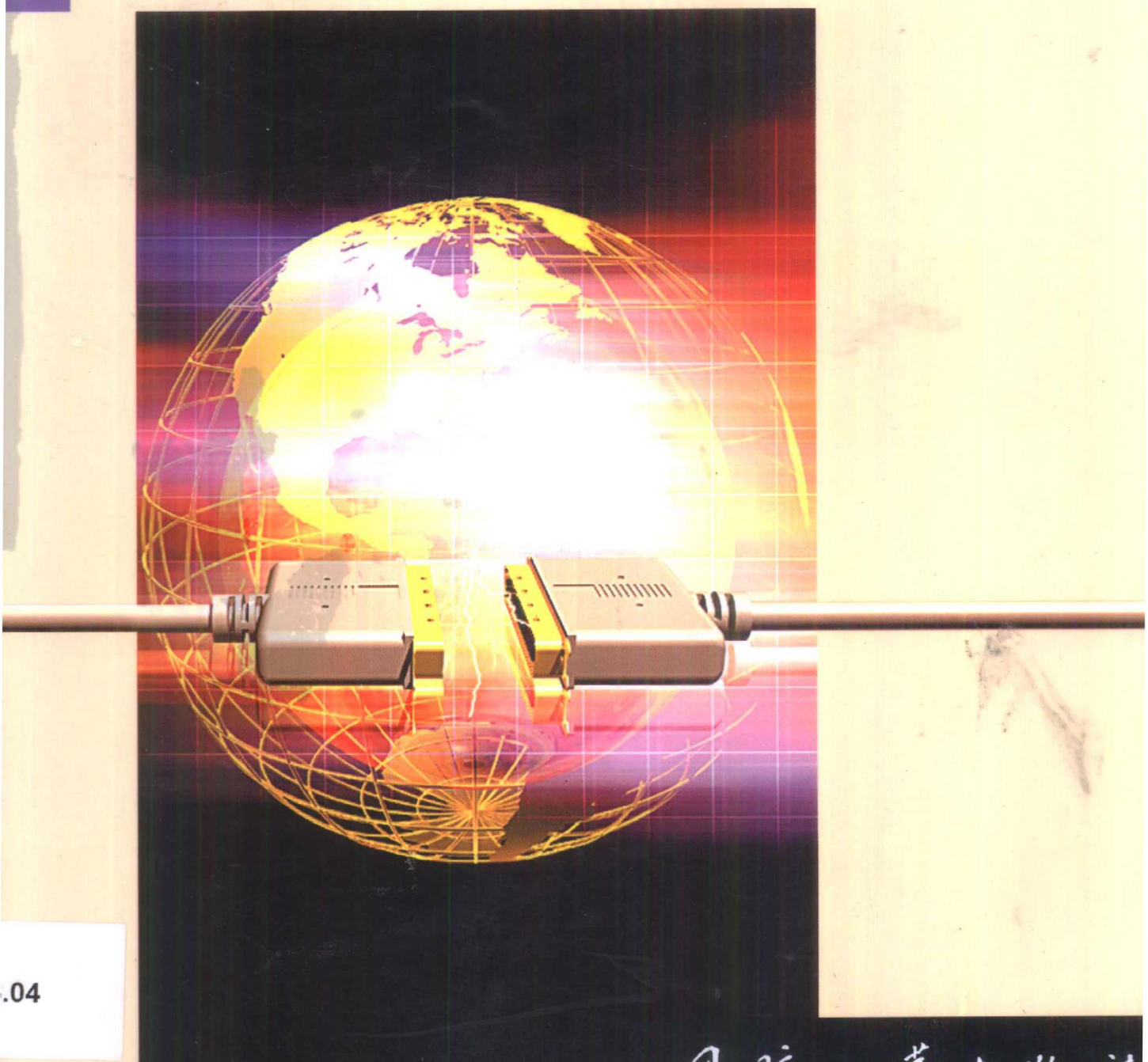
现代TCP/IP网络原理与技术

龚正虎　编著



国防工业出版社

现代 TCP/IP 网络原理与技术

龚正虎　编著

国防工业出版社

·北京·

内 容 简 介

本书是一本专门介绍 TCP/IP 网络前沿技术的书籍。全书共分八章，分别讨论计算机网络体系结构，TCP/IP 网络基础，路由技术，网络交换技术，多媒体网络技术，网络安全技术，IPv6 原理和网络应用技术。

本书内容丰富，叙述清楚，实用性强，可供从事计算机网络的科研教学人员和工程技术人员阅读参考，也可作为高等院校相关课程的教材。

图书在版编目(CIP)数据

现代 TCP/IP 网络原理与技术/龚正虎编著 .—北京：国防工业出版社，2002.9
ISBN 7-118-02862-2

Ⅰ.现… Ⅱ.龚… Ⅲ.计算机网络-通信协议
Ⅳ. TN915.04

中国版本图书馆 CIP 数据核字(2002)第 032947 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号)
(邮政编码 100044)
新艺印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 16 360 千字
2002 年 9 月第 1 版 2002 年 9 月北京第 1 次印刷
印数：1－3500 册 定价：22.00 元

前　言

在计算机网络的发展过程中，TCP/IP 网络是迄今为止对人类社会影响最重要的一种网络。TCP 和 IP 是两种网络通信协议，以这两种协议为核心协议的网络总称为 TCP/IP 网络。人们常说的国际互联网或因特网就是一种 TCP/IP 网络，大多数企业的内部网也是 TCP/IP 网络。

TCP/IP 网络经过了近 20 年的发展。早期的 TCP/IP 网络（经典 TCP/IP 网络）是一种面向科研教学的低速固定数据网络，不能满意地乘载多媒体信息，它不适合商业应用系统的运行。在不改变经典 TCP/IP 网络的基本原理和协议的前提下，完善其网络体系结构及各层协议，增加网络安全、服务质量控制、组播和移动计算能力，并引入高速网络及网络交换技术和 IPv6 协议，就形成了现代 TCP/IP 网络。TCP/IP 网络原理与相关技术以及它的发展过程反映在数千个由 IETF 公布的 RFC 文件中。

鉴于 TCP/IP 网络的重要性，出版一些使读者无需阅读大量 RFC 文件就能系统了解现代 TCP/IP 网络原理与技术的书籍是非常必要的。本书以 RFC 文件为基本参考资料，结合作者的长期科研教学实践编写而成。

第一章讨论计算机网络的体系结构、现代流行的高速局域网及广域网和计算机网络的范例。第二章系统地描述 TCP/IP 网络的基本原理。第三章讨论目前正在使用的主要路由协议以及正在发展中的组播路由技术和移动路由技术。第四章讨论组建现代 TCP/IP 网络的主要设备——网络交换机的工作原理。第五章描述了 TCP/IP 网络乘载多媒体信息要解决的若干关键技术。第六章系统地描述新一代 TCP/IP 网络（IPv6 网络）的工作原理。第七章讨论了 TCP/IP 网络的安全问题，包括密码学基础、数字签名、安全协议、密钥管理等。第八章重点描述网络管理、电子邮件、信息服务等主要网络应用系统的实现技术。本书的前两章为基础知识，对计算机网络和 TCP/IP 网络已经有初步了解的读者可以跳过这两章；后六章以深入浅出的方式系统地讲述现代 TCP/IP 网络所涉及的技术。各章有一定的独立性，读者可任意挑选自己感兴趣的章阅读。每章附有思考题，以帮助读者复习该章的主要内容，其中部分思考题需要读者参阅其它教科书或作一些研究才能找到答案。

本书既可作为大专院校本科生和研究生的教材或参考书，也可作为计算机网络工程技术人员的自学书籍。网络与通信热产生了大量口味不同的读者，虽然国内已出版了很多 TCP/IP 网络或因特网的书籍，作者相信本书的系统性、先进性和可读性能吸引很多的读者。

参加本书编写工作的有刘亚萍，可向民，彭元喜，夏建东，龚关等，最后全书由龚正虎统稿。书中如有错误，恳请读者批评指正。

目　录

第一章　计算机网络体系结构

1.1　计算机网络的定义

逻辑上，计算机网络由三大部分组成：将信息从一个地方传送到另一个地方的通信网络，借用通信网络将分布的计算机组织到一起的网络系统软件，以及建筑在网络系统软件之上的各种网络应用软件。用户通过网络应用软件使用计算机网络，实现数据传送、资源共享和分布计算三大功能。

1. 通信网络

计算机网络分为广域网（WAN，Wide Area Network）、城域网（MAN，Metropolitan Area Network）和局域网（LAN，Local Area Network）三类。广域网可以是公用电话网、分组数据网、数字数据网（DDN，Data Digital Network）、卫星通信网、无线移动通信网等。计算机网络一般不建立自己专用的广域网，而是租用电信局提供的通信网，这样可大幅度降低建网费用。城域网和局域网种类很多，它们包括以太网（Ethernet），EDDI 网，令牌环网等。局域网都是专用的，就是说人们一般不从电信部门租用局域网。计算机网络的规模可小到只有一个局域网，可大到数万个局域网。局域网可通过广域网互连起来。计算机可连在局域网上，也可连在广域网上。由于城域网和局域网的工作原理类似，它们的差别主要是覆盖范围（城域网的覆盖范围为数十千米，局域网的覆盖范围为数千米），所以人们通常将两者合称为局域网。

2. 网络系统软件

网络系统软件将多个连在网络上的计算机组织到一起进行高效而可靠的通信，它是计算机网络的核心部分。网络系统软件的主要功能包括：将多个通信网互连起来；将信息（报文）从一个网络传递到另一个网络并进行路由控制（类似于邮政总局对信件的分拣操作）；实行计算机之间端到端通信控制。网络系统软件使网络应用软件实行透明通信，就是说一个网络应用软件只要告诉网络系统软件将信息发往何处就可以，而不必关心信息是从哪个通信网络传送以及怎样传送的细节。网络系统软件在所有连网的计算机以及一部分网络互连设备（如路由器和网关）上运行。

3. 网络应用软件

网络应用软件在用户使用的计算机中运行，它直接向用户提供网络服务。这些服务可分成四类：通用类、信息服务类、分布计算类和特殊类。

（1）通用类：

- 运程登录
- 文件传输
- 电子邮件

- 网络文件系统
- 名字地址服务
- 网络管理等

(2) 信息服务类:

- Gopher 服务(信息查询)
- WWW 服务(多媒体信息查询)
- WAIS 服务(目录查询)
- WHOIS 服务(人名查询)等

(3) 分布计算类:

- 分布数据库
- 虚拟计算机
- 工作群计算等

(4) 特殊类:

- 办公自动化系统
- 电子商务系统
- 管理信息系统
- 网络教学系统等

通用类服务的应用软件一般包括在用户所购买的操作系统(如果操作系统有网络功能)中,而信息服务类和分布计算类应用软件需要单独购买。特殊类应用软件一般要针对具体要求进行一对一的开发,开发工作可在一定的网络应用程序接口上进行。一个计算机网络一旦建成,就可以运行多种应用。

在了解计算机网络的组成后,我们可以给计算机网络下这样一个定义:计算机网络是在网络系统软件和应用软件支撑下由各种通信网互连起来的独立计算机系统、终端设备以及网络专用设备的集合。计算机网络的三大功能是:数据通信、资源共享和网络计算。简单地说,计算机网络等于通信子网加资源子网。资源子网包括运行网络系统软件和应用软件的计算机(服务器和客户机)、网络终端设备和专用设备,通信子网包括局域网、广域网以及点到点专线。

关于计算机网络的定义还有其它三种说法。

第一种说法是:"计算机网络是一个计算技术与通信技术相结合并实现远程信息处理或进一步达到资源共享的系统"。这种定义强调通信技术和计算技术相结合这个侧面,就是说,通信专家建设通信子网,计算机专家建设资源子网,两者结合就形成计算机网络。这种说法强调了计算机网络的两大功能:低级分布计算(远程信息处理)和资源共享。

第二种说法是:"计算机网络是一个以能够相互共享资源的方式连接起来,并且各自具备独立功能的计算机系统的集合"。这种定义强调资源共享,强调"独立功能计算机"的概念。实际上,该说法力图将计算机网络和并行计算机系统(在并行计算机系统中各个计算机不是独立的计算机)区分开来。

第三种说法是:"存在一个能为用户自动管理资源的网络操作系统,由它来调用完成用户任务所需资源,而整个网络像一个大的计算机系统一样对用户是透明的"。这种说法强调计算机网络的高级分布计算功能。

随着计算机网络的发展,它的功能还在不断增加。传统概念上,计算机网络不执行“并行计算”,但现在,这个概念开始被打破,许多并行计算专家正在试图利用计算机网络构造大规模并行计算系统。这样,计算机网络、分布计算系统和并行计算系统之间的界限就模糊起来。另外,“数据通信”功能要理解为“多媒体通信”功能,现代计算机网络不只是传送数据,它还可传送图形、图像、声音和视频信息。

1.2 网络体系结构的模型

1.2.1 网络体系结构的作用

计算机网络是一个复杂的系统。为了将众多的网络设备组织成一个有机的整体,使之高效、安全、可靠地交换数据,必须有一个很好的模型及正确的通信协议和接口规范,必须定义明确的数据交换格式。也就是说,在建立一个实际的计算机网络之前,必须有完整且正确无误的逻辑设计。这些工作统属计算机网络体系结构(Network Architecture)的范畴。

网络层次结构模型,以及各层协议规范和接口规范的集合叫做网络体系结构。网络体系结构涉及以下几个问题。

(1) 设计网络层次结构模型。为了减少设计的复杂性,增强网络构造的灵活性,人们普遍将计算机之间的信息交换过程在功能上分成很多层。层次划分的原则是:层次少,功能明确,层次界限清晰,接口信息少。

(2) 设计各层通信协议。

(3) 设计层间接口规范。

(4) 确定信息交换格式。

研究计算机网络体系结构的原因和目的如下。

(1) 通信技术和计算机技术发展迅速,好的网络体系结构能使新技术容易纳入计算机网络,计算机网络能较快地适应于新技术发展。

(2) 计算机和计算机的操作系统种类很多,好的网络体系结构能大大减少异种机入网的复杂性。

(3) 目前,计算机网络种类很多,好的网络体系结构能大大减少网络互连的复杂性。

(4) 计算机网络的功能将越来越多,软件也将越来越复杂,好的网络体系结构能大大减少程序设计的复杂性,增加程序的模块性,因而软件的调试、修改、维护变得较容易。

(5) 网络体系结构是用户了解和开发具体计算机网络的基础。

历史上出现过很多种网络体系结构,如 DEC 公司的 DNA(Digital Network Architecture),IBM 公司的 SNA(System Network Architecture),因特网的 TCP/IP,国际标准化组织的 OSI 等。计算机公司的网络体系结构是为了发展它们自己的计算机网络提出的,不能很好地达到上述第(2)项和第(3)项的目的。有些公司的网络产品的名称和网络体系结构的名称相同,如 IBM 公司的 SNA 网,其体系结构也叫 SNA。有些公司的网络产品名和网络体系结构的名称不同,如 DEC 公司的网络产品叫 DECnet,它的体系结构叫 DNA。计算机网络的标准化工作变得日益重要,计算机网络的标准化前提就是网络体系结构的标准化。ISO 组织很早就注意到这个工作,提出开放系统互连参考模型(简称 OSI 模型),

并陆续颁布了各层通信协议和接口规范。

虽然因特网的 TCP/IP 越来越流行，并成为事实上的工业标准，但 OSI 模型仍然是设计、学习和理解计算机网络的最好模型。

1.2.2 OSI 模型简介

国际标准化组织(ISO)提出 OSI 模型的目的是：为协同已有的或将来发展的计算机网络，让人们理解不同的计算机网络系统，建立一个基本的共同的参考模型。OSI 模型不是网络设计规范，也不是网络性能评价的基准。

按照 OSI 协议标准互相交换信息的实际系统叫做开放系统。要求信息交换的应用实体可以是人，也可以是计算机内部进程(或任务、作业)，还可以是由计算机控制的物理过程。这些应用实体可在同一开放系统中，也可在不同的开放系统中。

两个应用实体交换信息的过程是一个很复杂的过程，描写、理解和设计复杂过程或系统的有效方法是：将系统或过程按功能进行层次模型化。根据各层功能明确，界限清晰，层间接口简单，层次越少越好，以及便于模块化程序设计等原则，OSI 模型将两个应用实体的信息交换过程划分为七层，它们是：物理层、数据链路层、网络层、传输层、会晤层、表示层和应用层。

上下层关系((*n*)层，(*n*+1)层)涉及很多重要的通信概念。本节不讨论各层具体内容，只讨论若干通信概念。

图 1.1 为(*n*+1)层，(*n*)层和(*n*-1)层之间的关系。处于同一层的通信实体叫同等层实体(Peer Entity)。例如图 1.1 中的 A、B、C 互为(*n*)层的同等层实体。同等层实体的通信按照一定规约实行，这些规约就构成协议。(*n*)层实体按照(*n*)层协议通信，(*n*+1)层实体按照(*n*+1)层协议通信等。除物理层之外，(*n*+1)层实体的信息交换是借助(*n*+1)层实体在(*n*)-SAP 之间提供的服务来实行的。服务访问点 SAP(Service Access Point)为上层和下层之间的接口。

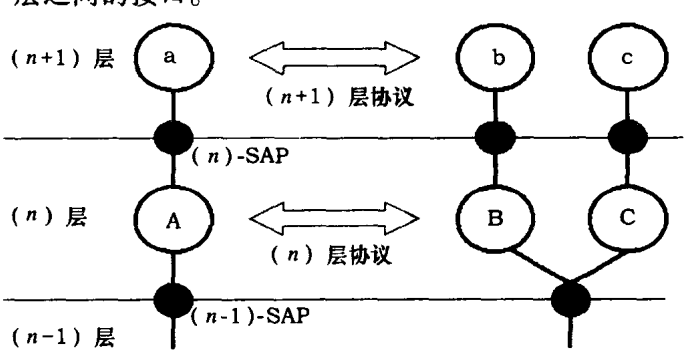


图 1.1 OSI 模型层次关系

全面理解 OSI 基本参考模型以及 ISO 颁布的各层协议，应从两方面去考虑。(*n*)层实体是怎样利用(*n*-1)层实体提供的服务交换信息的，信息交换遵循什么样的规律，这是关于(*n*)层协议规范的问题。(*n*)层实体向(*n*+1)层实体提供哪些服务，怎样接口，这是关于(*n*)层服务规范的问题。正因如此，ISO 所颁布的每一层协议都至少包括两本资料：一本是协议规范，一本是服务规范。

1.2.2.1 服务规范

1. 实体名/实体地址

每个实体都有它的名字和地址，例如图 1.2 中的 Ling 和 Wang 是两个($n+1$)层实体的名字。每个服务访问点 SAP 都有一个地址，叫做服务访问点地址，例如图 1.2 中(n)层实体 A 和 B 所对应的 SAP 的地址分别为 12345 和 67890。如果($n+1$)层实体 Ling 依附在地址为 12345 的(n) - SAP 上，那么 Ling 的地址就是 12345，如果它依附在地址为 67890 的(n) - SAP 上，那么它的地址就是 67890。因此，($n+1$)层实体的地址就是它所依附的(n) - SAP 地址。($n+1$)层有一张在($n+1$)层内是全局性的名字地址表。任何($n+1$)层实体的名字和地址的修改都会引起此表的修改。

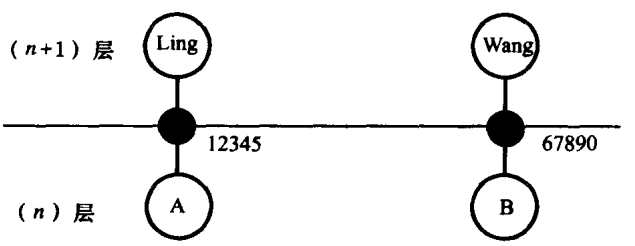


图 1.2 名字和地址

2. 有连接服务/无连接服务

图 1.2 中的 Ling 和 Wang 可利用(n)层实体提供的两类服务进行通信：有连接服务/无连接服务(Connection - oriented Mode / Connectionless Mode)。

如果(n) 层实体向($n+1$)层实体提供无连接服务，那么($n+1$)层实体之间通信过程是很简单的。例如 Ling 向 Wang 发送数据时，它只要向(n)层实体 A 发送数据传送请求即可，在请求消息中，Ling 告诉 A 发者地址，收者地址以及传输质量要求等参数。(n)层实体 A 和 B 合作将 Ling 的数据发送给 Wang。

如果(n)层实体向($n+1$)层实体提供有连接服务，那么($n+1$)层实体之间通信必须经过三个阶段：连接建立阶段、数据传送阶段、连接撤消阶段。例如图 1.2 中的 Ling 要和 Wang 通信，它必须首先向 A 发连接建立请求。请求发出之后，(n)层实体 A 和 B 合作，为 Ling 和 Wang 建立一条连接线路，并在(n) - SAP 内建立连接端点 CEP(Connection End Point)。连接端点建立之后，Ling 和 Wang 只要通过 CEP 就可传送数据。数据传送完成之后，Ling 或者 Wang 请求(n)层实体 A 或者 B 撤消连接。

3. 服务原语

(n)层实体所提供的服务用服务原语(Service Primitive)来表示，ISO 协议使用了三类不同服务原语，它们的结构如图 1.3 所示。

图 1.3(a)示出无认可式服务原语时序关系。图 1.3(b)和(a)是等价的。图 1.3(c)示出认可式服务原语时序关系。对于认可式服务原语，发出请求的($n+1$)层实体可收到同等层接收者的认可信息。图 1.3(d)示出不完全认可服务原语时序关系，IEEE 802.2 协议采用此类原语。对于不完全认可式服务原语，发出请求的一方不是从同等层接收者那里收到认可信息，而是收到从低层来的认可信息。即一个(n)层实体向($n+1$)层实体发送指示的同时也向($n+1$)层发送者发送认可。

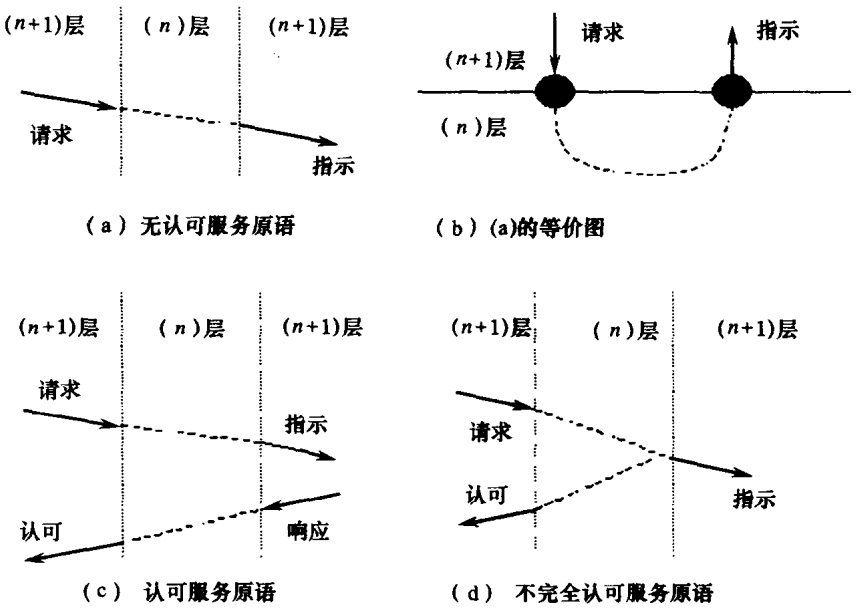


图 1.3 服务原语的结构

1.2.2.2 协议规范

1. 协议数据单元

同等层实体之间交换的信息单元叫做协议数据单元(PDU, Protocol Data Unit)。每个 PDU 可能包括两部分内容。第一部分内容为协议控制信息(PCI, Protocol Control Information),第二部分内容是上层交付下来的服务数据单元(SDU, Service Data Unit)。一个 PDU 可无 SDU。它们之间的关系如图 1.4 所示。

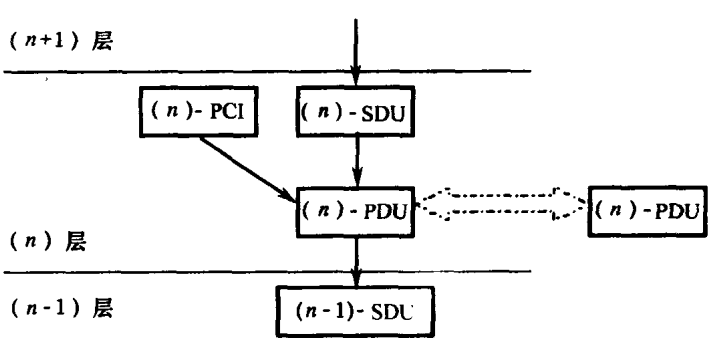


图 1.4 协议数据单元

在非 OSI 网络中,习惯上把应用层、表示层、会晤层、传输层 PDU 叫做报文(Message),网络层 PDU 叫做分组或数据报(Packet, Datagram),数据链路层 PDU 叫做帧(Frame),物理层 PDU 叫做位或比特。

2. 协议功能

OSI 模型各层的功能各不相同,包括以下内容。

1) 连接建立和撤消功能

(n)层实体应($n+1$)层的一个实体的请求,按照一定约定为($n+1$)层实体建立连接或撤消连接。

2) SDU 和 PDU 之间变换

信息发送时,(n)层实体可将多个 SDU 放在一个 PDU 中,也可以将一个 SDU 分段放在多个 PDU 中。接收时,可做相反的工作。这些功能也叫做信息的分割/装配、拼接/分离功能。

3) PDU 传送控制功能

PDU 在(n)层实体之间传送时,要进行流控制、优先级别控制和顺序控制。

4) PDU 错误处理功能

PDU 传送后可能出错,(n)层协议进行 CRC 检验、重发控制、复位处理等。

5) 路由选择功能

如果(n)层内包含多个实体,那么(n)层实体为($n+1$)层实体建立连接时,或(n)层向($n+1$)层提供无连接服务时,(n)层实体按照一定算法选择 PDU 的中继路线。

6) 同步、并发、恢复功能

OSI 的应用层可为多进程环境提供同步、并发和恢复控制功能。

7) 其它功能

例如协议选择、令牌管理、安全保密控制、编码等。

1.3 网络协议栈

1.3.1 OSI 协议栈

20 世纪 70 年代和 80 年代计算机网络百花齐放,许多计算机公司和电信公司都设计生产了自己的封闭式的计算机网络,不同厂商的计算机网络的互连成为人们关注的问题。国际标准化组织在提出开放系统互连模型(OSI 模型)的同时也为模型的各层颁布了一系列协议标准。OSI 模型及各层主要协议如图 1.5 所示。所有 OSI 各层协议的集合叫做 OSI 协议栈,执行 OSI 协议栈的网络叫做 OSI 网络。虽然世界上很少有全 OSI 网络,但它的许多协议为其它网络所用(如高级数据链路控制协议 HDLC,电子邮件协议 X.400,目录服务协议 X.500,路由协议 IS-IS 等)。由于传输层协议 TP 和网络层协议 CLNS 及 CONS 为 OSI 网络的主要协议,所以 OSI 协议栈也叫做 TP/CLNS 或 TP/CONS 协议栈。

1. 应用层

应用层处于 OSI 模型最高层,它是应用进程访问 OSI 环境的主要途径。应用层由多个服务元素组成,这些服务元素分两类。第一类为公共应用服务元素(CASE,Common Application Service Element);第二类为特殊应用服务元素。CASE 包括两个服务元素:AP(Association Protocol)和 CCR(Commitment, Concurrency and Recovery)。特殊应用服务元素也包括多个服务元素,ISO 已颁布的有:FTAM(File Transfer, Access and Manipulation),JTM(Job Transfer and Manipulation),VT(Virtual Terminal),网络管理等。这些服务元素的总和构成应用层。