全国信息化计算机应用技术资格认证指定教材

网络安全

基础教程

全国信息化计算机应用技术资格认证管理中心　组编
主编　姚华　肖琳　副主编　尹晶海　夏丽衡

- 系统安全概述
- 计算机网络安全体系
- 网络入侵初步分析
- 网络入侵的工具
- 网络安全策略
- 网络安全专题——防火墙、入侵检测、数据库加密

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

全国信息化计算机应用技术资格认证指定教材

网络安全基础教程

全国信息化计算机应用技术资格认证管理中心 组编

主 编 姚 华 肖 琳

副主编 尹晶海 夏丽衡

北京理工大学出版社

BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 提 要

本书是全国信息化计算机应用技术资格认证（CCAT）项目的指定教材，属于工程师级认证体系。CCAT资格认证项目设立的目的除了培养学生掌握相应专业的理论知识，注重学员动手能力、创新能力的训练外，还注重培养和提高学员的企业管理能力，为社会和企业培养既懂技术又懂管理的复合型人才，以改变人才培养中存在的重理论轻实践、重文凭轻能力的缺陷。

本书主要针对网络技术员的网络安全知识进行介绍，并对网络安全涉及的领域进行了详细的详解，其中，第1章详细介绍了系统安全的几个概念，第2章介绍了计算机网络安全体系，第3章对网络入侵进行初步分析，第4章介绍了网络入侵的工具，第5章主要介绍网络安全策略，第6章就网络安全进行专题的讲解。随书配有多媒体教学光盘，方便读者实际操作，让读者在最短时间内掌握最多的知识和技能。

本书可作为计算机、信息与通信等专业师生的教材，对从事计算机和信息与通信专业的技术人员有参考价值，对于网络管理人员，本书也是一本极为有用的入门指导书。

图书在版编目（CIP）数据

网络安全基础教程／姚华，肖琳主编；全国信息化计算机应用技术资格认证管理中心组编．—北京：北京理工大学出版社，2007.1（2007.6重印）

全国信息化计算机应用技术资格认证指定教材

ISBN 978－7－5640－0923－6

Ⅰ．网…　Ⅱ．①姚…②肖…③全…　Ⅲ．计算机网络－安全技术－资格考核－教材　Ⅳ．TP393.08

中国版本图书馆CIP数据核字（2007）第005723号

出版发行／北京理工大学出版社

社　　址／北京市海淀区中关村南大街5号

邮　　编／100081

电　　话／（010）68914775（办公室）68944990（批销中心）68911084（读者服务部）

网　　址／http://www.bitpress.com.cn

经　　销／全国各地新华书店

印　　刷／保定市中画美凯印刷有限公司

开　　本／787毫米×1092毫米　1/16

印　　张／17

字　　数／368千字

版　　次／2007年1月第1版　2007年6月第2次印刷

印　　数／4001～8000册　　责任校对／郑兴玉

定　　价／28.00元　　责任印制／母长新

全国信息化计算机应用技术资格认证
专家委员会名单

编 委 会

主　任		
李国杰	中国工程院	院士
	中国科学院计算技术研究所	所长
副主任		
李增泽	人事部中国高级公务员培训中心远程培训处	处长
	人事部中国国家人事人才培训网	总裁
袁开榜	全国高等学校计算机教育研究会	理事长/教授
	世界教科文卫组织	专家

执行委员会

杜建京	人事部中国高级公务员培训中心远程培训处	副处长
李大友	全国高等学校计算机教育研究会	副理事长
	北京工业大学	课程与教材建设委员会主任教授
陈蜀宇	全国高等学校计算机教育研究会网络分会	常务副理事长
	重庆大学软件学院	博导　院长/教授
丁石藤	复旦大学网络教育学院	副院长/教授
胡剑锋	江西蓝天学院	博士/院长助理
（以下按汉语拼音排序）		
丁　新	全国高等学校计算机教育研究会网络分会	副理事长
	华南师范大学网络教育学院	院长
丁晓明	西南大学计算机学院	博士　院长助理/教授
郝成义	中国人民大学网络教育学院	副院长/副教授
焦金生	《计算机教育》杂志社	主编
焦宝文	清华大学信息科学技术学院	教授
姜令嘉	山东大学网络教育学院	副院长/副教授

林亚平	湖南大学计算机学院	副院长/博导
卢先和	清华大学出版社计算机与信息分社	博士　社长
孟昭鹏	天津大学网络教育学院	硕士　副院长
冉蜀阳	四川大学网络教育学院	博士　常务副院长
盛鸿宇	教育部高职高专电子信息类教学指导委员会 北京联合大学	秘书
王晓军	北京邮电大学网络学院	副院长
徐乃庄	上海交通大学网络教育学院	副院长/教授
印　鉴	中山大学计算机科学系	副主任/副教授
张长利	东北农业大学	副校长
	东北农业大学网络教育学院	院长

秘　书

李顺福	全国高等学校计算机教育研究会网络分会	秘书长/高级工程师
杨志坚	北京理工大学出版社	社长
张文峰	北京理工大学出版社	社长助理

委　员

办公自动化应用模块委员名单

丁建民	全美测评软件系统有限公司	副总裁
丁晓明	西南大学计算机学院	博士　院长助理/教授
刘兴东	深圳职业技术学院	副院长/高级工程师
卢冠忠	华东理工大学	博导　副校长/党委副书记
马希荣	天津师范大学计算机与信息工程学院	博士　院长/教授
司银涛	北京交通大学远程继续教育学院	副院长/高级工程师
冉蜀阳	四川大学网络教育学院	博士　副院长
宋真君	辽宁交通高等专科学校计算机系	硕士　系主任
苏开荣	重庆邮电大学应用技术学院	常务副院长/副教授
吴子文	福建师范大学数学与计算机科学学院	院长/教授
谢咏才	中国农业大学网络学院	常务副院长/教授
闫洪亮	河南平顶山工学院计算机科学与工程系	副主任

张长利	东北农业大学	副校长
	东北农业大学网络教育学院	院长
何履胜	重庆电子职业技术学院	副院长/副教授
	重庆高技能人才开发协会	副理事长

多媒体与平面设计模块委员名单

丁振国	西安电子科技大学计算机应用学院	博士　副院长/教授
常建平	河南公安高等专科学校警察管理系	系主任
迟呈英	鞍山科技大学计算机学院	副院长
丁　新	华南师范大学网络教育学院	院长
符云清	重庆大学网络学院	博士　副院长/教授
龚晓阳	东华大学网络教育学院	副院长/副教授
刘希玉	山东师范大学信息管理学院	博士　院长/教授
刘正岐	陇东学院计算机科学系	主任/教授
马希荣	天津师范大学计算机与信息工程学院	博士　院长/教授
孟昭鹏	天津大学网络教育学院	副院长
苏开荣	重庆邮电大学应用技术学院	常务副院长/副教授
王世伟	中国医科大学网络中心	主任/教授
杨　涛	重庆天极信息发展有限公司	副总裁
印　鉴	中山大学计算机科学系	副主任/副教授
朱巧明	苏州大学计算机科学与技术学院	院长/教授
陈传文	南昌大学艺术设计学院	副院长
梅小清	南昌大学艺术设计学院	副主任

网络设计模块委员名单

鲍有文	北京联合大学信息学院	硕士　副院长/教授
何东建	西北农业科技大学信息工程学院	院长/教授
高占国	重庆通信学院地管部	主任/副教授
郝成义	中国人民大学网络教育学院	副院长/副教授
林亚平	湖南大学计算机学院	博导　副院长
刘革平	西南大学网络教育学院	博士　副院长/副教授
欧朝全	全国高等学校计算机教育研究会网络分会	理事
石　岗	武汉大学网络中心	博士　主任/教授

石　忠	渤海大学信息学院	硕士　院长
王世伦	四川师范大学计算机学院	副院长/副教授
王晓军	北京邮电大学网络学院	副院长
徐贯东	温州师范学院计算机科学与工程学院	博士　院长/副教授
徐乃庄	上海交通大学网络教育学院	副院长/教授
许晓艺	华南师范大学网络教育学院	副院长/高级工程师
杨　涛	重庆天极信息发展有限公司	副总裁
曾　鹏	南京邮电学院计算机系	博士　副主任
崔雅娟	北京语言大学	副教授

网络安全模块委员名单

陈庆章	浙江工业大学信息学院	党委书记/教授
丁振国	西安电子科技大学网络教育学院	博士　副院长/教授
龚晓阳	东华大学网络教育学院	副院长/副教授
何东健	西北农业科技大学信息工程学院	院长/教授
林筑英	贵州师范大学数学与计算机学院	院长/教授
刘革平	西南大学网络教育学院	博士　副院长/副教授
刘建臣	河北建筑工程学院	主任/教授
姜令嘉	山东大学网络教育学院	副院长/副教授
冉蜀阳	四川大学网络教育学院	博士　常务副院长
丘　威	广东梅州市嘉应学院计算机科学与技术系	硕士　主任
司银涛	北京交通大学远程继续教育学院	副院长/高级工程师
苏小兵	华东师范大学网络教育学院	院长助理
万常选	江西财经大学信息管理学院	博士　副院长/教授
王永书	重庆网络安全学会	常务副理事长
王振友	山东理工大学计算机学院	院长/教授
徐乃庄	上海交通大学网络教育学院	副院长/教授
张长利	东北农业大学 东北农业大学网络教育学院	副校长 院长
郑　宁	杭州电子工业学院计算机分院	院长/教授
朱巧明	苏州大学计算机科学与技术学院	院长/教授
姚　华	江西蓝天学院	副教授

总　序

努力造就数以亿计的高素质劳动者以及大批的创新人才，大力提升国家核心竞争力和综合国力，走人才强国之路，是实现中华民族伟大复兴的一项重大而紧迫的任务。

国务院《关于大力推进职业教育改革与发展的决定》和国务院办公厅转发教育部等部门《关于进一步深化普通高校毕业生就业制度改革的有关问题意见的通知》以及劳动和社会保障部、教育部、人事部《关于进一步推动职业学校实施职业资格证书制度的意见》等文件指出：应“在全社会实行学历证书、职业资格证书并重的制度，提高劳动者素质，推动就业准入制度”，“鼓励普通高校毕业生参加职业资格考核鉴定，进一步拓宽毕业生的就业渠道”。中央决定对专业技术人才的评价要由社会、行业直至企业认可，在专业技术人员中实施职业资格认证制度和执业资格制度，打破技术职务终身制，不拘一格选用人才、任用人才，走专业技术人才职业资格与国际接轨的道路，努力实现国际互认。

“全国信息化计算机应用技术资格认证（CCAT）”项目重点是培养学员的学习能力、实践能力，着力提高学员的创新能力和实际动手能力，提升学员的综合素质和就业、创业能力，特别是注重管理能力的培养和提升，改变目前教育体系普遍存在的重理论轻实践、重文凭轻能力、重技术轻管理的传统的教学模式。

“全国信息化计算机应用技术资格认证（CCAT）”考试的推行，为社会各界人士以及在校学生提供了学习最新的与国际接轨的计算机应用技能的机会，也为各类考生搭建了参加全国范围内考试的平台及获得国际性证书的机会，从而为以信息技术为核心的各行各业培养和造就符合《决定》精神的专业技术人才。该项考试一经推出，立即获得了社会的广泛认可和一致好评。

CCAT 系列教程是在全国高等学校计算机教育研究会和国际权威认证机构的指导下，按照国际通行的考试大纲、教学大纲并结合中国国情编写的，由全国信息化计算机应用技术资格认证管理中心组织各级专家、教授承担教程的编写与审定工作，由北京理工大学出版社和清华大学出版社共同出版。CCAT 系列教程不仅适用于社会各界人士以及在校学生参加“全国信息化计算机应用技术资格认证”考试的需求，同样适用于各级院校进行课程置换开展相关内容的教学工作。

加快高等教育的创新，促进高等教育、高等职业技术教育和经济社会发展紧密结合，调

整学科和专业结构，创新人才培养模式，是我们责无旁贷的历史重任。为此，我们呼吁各级高校把认证项目列入教学计划，使学生取得相应模块的认证资格，并计入学分，创立高校教育培养同人才需求结构相适应的有效机制。

全国高等学校计算机教育研究会理事长　袁开榜

前　言

为贯彻中共中央、国务院《关于进一步加强人才工作的决定》，培养高层次、高技能和复合型的社会急需人才，全国信息化计算机应用技术资格认证管理中心受人事部中国高级公务员培训中心和教育部全国高等学校计算机教育研究会的委托，组织编写了全国信息化计算机应用技术资格认证（简称“CCAT 资格认证”）项目的指定教材。CCAT 资格认证项目是全国性的 IT 培训认证项目，其主要特色是为社会培养动手能力和管理能力兼备的人才。该培训认证与在国际上享有盛誉的瑞士管理论坛（Swiss Management Forum，简称“SMF”）已实现了国际互认。本书属于 CCAT 资格认证项目中工程师级认证体系。

以 Internet 为代表的全球性信息化浪潮日益高涨，信息网络技术的应用正日益普及，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随着网络的普及，安全日益成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。面对日益严重的安全问题，我们应该如何去认识、分析和防范，是当前每一个投身于 Internet 的人所面临的一个迫切的问题，本书就是从这个目的出发，希望通过对安全问题的一些探讨和对网络入侵（黑客）技术的分析，来提高广大读者在网络及整个系统安全方面的意识。

本书在编写过程中，力求体现下列特点：

1. 一般归纳和实例并重，在较难的地方，通过图形方式直观进行解释。

2. 从网络安全方面，系统地对各个方面进行阐述，对于复杂的理论知识，进行简单化的描述，作为网络入门书籍，力求给读者一个系统的轮廓。

3. 通过详细的操作流程介绍，使读者能够一步一步地跟随作者进行学习。

4. 内容阐述循序渐进，图文并茂、条理清楚，便于自学。

5. 配有多媒体教学光盘，使读者能在最短的时间内掌握最多的知识和技能。

本书是 CCAT 资格认证指定教材，适用于社会各界人士以及在校学生参加“全国信息化计算机应用技术资格认证”考试的需求，尤其适用于高等院校、大中专学校等进行课程置换，作为相关课程的教材，亦可作为计算机职业技能考试及继续教育的培训教材或自学教材。

由于时间仓促，加之编者水平有限，书中难免有疏漏之处，恳读广大读者批评指正。

编　者

目　录

第 1 章　系统安全概述

1.1　计算机网络和网络安全

1.1.1　计算机网络发展概况

当 1969 年 12 月世界上第一个数据包交换计算机网络 ARPANET 出现时，如同世界上第一台电子计算机的诞生一样，虽然在当时人们认为这是很大的创举，但没有人预测到其深远的影响和对社会生活的剧烈改变。现在，计算机网络在现代信息社会中扮演着非常重要的角色。ARPANET 网络已经从最初的 4 个节点发展为横跨全世界 100 多个国家和地区，挂接数以万计的网络、计算机和几亿用户的 Internet，成为最大的国际性计算机互联网络，并且还在不断地快速发展。

在第一代计算机网络中，人们利用通信线路、集线器、多路复用器以及公用电话网等设备，将一台计算机与多台用户终端相连接，用户通过终端命令以交互的方式使用计算机系统，从而将单一计算机系统的各种资源分散到每个用户手中。面向终端的计算机网络系统（分时系统）的缺点是：如因各种原因导致计算机负荷较重时，系统响应时间将延长；可靠性较低，一旦计算机发生故障，将导致整个网络系统的瘫痪。在第二代计算机网络中，多台计算机通过通信子网构成一个有机整体，既分散又统一，系统性能大大提高，而且网络负载可以分散到全网的各个机器上，提高了网络响应速度和稳定性。第三代计算机网络是在各种分层模型（如 OSI 参考模型、TCP/IP 参考模型等）之上的标准化网络体系，Internet 就属于第三代网络。

1.1.2　计算机网络的功能和分类

计算机网络是指独立自治、相互连接的计算机集合。独立自治意味着每台联网的计算机是一个完整的计算机系统，可以独立运行；相互连接意味着两台计算机之间能交换信息。计算机之间的连接是物理的，由硬件实现，其介质是有线介质（如光纤）或无线介质（如微波）。计算机之间的信息交换也有物理和逻辑双重意义，在计算机网络的最底层实现的信息交换体现为两台计算机之间无结构的比特流传输；在物理层之上的信息就有了一定的逻辑结构，其交换由相关软件实现。

从功能上分析，计算机网络包括如下几个方面：数据通信、资源共享、增加可靠性和提高系统处理能力。在未来，谁拥有“信息资源”，谁就能有效地利用“信息资源”，在各种竞争中占据有利地位。随着美国“信息高速公路”计划的提出和实施，计算机网络作为信息收集、存储、传输、处理和应用的综合系统，将在信息社会中得到更广泛的应用。

计算机网络的分类标准很多，如按拓扑结构、介质访问方式、交换方式以及数据传输率等。此外还有一种可以反映网络技术本质的划分标准，即计算机网络的覆盖范围。按照这个标准，可以将计算机网络分为局域网（LAN）、城域网（MAN）和广域网（WAN）。

局域网（Local Area Network）是指范围在几百米到十几千米内的办公楼群或校园内的计算机互相连接形成的计算机网络。城域网（Metropolitan Area Network）所采用的技术和局域网基本类似，但是规模上要大一些。广域网（Wide Area Network）一般跨接很大的物理范围，通常包含很多用来运行用户应用程序的机器集合，即主机（Host）；把主机连接在一起的是通信子网（Communication Subnet），通信子网一般包括两部分——传输信道（包括传输设备）和转接设备，任务是在主机之间传送报文。由多个网络采用一定的网络互联设备连接构成的集合称为互联网（Internet）。比较通信子网、网络和互联网三者，通信子网作为广域网的一个重要组成部分，通常是由 IMP（中间转接站点）和通信线路构成的；通信子网和计算机组合构成计算机网络，互联网一般是不同网络的相互连接，如局域网和广域网的连接，两个局域网的连接或多个局域网通过广域网连接。

1.1.3 网络体系结构

为了方便两台计算机之间的通信，必须使它们采用相同的信息交换规则。把计算机网络中用于规定信息的格式以及如何发送、接收信息的一套规则称为网络协议（Network Protocol）或通信协议（Communication Protocol）。分层协议（Layering Model）是一种用于开发网络协议的设计方法，将通信问题分成若干个小问题（层次），分别设计协议。

1. 协议分层

所谓协议分层，是指按照信息的流动过程，将网络整体功能划分成一个个的功能层，不同机器上的相同功能层采用相同的协议，同一机器上的相邻功能层之间通过接口进行信息传递。为了减少网络设计的复杂性，人们往往按照功能将计算机网络划分为多个不同的功能层。网络中同等层之间的通信规则集合构成该层的协议，而同一计算机之间不同功能层之间的通信规则称为接口（Interface）。总地来说，协议是不同机器同等层之间的通信约定，接口是同一机器相邻层之间的通信约定，网络中每一层的目的是向其上层提供一定的服务。分层设计方法将整个网络通信功能划分为垂直的层次集合后，在通信过程中下层向上层隐蔽其操作细节，上层对下层的操作需求通过下层对上层提供的服务来实现。

2. 网络服务

在网络体系结构中，服务（Service）就是网络中各层向其相邻上层提供的一组操作，是相邻两层之间的界面。网络分层结构具有单向依赖关系，相邻层之间的界面也是单向的，相邻下层提供服务，其相邻上层是服务用户，服务的表现形式是原语（Primitive）。在网络中，下层向上层提供的服务有面向连接服务（Connection Oriented Service）和无连接服务（Connectionless Service）两大类。面向连接服务是电话系统服务模式的抽象。每一次完整的数据传输都必须经过建立连接、数据传输和中断连接 3 个过程。在数据传输过程中，连接起到一个输送管道的作用，发送方在一端输入数据，接收方在另一端接收数据。无连接服务是

邮政服务模式的抽象。其中每个报文都带有完整的目的地址，每个报文在系统中都独立传送。它不保证报文到达的先后次序，也不保证报文传输的可靠性。

在计算机网络中，可靠性一般通过确认和重传（Acknowledgement And Retransmission）机制来实现，大多数面向连接服务都支持确认和重传机制，但这将给传输带来额外的延迟，有些对可靠性要求不高的面向连接服务不支持确认和重传。大多数无连接服务不支持确认和重传机制，所以其可靠性往往不高。

3. ISO/OSI 参考模型和 TCP/IP 参考模型

（1）OSI

OSI 的体系结构指 7 层开放式系统互联标准（Open System Interconnection，OSI）参考模型。OSI 参考模型将原体系结构中的应用层再划分成 3 个层次，因此成为 7 个层次的体系结构。其名称从下到上排序为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

OSI 模型是基于国际标准化组织（International Standard Organization，ISO）的建议，作为各层使用国际标准化协议的第一步发展起来的。这一模型被称作 ISO OSI 开放系统互联参考模型（Open System Interconnection Reference Model），因为它是关于如何把相互开放的系统连接起来的，所以常简称为 OSI 模型。

OSI 模型有 7 层，其分层原则如下：

① 根据不同层次的抽象分层。

② 每层应当实现一个定义明确的功能。

③ 每层功能的选择应该补助于制定网络协议的国际标准。

④ 各层间边界的选择应尽量减少跨过接口的通信量。

⑤ 层数应足够多，以避免不同的功能混杂在同一层中，但也不能太多，否则体系结构会过于庞大。

值得注意的是：OSI 模型本身不是网络体系结构的全部内容，因为它并未确切地描述用于各层的协议和服务，它仅说明每层应该做什么。ISO 已经为各层制定了标准，但它们并不是参考模型的一部分，而是作为独立的国际标准公布的。

各层的主要功能简述如下：

① 物理层（Physical Layer）：负责提供和维护物理线路，并检测处理争用冲突，提供端到端错误恢复和流控制，提供为建立维护和拆除物理链路所需的机械的、电气的、功能的和规程的特性。物理层涉及通信在信道上传输的原始比特流。这里的设计主要是处理机械的、电气的和过程的接口以及物理层下的物理传输媒体等问题。

② 数据链路层（DataLink Layer）：主要任务是加强物理传输原始比特的功能。发送方把输入数据组成数据帧（Data Frame）方式（典型的帧为几百或几千字节），按顺序传送各帧，并处理接收方送回的确认帧（Acknowledgement Frame）。由于物理层仅接收和传送比特流，只能依赖各链路层来产生和识别帧边界。可以通过在帧的前面和后面附加特殊的二进制编码来达到这一目的，但必须采取特殊措施以避免这些二进制编码混淆。

同时数据链路层必须解决由于帧的破坏、丢失和重复所出现的问题。数据链路层还要向上一层（网络层）提供几类不同的服务。数据链路层要解决的另一个问题（在大多数层上也

存在）是防止高速的发送方的数据把低速的接收方“淹没”。因此需要有某种流量调节机制，使发送方知道当前接收方还有多少缓存空间。通常流量调节和出错处理是同时完成的。广播式网络在数据链路层还要处理、控制对共享信道的访问。数据链路层的一个特殊子层（媒体访问子层）就是专门处理这个问题的。

③ 网络层（Network Layer）：关系到子网的运行控制，其中一个关键问题是确定分组从源端到目的端的“路由选择”。

④ 传输层（Transport Layer）：基本功能是从会话层接收数据，必要时把它分成较小的单元传递，并确保到达对方的各段信息正确无误。这些任务都必须高效率地完成。从某种意义上讲，传输层使会话层不受硬件技术变化的影响。传输层是真正的从源到目标的“端到端”层。也就是说，源端主机上的某程序利用报文头和控制报文与目标主机上的类似程序进行对话。在传输层以下的各层中，协议是每台机器和它直接相邻的机器之间的协议，而不是最终的源机与目标机之间的协议，在它们中间可能还有多个路由器。1～3 低层是通过通信子网链接起来的，4～7 高层是“端到端”的链接。

⑤ 会话层（Session Layer）：进行高层通信控制，允许不同机器上的用户建立会话（Session）关系。会话层允许进行类似传输层的普通数据传输，并提供对某些应用有用的增强服务会话，也可用于远程登录到分时系统或在两台机器之间进行文件传递。

⑥ 表示层（Presentation Layer）：完成某些特定功能。例如，解决数据格式的转换。表示层关心的是所传输信息的语法和语义，而表示层以下各层只关心可靠地传输比特流。

⑦ 应用层（Application Layer）：提供与用户应用有关的功能，包括网络浏览、电子邮件、不同类文件系统的文件传输、虚拟终端软件、过程作业输入、目录查询和其他各种通用的及专用的功能等。

（2）TCP/IP

TCP/IP（Transmission Control Protocol/Internet Protocol）指传输控制协议/网际协议，表示 Internet 中所使用的体系结构或指整个的 TCP/IP 协议簇；网络体系起源于美国 ARPANET 工程，由它的两个主要协议即 TCP 协议和 IP 协议而得名。实际上，TCP/IP 框架包含了大量的协议和应用，是多个独立定义的协议集合，简称为 TCP/IP 协议集（簇），已成为国际互联网上与所有网络进行交流的共同“语言”，是 Internet 上使用的一组完整的标准网络连接协议。虽然 TCP/IP 不是 ISO 标准，但广泛的使用使 TCP/IP 成为一种“实际上的标准”，ISO 的 OSI 参考模型的制定参考了 TCP/IP 协议集及其分层体系结构的思想，TCP/IP 的不断发展也吸收了 OSI 和 SNA 标准中的概念及特征。

TCP/IP 从开始就考虑到多种异构网的互联问题，并将网际协议 IP 作为 TCP/IP 的重要组成部分。ISO 和 CCITT 组织最初只考虑使用一种标准的公用数据网将各种不同的系统互联在一起，后来在网络层中划分出一个子层，完成类似 TCP/IP 中 IP 的作用。TCP/IP 有较好的网络功能，一开始就将面向连接服务和无连接服务并重考虑，而 OSI 开始时只考虑面向连接服务，很晚才开始考虑制定无连接服务的有关标准。

TCP/IP 体系共有 4 个层次，实际只有 3 个层次：应用层、传输层和网络层，第 4 个层次为网络接口层，但内容很少。各层的主要功能简述如下：

① 应用层：应用层有许多著名的协议，例如，简单邮件传送协议（(SMTP)、文件传送协议（FTP）、远程登录协议（Telnet）等。

② 传输层：该层传送的数据单位是报文（Message）或数据流（Stream），可使用两种不同的协议——面向连接的运输控制协议 TCP 和无连接的用户数据报协议 UDP。

③ 网络层：主要协议是无连接的网际协议 IP。与 IP 配合使用的协议还有 Internet 控制报文协议（Internet Control Message Protocol，ICMP），Internet 组报文协议（Internet Group Message Protocol）、地址解析协议（Address Resolution Protocol，ARP）和逆向地址解析协议（Reverse Address Resolution Protocol，RARP），它们起地址翻译的作用，该层传送的数据单位是分组（Packet）。

（3）TCP/IP 与 OSI 体系结构的对照。

计算机网络是一个体系结构非常复杂而又发展迅速的系统。为了减少协议设计的复杂性，大多数网络都是按层的方式来组织的，每一层都建立在它的下层之上。不同的网络模型（比如 OSI 和 TCP/IP）其层的数量、各层的名字、内容以及功能等不尽相同。然而，在所有的网络模型中，每一层的目的都是向它的上一层提供一定的服务，并且隐藏本层的实现细节。在实际运用中，表示层和会话层作用不大，TCP/IP 参考模型中没有这两层；它的网络层只定义了网络互联所需的最低功能，即为了使得该体系结构能拥有“无缝地连接多个网络的能力”。

两种参考模型的相同点是：OSI 参考模型与 TCP/IP 参考模型都是用来解决不同计算机之间数据传输的问题。这两种模型都基于独立的协议栈的概念，采用分层的方法，每层都建立在它的下一层之上，并为它的上一层提供服务。例如，在两种参考模型中，传输层及其以下的各层都为需要通信的进程提供端到端的、与网络无关的传输服务，这些层成了传输服务的提供者；同样，在传输层以上的各层都是传输服务的用户。

两种参考模型的不同点是：① OSI 参考模型的协议比 TCP/IP 参考模型的协议更具有面向对象的特性。OSI 参考模型明确了 3 个主要概念：服务、接口和协议。这些思想和现代的面向对象的编程技术非常吻合。一个对象有一组方法，该对象外部的进程可以使用它们，这些方法的语义定义该对象提供的服务，方法的参数和结果就是对象的接口，对象内部的代码实现它的协议。当然，这些代码在该对象外部是不可见的。TCP/IP 参考模型最初没有明确区分服务、接口和协议，人们也试图改进它，使其更加接近 OSI 参考模型。从上述的比较分析可以看出，OSI 参考模型中的协议比 TCP/IP 参考模型中的协议具有更好的面向对象的特性，在技术发生变化时，由于它具有封装性和隐藏性，所以能够比较容易地进行替换和更新。TCP/IP 参考模型由于没有明确区分服务、接口和协议的概念，对于使用新技术设计新网络来说，这种参考模型就会遇到许多不利的因素。另外，TCP/IP 参考模型完全不是通用的，不适合描述该模型以外的其他协议栈。② TCP/IP 参考模型中对异构网（Heterogeneous Network）互联的处理比 OSI 参考模型更合理。TCP/IP 首先考虑的是多种异构网的互联问题，并将网际协议 IP 作为 TCP/IP 的重要组成部分。③ TCP/IP 参考模型比 OSI 参考模型更注重面向无连接的服务。TCP/IP 一开始就将面向连接服务和无连接服务并重，而 OSI 在开始时只强调面向连接服务。经过相当长的一段时间，OSI 才开始制定无连接服务的有关标准。

通过对 OSI 和 TCP/IP 两种参考模型的比较，OSI 协议似乎应该更加流行，但实际的情况并非如此。从以上两种参考模型的产生和发展的实际情况来看，由于 OSI 参考模型及其协议从一开始就太过复杂，最初的实现又大又长，并且速度较慢，因此，不利于应用和推广；与之相反，TCP/IP 参考模型的最初实现是作为 UNIX 的一部分而发布的，而且源代码是公开和免费的，使一部分大学和研究所能很快地投入使用，这反过来又推动了对有关协议及其实现