网络信息安全

刘冬梅　迟学芝　编著

中国石油大学出版社

网络信息安全

刘冬梅　迟学芝　编著

中国石油大学出版社

图书在版编目（CIP）数据

网络信息安全/刘冬梅，迟学芝编著. —东营：
中国石油大学出版社，2013.7
ISBN 978-7-5636-3998-4

Ⅰ. ①网… Ⅱ. ①刘… ②迟… Ⅲ. ①计算机网络－
安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 115187 号

书　名：网络信息安全
作　者：刘冬梅　迟学芝

责任编辑：刘玉兰（0532-86981535）

出 版 者：中国石油大学出版社（山东 东营，邮编 257061）
印 刷 者：莱芜凤城印务有限公司
电子邮箱：eyi0213@163.com
发 行 者：中国石油大学出版社（电话 0532-86981535）
开　　本：185 mm × 260 mm　印张：13.5　字数：342 千字
版　　次：2013 年 7 月第 1 版第 1 次印刷
定　　价：27.80 元

前　言

随着全球信息化的飞速发展，网络作为一种重要的信息传递手段，对于经济的发展和人们之间的交流起着越来越重要的作用。同时，网络信息面临着种种威胁，其脆弱性和安全性直接关系到国家的安全和社会的稳定。信息技术发达的国家普遍认识到，“计算机安全与计算机应用必须同步发展”，所以，网络信息安全的研究不仅受到学术界和工业界的广泛关注，也受到各国政府的普遍重视。

保护国家网络基础设施的安全、打击网络犯罪是公安机关的职责，信息化社会要求每一个公安干警必须掌握一定的信息和网络安全知识。正是在这种背景下，在山东警察学院各级领导的支持下，我们计算机教研室组织力量编著了这本《网络信息安全》，以期为我国的网络信息安全事业尽微薄之力，为公安干警学习信息和网络安全知识贡献力量。同时，该书的出版也是我们山东警察学院计算机教研室几年来在网络安全方面的研究工作的一个总结，是对我们下一步研究工作的一个促进。

全书共分 10 章。

第 1 章介绍了计算机网络的基本概念和基本知识、网络安全所面临的威胁；

第 2 章分析了操作系统的安全机制，阐述了安全操作系统的设计原则、方法，并就 UNIX、Windows 操作系统探讨了它们的一些安全漏洞；

第 3 章介绍了黑客攻击的各种方法和途径，并有针对性地提出了各种防范措施；

第 4 章介绍了计算机病毒的概念、工作原理和防治措施；

第 5 章介绍了防火墙的定义、功能、体系架构及其实现技术；

第 6 章在给出常规加密模型的基础上，对常规加密的经典技术和现代技术进行了讨论；

第 7 章介绍了入侵检测模型、入侵检测系统及常用的 Snort 入侵检测系统；

第 8 章阐述了计算机犯罪与取证的原则、方法、步骤等，介绍了常用的取证工具；

第 9 章介绍了数据备份和恢复技术，并就目前的热门技术系统容灾进行了探讨；

第 10 章介绍了信息安全风险评估的基础知识、评估标准、评估模式和评估技术。

本书题材新颖，可作为从事网络安全方面工作人士，尤其是公安干警学习网络信息安全知识的参考书，也可作为公安院校本科教材。

在本书的策划和编写中，参阅了国内外大量相关的文献和资料，得到了山东师范大学刘培玉教授的精心指导和大力帮助。本书第 1 章、第 6 章和第 9 章由张辉编著，第 2 章和第 5 章由张璇编著，第 3 章和第 4 章由刘冬梅编著，第 7 章、第 8 章和第 10

章由迟学芝编著，全书由刘冬梅、迟学芝统稿。尉永清教授对本书的规划、编著、出版起了重要作用，山东警察学院各级领导对本书的出版给予了大力支持，中国石油大学出版社给予了极大帮助，在此一并感谢。

本书内容涉及了大量前沿知识和研究领域，编者虽然极尽努力，但仍感问题难免，望各位同仁不吝赐教。

编　者

2013 年 4 月

目　录

第 1 章　网络信息安全概述

本章要点：

网络信息安全是一个综合、交叉的学科，充分利用了数学、电子、通信、计算机等诸多学科长期积累的知识和最新的发展成果。本章主要介绍了计算机网络的基础知识和网络信息安全的相关概念。学完本章，需要掌握：

- 计算机网络的概念、分类、起源与发展
- 计算机网络的基本体系结构
- 计算机网络协议
- 网络信息安全的概念、影响因素及安全模型

1.1　网络基础知识概述

1.1.1　计算机网络基础

1. 计算机网络的定义与分类

从不同的角度，以不同的观点，可以给计算机网络下不同的定义。目前，比较公认的定义是："凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路连接起来，以功能完善的网络软件实现网络中的资源共享的系统，称之为计算机网络。"

人们通常按照计算机网络辖域的不同将其分为局域网（LAN，Local Area Network）、城域网（MAN，Metropolitan Area Network）和广域网（WAN，Wide Area Network），如图 1-1~1-3 所示。局域网通信距离较短，一般为 1 ~ 20 公里，多指位于一座办公楼或一个建筑楼（如校园、企业等）范围内的计算机网络，数据传输速率较高，一般为 10 ~ 100 Mb/s，误码率较低。局域网多为一个单位所拥有，内部通信不受外界制约，当与外部交换信息时有可能受到某种形式的管理。除局域网以外的计算机网络均可称为广域网，广域网的覆盖范围很大，可以是一个地区，一个国家甚至全世界，数据传输速率较低，目前一般为 64Kb/s ~ 44 Mb/s。人们有时也把覆盖一个城市范围内的计算机网络称为城域网。

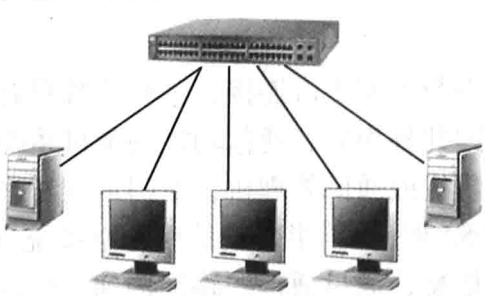

图 1-1　局域网

图 1-2　广域网

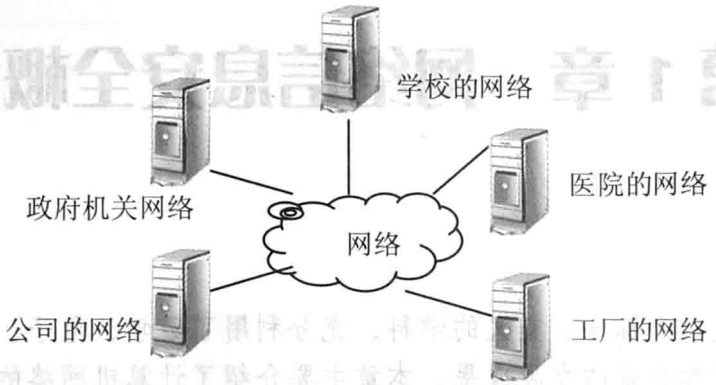

图 1-3 城域网

2. 计算机网络的功能

根据计算机网络的定义可知，网络不仅超越了地理位置，更重要的是增加了计算机本身的功能。计算机网络具有以下功能：

1）资源共享

资源共享是建立计算机网络的主要目的。接入网络的所有用户可以利用网络中的全部或部分资源，包括各种软件、硬件及数据资源。网络用户一方面节省了软件、硬件资源的开销，同时还能达到提高资源利用率，获得高经济效益的目的。有效实现共享信息资源，可以使用户及时地、不受地理位置限制地获取交流的信息，共享某台设备中的数据资源。这是计算机网络最主要的目标。

2）提高可靠性

网络中的多台计算机可互为备用，当某台设备出现故障或负担过重时，需处理的数据可以转移到其他设备中继续处理，这样能够提高整个系统的可靠性。

3）分布式处理

在计算机网络中，可以方便地实现分布式处理。根据实际工作的需要，可以将一些复杂的大型问题进行多步分解。利用网络中的多台计算机进行分布式处理也可以将多部门、多单位或多行业的各台计算机的数据集中起来进行高性能计算机处理，这使得网络中的信息处理达到灵活高效的目的。

计算机网络的功能与作用繁多，除传统基本功能外，多种新型业务功能与作用也会层出不穷，但总的来说，随着信息科学技术的不断发展，计算机网络的功能将向着高速化、多元化、可视化和智能化的方向发展。

3. 计算机网络的发展阶段

计算机网络从出现到现在，经历了由简单到复杂、由初级到高级的发展过程，大体划分为 4 个阶段。

1）远程终端联机阶段

20 世纪 50 年代，人们利用通信线路将远程终端与大型主机连接，远程终端只有输入输出功能，数据处理工作是利用主机的资源完成的，因此称为具有通信功能的单机系统。为了提高主机的工作效率，在主机之前配备一台前置处理机或通信处理机，专门负责与终端的通信控制，从而使主机有更多的时间进行数据处理。1952 年，美国半自动地面防空系统（CAGE）的科研人员首次研究把远程雷达或其他测量设备的信息，通过通信线路汇接到一台计算机上进行集中处理和控制。60 年代初，美国航空公司与 IBM 联手研究并首先建成了由一台计算机遍布全美 2 000 多个终端组成的美国航空订票（SABRE-1）。这种具有通信功能的客机系统

构成了计算机网络的雏形。

2）计算机网络阶段

为了共享各个联机系统的资源，利用通信线路将若干联机系统中的大型主机连接起来，就构成了计算机网络。1969 年 9 月，美国国防部高级研究计划所和十几个计算机中心一起，研制出了 ARPA 网，将若干大学、科研机构和公司的多台计算机连接起来，实现资源共享。ARPAnet 从逻辑上把数据处理和数据通信分开，通过数据处理网（资源子网）和数据通信网（通信子网）组成两级网络结构。从此以后，计算机网络取得较大的发展，特别是主要由微型机组成的局域网的出现更促进了网络的普及，以后又发展成许多城域网和广域网。

3）计算机网络互连阶段

20 世纪 70 年代末至 90 年代的计算机网络互连阶段是具有统一的网络体系结构并遵循国际标准的开放式和标准化的网络，最有代表性的是因特网（Internet）。ARPA 网兴起后，计算机网络发展迅猛，各大计算机公司相继推出自己的网络体系结构及实现这些结构的软硬件产品。由于没有统一的标准，不同厂商的产品之间互连很困难，人们迫切需要一种开放性的标准化实用网络环境，这样应运而生了两种国际通用的重要的体系结构，即国际标准化组织的 OSI 体系结构和 TCP/IP 体系结构。

4）信息高速公路阶段

信息高速公路是由通信网络、计算机、数据库以及日用电子产品组成的一个完备网络体系。它把多个国家乃至全世界的计算机资源、家用电子设备、广播电视系统等通过高速通信网连接起来，实现信息资源共享，极大地提高了经济发展速度、社会信息化水平和人民的生活水平。

4. 计算机网络的组成

计算机网络主要由网络主机、通信处理机、终端、联网部件和通讯介质等组成。

1）主机（Host）

主机是资源子网的主要设备，可包括巨型机、数据流机、并行机、向量机等。在局域网中，主机可泛指服务器、网络打印机、绘图仪等资源主设备。

2）通信处理机

通信处理机也称前端机，主要用于对各主机之间的通信进行控制和处理，由通信处理机组成的网络可称为通信子网。主机是网络资源的拥有者，组成网络的资源子网。通信子网为资源子网提供信息传送服务，是支持资源子网上用户之间相互通信的基本环境。主机通过处理机接入通信子网，主机与通信处理机之间可采用高性能并行接口（HIPPI，High Performance Parallel Interface）连接。在局域网中，通信处理机的功能一般可由网卡的通信控制器来承担。

3）终端

终端是用户访问网络的连接界面。终端可作为主机的配置与主机相连接的网络软件来访问网络，并与其他用户进行交互。根据不同的应用环境，终端可分为图形、文字处理、图像、CAD/CAM 等常规终端和智能终端。

4）联网部件

除上述通信处理机或网卡外，联网部件还包括：调制解调器（Modem）；集线器（Hub），如 ATM 交换机（AMT Switch）；IBM 8260 多协议智能交换集线器（Multi-Protocol Intelligent Switch Hub）交换机；FAX 卡；外收发器（Transceiver）等。在网络环境中，其网络互联部件还包括中继器（Repeater）、网关（Gateway）、网桥（Bridge）、路由器（Router）等。

5）通讯介质

通信介质可包括：硬缆，即同轴电缆、双绞线、光纤等；软缆，即微波、无线电、激光、红外、卫星信道等。

5. 网络的拓扑结构

拓扑学是几何学的一个分支，是研究不同大小、形状的线和面的特性的学科。计算机网络的拓扑结构是指网络中节点和链路的几何排序，它是影响网络性能和费用的重要环节。利用网络的拓扑结构，可研究网络的链路比价、最短路径、网络的重构、容错及最优结构等性能。在实际建网中，计算机网络的拓扑结构应根据实际应用环境的需求综合考虑，进行合理设计。考虑的技术因素包括：应用环境的物理区域及应用对象的几何布局；应用环境的管理控制级别和层次；应用对象的相关性和它们之间交互的频率；可靠性、容错性、重构性及其安全性；路由选择因素；传输介质信道访问控制协议等。

局域网的物理拓扑结构决定了局域网的工作原理和数据传输方法。目前，局域网的物理拓扑结构主要有总线型、环形、星形和树形四种形式。

总线型拓扑结构指各工作站和服务器均挂在一条总线上，各工作站地位平等，无中心节点控制，公用总线上的信息多以基带形式串行传递，其传递方向总是从发送信息的节点开始向两端扩散，如同广播电台发射的信息一样，因此又称为广播式计算机网络，如图 1-4 所示。

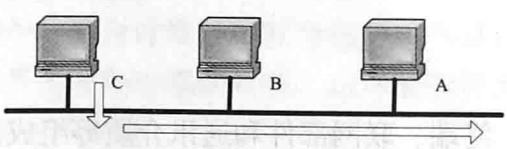

图 1-4　总线型拓扑结构

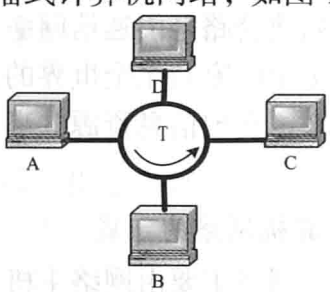

图 1-5　环形拓扑结构

环形结构由网络中若干节点通过点到点的链路首尾相连形成一个闭合的环，这种结构使公共传输电缆组成环形连接，数据在环路中沿着一个方向在各个节点间传输，信息从一个节点传到另一个节点。环形结构的网络信息是单向传送的，与双向传送相比，它不会由于两帧数据相对发送而造成丢失。这种结构布局简单，成本低，但如果一个设备发生故障，将导致整个网络不能正常工作，如图 1-5 所示。

星形结构是指各工作站以星形方式连接成网。网络有中央节点，其他节点（工作站、服务器）都与中央节点直接相连。这种结构以中央节点为中心，因此又称为集中式网络，如图 1-6 所示。

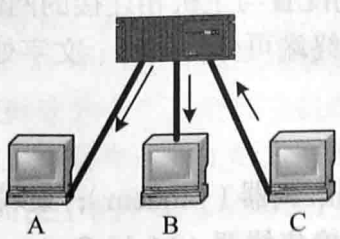

图 1-6　星形拓扑结构

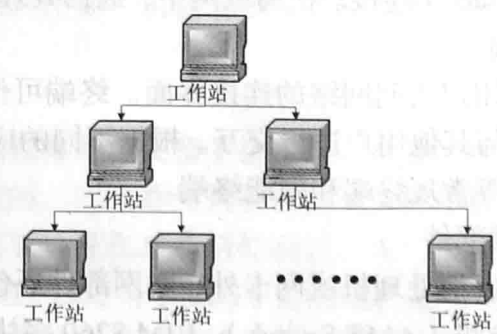

图 1-7　树形拓扑结构

树形结构是总线型结构的扩展，它是在总线网上加上分支形成的。其传输介质可有多条分支，但不形成闭合回路，如图 1-7 所示。

1.1.2　计算机网络协议

计算机网络中各台主机的类型和规格可能不同，每台主机使用的操作系统也可能不同，因此，为使计算机网络能正常运行，就必须有一套网络中各节点共同遵守的规程，这就是网络协议。网络协议是一组关于数据传输、输入输出格式和控制的规约，有了这些规约就可在物理线路的基础上，构成逻辑上的连接，实现在网络中的计算机、终端及其他设备之间直接进行数据交换。开放系统互连参考模型（OSI/RM）和 TCP/IP 是最为重要的两个计算机网络互连的模型体系。

1. 开放系统互连参考模型（OSI/RM）

1978 年，国际标准化组织（ISO）提出了著名的开放系统互连参考模型（OSI），将网络中的通信管理程序与其他程序分开，并按照数据在网络中传输的过程将通信管理程序分为 7 个层次的模块，从下往上依次为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。其中，各层都有相对独立的明确的功能，上一层的功能依赖于下一层的服务，相邻的上下两层间通过界面接口通信。OSI 参考模型的分层协议及网络中任意两个端点间的通信过程如图 1-8 所示。

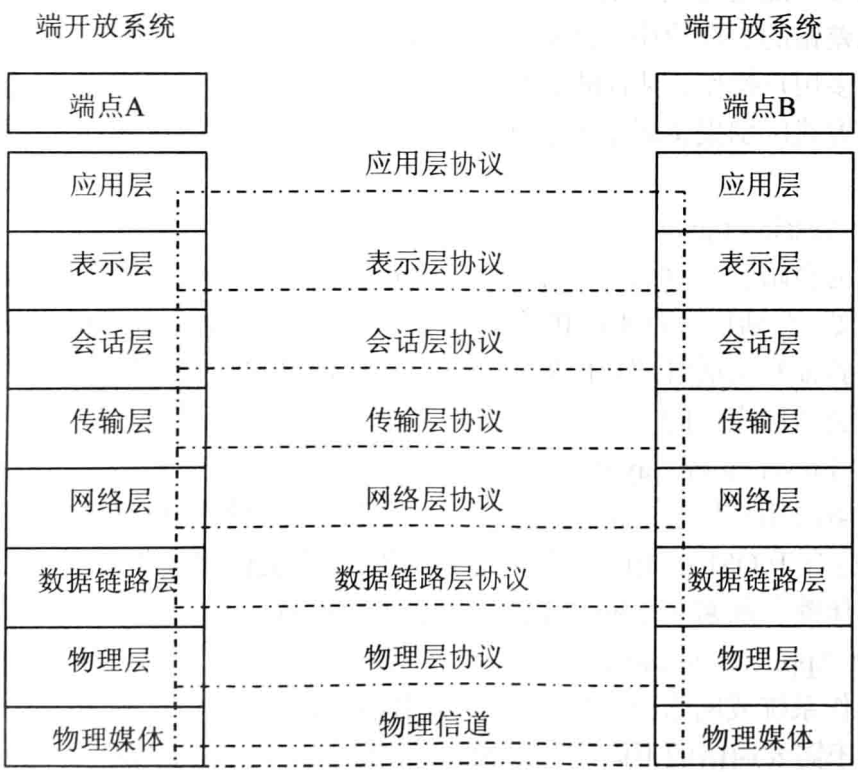

图 1-8　OSI 分层协议

1）物理层（Physical Layer）

物理层位于 OSI 参考模型的最底层，功能是传送比特流，它从第二层数据链路层接收数据帧，并将帧的结构和内容串行发送，即每次发送一个比特。物理层与电信号技术和光信号技术的物理特征相关，只能传递 0 和 1 数据。这些特征包括用于传输信号电流的电压、介质类型及阻抗特性。该层的传输介质是同轴电缆、光缆、双绞线等。物理层可能受到的安全威胁是搭线窃听和监听。可以利用数据加密、数据标签加密、数据标签、流量填充等方法保护物理层的安全。

2）数据链路层（Data Link Layer）

数据链路层位于OSI参考模型的第二层，不仅负责发送和接收数据，还要提供数据有效传输的端到端连接。在发送方，数据链路层负责将数据与指令等信息包到帧中。数据帧是该层的基本结构：帧中包含足够的信息，确保数据可以安全地通过本地局域网到达目的地。为保证数据传送能够完整安全地到达，应做到两点：在帧完整无缺地被目标节点收到时，源节点必须收到一个响应；在目标节点发出收到帧的响应之前，必须能够验证帧内容的完整性。

数据链路层负责检测并修正有可能导致帧的发送不能到达目标或者在传输过程中被破坏的情形。不管是局域网还是广域网，任何类型的通信都要求第一层和第二层的参与。

3）网络层（Network Layer）

在计算机网络中进行通信的两个计算机之间可能会经过很多个数据链路，也可能还要经过很多通信子网。网络层的任务就是选择合适的网间路由和交换节点，确保数据及时传送。网络层将数据链路层提供的帧组成数据包，包中封装有网络层包头，其中含有逻辑地址信息——源站点和目的站点地址的网络地址。在这一层，数据的单位称为数据包（packet）。地址解析和路由选择是网络层的重要功能，还可以实现拥塞控制、网际互连等。

4）传输层（Transport Layer）

传输层的主要功能是完成网络中不同主机上的用户进程之间可靠的数据通信。最好的传输连接是一条无差错的、按顺序传送数据的管道，即传输层连接是真正端到端的。由于绝大多数主机都支持多用户操作，因而机器上有多道程序，这意味着多条连接将进出于这些主机，因此需要以某种方式区别报文属于哪条连接。识别这些连接的信息可以放入传输层的报文头中。

5）会话层（Session Layer）

会话层也称为会晤层或对话层。在会话层及以上的高层次中，数据传送的单位不再另外命名，统称为报文。会话层允许不同机器上的用户之间建立会话关系，但不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制。例如，服务器验证用户登录便是由会话层完成的。

6）表示层（Presentation Layer）

表示层主要解决用户信息的语法表示问题。它将准备交换的数据从适合于某一用户的抽象语法，转换为适合于OSI系统内部使用的传送语法，即提供格式化的表示和转换数据服务。数据的压缩和解压缩、加密和解密等工作都由表示层负责。

7）应用层（Application Layer）

应用层为操作系统或网络应用程序提供访问网络服务的接口。应用层包含大量人们普遍需要的协议，对于需要通信的不同应用来说，应用层的协议都是必需的。例如，PC机用户使用仿真终端软件通过网络仿真某个远程主机的终端，并使用该远程主机的资源。这个仿真终端程序使用虚拟终端协议将键盘输入的数据传送到主机的操作系统，并接收显示于屏幕的数据。

由于每个应用有不同的要求，应用层的协议集在OSI模型中并没有定义，但是，有许多确定的应用层协议，比如虚拟终端、文件传输和电子邮件等都可以作为标准化的候选。

OSI/RM参考模型是目前国际上数据网的公认标准，但它仅仅是一个框架，并未在每一层都限定统一的一种协议，更没有给出协议的具体实现。在通信领域，制定标准的组织机构很多，最具权威性的机构除ISO外，还有IEEE（电气电子工程师学会，美国）802委员会、CCITT（国际电话电报咨询委员会）等，它们也制定了一些国际通用的标准，并已得到了广

泛应用。IEEE 802 委员会制定的 IEEE 802.1-IEEE 802.8 标准对局域网的发展起到了重要作用。CCITT 制定的 x.25 也是一个重要的通信协议，它实现了 ISO 模型的下面三层（物理层、数据链路层和网络层），可用于广域网。EIA（电子工业协会，美国）制定的 RS-232-C 标准应用也十分广泛，它提供了物理层二进制数据串行通信的标准接口。

2. TCP/IP

TCP/IP 也是一个开放模型，与 OSI 参考模型相比，其结构更为简单。在现实网络世界里，TCP/IP 获得了更为广泛的应用，是事实上的计算机网络互连标准。目前，每一个重要的操作系统都支持 TCP/IP 进行网络通信，并且随着 TCP/IP 的广泛使用，许多依赖专有协议的网络操作系统也开始使用 TCP/IP。

1）TCP/IP 协议模型

与其他网络协议一样，TCP/IP 有自己的参考模型用于描述各层的功能。TCP/IP 参考模型实现了 OSI 模型中的所有功能。不同之处是 TCP/IP 协议模型将 OSI 模型的部分层进行了合并，OSI 模型对层的划分更精确，而 TCP/IP 模型使用比较宽的层定义。TCP/IP 协议族的 4 层、OSI 参考模型和常用协议的对应关系如图 1-9 所示。

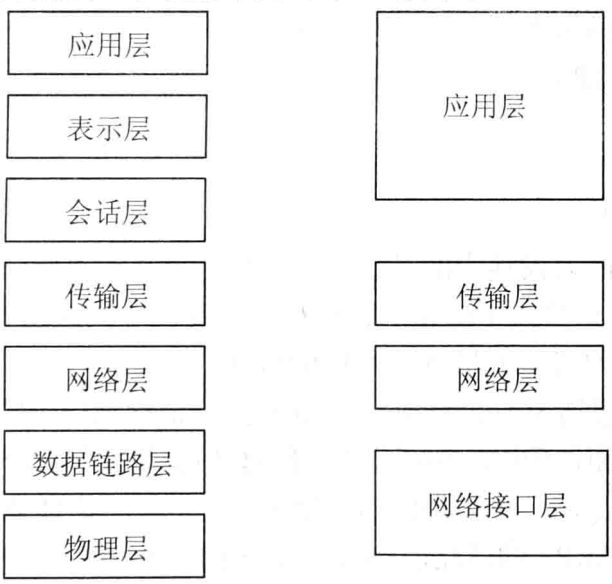

图 1-9　OSI 参考模型和 TCP/IP 的层次对应关系

TCP/IP 协议族包括 4 个功能层：网络接口层、网络层、传输层和应用层。这四层概括了 OSI 参考模型中的 7 层。

（1）网络接口层：

网络接口层协议实现了网络中相邻设备之间的互连，也称为数据链路层，它定义了各种介质的物理连接特性以及数据在不同介质上的信息帧格式。网络接口层涵盖了各种物理介质层网络技术，可以支持以太网、令牌环、ATM（Asynchronous Transfer Mode）、FDDI（Fiber Distributed Data Interface）、帧中继等数据链路技术。TCP/IP 模型中的网络接口层结合了 OSI 模型中物理层和数据链路层的功能。

（2）网络层（Internet 层）：

网络层由在两个主机之间通信所必需的协议和过程组成，这意味着数据报文必须是可路由的。网络层支持路由和路由管理功能，这些功能由外部对等协议提供，称这些协议为路由协议。这些协议包括内部网关协议（Interior Gateway Protocol，IGP）、外部网关协议（External Gateway Protocol，EGP）。实际上，许多路由协议能够在多路由协议地址结构中发现、计算