HZ BOOKS
华章教育

网络空间安全学科规划教材

网络协议分析

Network Protocol Analysis

寇晓蕤 蔡延荣 张连成◎编著

机械工业出版社
China Machine Press

网络空间安全学科规划教材

网络协议分析

Network Protocol Analysis

第2版

寇晓蕤 蔡延荣 张连成◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络协议分析 / 寇晓蕤，蔡延荣，张连成编著 . —2 版 . —北京：机械工业出版社，2017.9
（网络空间安全学科规划教材）

ISBN 978-7-111-57614-3

I. 网… II. ①寇… ②蔡… ③张… III. 通信协议 - 教材 IV. TN915.04

中国版本图书馆 CIP 数据核字（2017）第 190084 号

本书以 TCP/IP 协议族中构建 Internet 所必需的、与我们交互最直观的协议作为主题，详细讨论了 TCP/IP 的体系结构和基本概念。书中涉及的主要协议包括 PPP、ARP、RARP、IP、ICMP、UDP、TCP、NAT、RIP、OSPF、BGP、IGMP、BOOTP、DHCP、DNS、SNMP、HTTP、MIME、POP、IMAP、FTP、NVT、Whois、NTP 等。

本书可作为高等院校计算机、网络工程、通信工程、信息安全等专业本科生与研究生“网络协议分析”课程的教材，也可作为相关领域工程技术人员的参考用书。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：迟振春　　责任校对：李秋荣
印　　刷：北京瑞德印刷有限公司　　版　　次：2018 年 9 月第 2 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：21
书　　号：ISBN 978-7-111-57614-3　　定　　价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

第 2 版前言

本书第 1 版自 2009 年面世以来，深受读者喜爱，被多所院校选作教材。在阅读和使用本书的过程中，许多读者提出了非常宝贵的意见和建议。

网络技术更新换代极快，尽管网络协议本身的架构和基本内容相对稳定，但是随着网络新技术的不断出现，网络协议也在不断进行更新。2013 年，机械工业出版社朱劼编辑就从把握协议新发展的角度提出编写第 2 版的建议，并与编者进行了多次沟通。2014 年，我们启动了本书第 2 版的编写工作，参阅了大量的最新文献，特别是 IETF 的 RFC 原文，在系统梳理脉络和深入研读之后，再把最新进展融入本书。这项工作十分艰巨，历时 3 年，更新版终于完成。虽然内容相比第 1 版没有颠覆性的变化，但更新部分花费的心血并不比第 1 版少。

相比第 1 版，本书的主要变化有：

第 1 章　TCP/IP 概述。基于 Modem 拨号的远程接入技术早已废弃不用，而现在用户更常使用的是无线上网，所以在引入网络互联的原理时，将 Wi-Fi 技术作为实例。此外，对 TCP/IP 的标准化进程和互联网在我国的发展历程进行了系统梳理，以便给读者一个全面而准确的认识。

第 2 章　点到点协议 PPP。用于 64K 电话线路接入互联网的 PPP 早已退出历史舞台，但基于 PPP 思想的 PPPoE 等新技术的应用极为广泛。本次修订，特别加强了 PPPoE 的相关内容。

第 3 章 Internet 地址及地址解析。针对 IP 地址分配管理出现的新变化，我们相应地进行了更新。此外，在 ARP 部分，根据 RFC 标准给出了用 ARP 检测 IP 地址冲突等应用，以及它的新进展。

第 4 章　互联网协议 IP。IP 是 TCP/IP 协议族的“咽喉”，其体系结构及报文格式等变化不大，但其首部的 ID 字段、选项等有一些新变化，我们对此进行了更新。同时梳理了 IP 的发展变化历程，增加了安全相关的内容。

第 5 章　Internet 控制报文协议 ICMP。ICMP 的变化相对较大，我们梳理了其新发展，对内容进行了重组，淘汰了过时的功能，增加了新功能的描述。

第 6 章　用户数据报协议 UDP。UDP 协议本身变化不大，主要增加了安全相关的内容。

第 7 章　传输控制协议 TCP。TCP 协议本身十分复杂，我们对 TCP 报文中 ISN 的选取、MSS 协商、报文选项等内容进行了更新，对端口号进行了重新梳理，对快速重传和快速恢复算法进行了更为细致的描述，同时增加了安全相关的内容，并对读者系统研究协议给出了 RFC 文档导览建议。

第 8 章　Internet 地址扩展技术。增加了匿名的点到点链路技术、NAT 与 ICMP 的交互等新内容，同时对 NAT 穿越进行了重新描述。

第 9 章　路由协议概述。主要增加了 AS 新进展的介绍。

第 10 章　选路信息协议 RIP。增加了认证、RIPng 等新内容。

第 11 章　开放式最短路径优先 OSPF。增加了认证、隐藏完全传输网络、TTZ 等新内容。

第 12 章　边界网关协议 BGP。为了让读者对互联网的整个路由体系有更为深入的认识，特别用实例给出了 EGP 和 IGP 的交互方法；介绍了 BGP 的最新发展，特别是对于 4 字节 AS 号的支持；增加了 BGP 安全相关的实例。

第 13 章　Internet 组播。针对组播地址的新发展，对地址的使用方式进行了系统梳理。

第 14 章　移动 IP。更新了代理通告、注册扩展等内容。

第 15 章　应用层系统服务。给出了 DHCP 的最新发展，包括选项扩展、租用更新扩展等，描述了 DHCP 的安全问题。DNS 方面，对于域名的最新变化、根服务器的最新变化进行了更新，同时给出了一些 DNS 安全事件的实例。

第 16 章　网络管理标准 SNMP。全面梳理了 SNMP 的发展历程，对“对象”“实例”等概念以及读取单个对象、表格对象的实例进行了更新，同时总结了 SNMP 面临的安全威胁。

为突出重点，方便阅读，我们把第 1 版的“第 17 章应用层协议”根据协议的应用相似性拆分成三章，并增加了 Telnet 和 NTP 两个新协议。具体为：

第 17 章　万维网与电子邮件系统。在万维网方面，更新了其发展历史，增加了最新的 HTTP2 协议简介，并描述了 HTTP 面临的安全问题。在电子邮件系统方面，着力描述了其面临的安全问题。

第 18 章　文件共享与远程登录。在文件共享方面，更新了 FTP 的主动模式、被动模式等内容，同时描述了其安全问题；新增了远程登录协议 Telnet。

第 19 章　信息查询与时间服务。在信息查询方面，对 Whois 的新进展进行了系统梳理和描述；新增了网络时间协议 NTP。

总的来说，在本书更新时，我们着力考虑了以下四点：一是给读者最新、最权威的解读，所有协议的内容都覆盖到本书修订完成之际（2017 年 4 月）的最新信息，所有解读都尽量查找最原始的出处；二是适应当前网络安全研究的热点，给出了每个协议存在的一些安全缺陷和风险；三是尽量反映我国科技工作者在网络协议发展中所做出的贡献；四是对于每一个协议都增加了发展历程，以便给读者一个清晰的脉络，同时也便于读者查找相关资源进行进一步的研究。

在本书第 2 版即将出版之际，笔者特别感谢机械工业出版社的支持，感谢朱劼编辑和迟振春编辑的辛勤工作！在本书第 1 版前言中，笔者介绍了本书的形成过程。没有解放军信息工程大学王清贤教授的前期积累，我们可能需要走更艰苦的路。本书第 2 版编写完成后，王清贤教授再次通读了全文，并对每一章都提出了修改建议，在此表示衷心的感谢！

本书在编写过程中参阅了不少文献，书后的参考文献中未必能一一列举，不周之处还望谅解，并在此一并感谢！

由于水平有限，错漏之处在所难免，热忱欢迎广大读者批评、指导及交流，编者的电子邮箱为：kouxiaorui@263.net。

编　者

第 1 版前言

网络的重要性和普及性已毋庸多言。在网络通信的方方面面中，网络协议发挥着基础的支撑作用。现有的协议很多，本书重点关注 TCP/IP 协议族，因为它是目前使用最为广泛的协议族，也是 Internet 出现、发展和普及的基础。如果说没有协议就不会有网络，那么也可以说没有 TCP/IP，可能就没有今天的 Internet。

TCP/IP 有效解决了异构网络互联问题，并且提供了确保网络高效、可靠运转的一系列机制。在 TCP/IP 搭建的这个平台上，可以使用单点和多点通信方式、固定和移动通信方式，并构建各种网络应用。

1974 年，出现 TCP/IP 的雏形。到 20 世纪 80 年代，它就已经在异构网络互联中占据统治地位。但协议设计者的脚步并没有停止，至今，新的协议标准以及现有标准的新版本仍在不断涌现。

这种发展将是一个长期的过程，因为从用户的角度，新的应用将不断出现；而从基础设施的角度，TCP/IP 不仅要把物理设备和链路激活，更要充分发挥硬件的性能。而硬件技术的发展是极其迅速的，这个趋势近年来表现得尤其明显。因而 TCP/IP 的设计者和研究者们也在不断适应这种发展速度而推陈出新。

TCP/IP 是个庞大的体系，本书则着眼于那些构建 Internet 所必需的、与我们交互最直观的协议，并着力保持全书的简洁性和易读性。在内容选取上，本书力图保证协议体系的完整性、连贯性和先进性。本书选取的大部分协议都是在目前互联网体系中经常使用的。虽然本书涉及的 RARP、BOOTP 这两个协议现在已经不再使用，但它们的思想有可取之处，目前经常使用的 DHCP 也是基于 BOOTP 定义，所以我们也用简短的篇幅对它们进行了讨论。

本书也体现了协议的新发展，比如加入 ICMP 的域名报文和安全失败报文，以及轻量级 UDP（UDP-Lite）等。此外，我们将有关应用及安全问题体现于各个章节中，以便读者能够对这些应用有更为深入的了解，并反过来促进对协议的理解。在部分章节和参考文献中，还给出有关的研究方向和研究成果，为读者开展相关领域的研究抛砖引玉。

本书共有 17 章。第 1 章讨论 TCP/IP 的引入、思想、分层以及发展历史等内容，并给出本书所涉及的协议在整个协议栈中的位置及依赖关系。随后 16 章讨论具体协议，并按照在协议栈中的位置由下向上的次序组织。

第 2 章讨论数据链路层协议 PPP 以及认证相关的 PAP 和 CHAP。

第 3 章讨论基本的 IP 编址方法，以及 IP 地址与物理地址的映射技术，涉及 ARP 和 RARP 两个协议。

第 4 章讨论互联网协议 IP，包括 IP 数据报以及 IP 选路。

第 5 章讨论 Internet 控制报文协议 ICMP。

第 6 章和第 7 章讨论传输层的引入及 UDP、TCP 这两个传输层协议。

第 8 章讨论透明路由器、代理 ARP、子网编址、超网和 CIDR 以及网络地址转换等提高 IP 地址使用效率的技术。

第 9 章讨论路由表维护方式、路由算法以及 Internet 的路由体系结构。

第 10 章和第 11 章讨论两个内部网关协议 RIP 和 OSPF。第 12 章则讨论边界网关协议 BGP。

第 13 章讨论组播相关内容，包括组播编址、IGMP、组播路由算法、组播路由协议以及组播性能。

第 14 章讨论移动 IP，包括其工作机制和隧道技术。

第 15 章讨论那些对互联网正常高效运转起支撑作用的应用层协议，包括 BOOTP、DHCP 和 DNS。

第 16 章讨论网络管理标准 SNMP，包括 MIB、SMI 以及 SNMP 通信协议。

第 17 章讨论常用的应用层协议，包括用于文件传输的 NFS 和 FTP，用于 WWW 的 HTTP，用于电子邮件系统的 SMTP、POP、IMAP 和 MIME，以及用于信息查询的 Whois。

附录中给出了本书所出现的所有缩略词的全称。

本书的很多章节都包含实例，其中出现的大部分 IP 地址都只是为说明某个问题而随机选取的，不与任何实际目标相关。对于某些实例中出现的地址，出于隐私考虑，我们将其中部分字节用“*”代替。图片中涉及的隐私信息则作涂黑处理。

阅读本书的读者应掌握一定的计算机网络基础知识。在阅读本书时，除了掌握协议规定的内容外，更应该吸取其思想。比如，我们可能不会去实现一个 IP 分片重组的算法，但本书给出的重组算法思想对于设计一个分块下载文件的程序具有指导作用。

本书由解放军信息工程大学信息工程学院网络工程系组织编写。我们从 2000 年开始正式在研究生和本科生两个层次开展“网络协议分析”课程的教学工作，受到了广泛的好评。本书在正式出版之前，相关讲义已经在学院内部 8 届次学生中使用，并以此为基础根据学生平时的提问及反馈意见进行了修改。

在本书即将出版之际，特别要感谢王清贤教授。他最先开始该课程的教学，并整理了一个非常清晰的框架，本书很大部分内容参考了他的教案。在本书编写完成后，王清贤教授和武东英副教授作为本书的主审，认真通读了全书，提出了中肯而宝贵的建议。

另外，还要感谢解放军信息工程大学信息工程学院的支持，感谢机械工业出版社华章分社的支持，感谢参与本书校对的王佳杉先生，感谢解放军信息工程大学信息工程学院各位教员和学员提出的宝贵意见和建议。

热忱欢迎广大读者批评、指导及交流，编者的电子邮箱为：kouxiaorui@263.net。

编　者

2009 年 1 月

目录

第1章 TCP/IP概述

1.1 网络互联与TCP/IP

Internet给我们带来了极大的便利，但究竟什么是Internet，对此很难给出准确的回答。幸运的是，已经有人为我们把握这个问题提供了一个非常有帮助的描述：Internet是一个世界范围的“Network of Networks”（网络之网络）。Networks意味着有多个网络，其中既有局域网，又有城域网和广域网，还有一般意义的互联网（internet，即使仅有两台主机，不论用何种技术使其彼此通信，也叫internet）。其中所涵盖的种类很多，单从局域网来讲，就有以太网、令牌环网、光纤网和无线局域网等。这些网络在信道的访问方式和数据的传送方式上都存在差异。

出现如此多种的网络类型并非偶然，因为没有任何一种类型可以满足所有的需求：价格低廉的高速局域网受到地理跨度的限制，跨越长距离的广域网不能提供低费用的本地通信，而移动用户不能使用有线通信技术等。

虽然从技术角度看各类网络都存在差异，但从用户的角度看，却需要一种通用的互联。举个直观的例子，学校的校园网通常采用以太网技术，学校的网站服务器、邮件服务器都通过以太网技术连接于校园网中。在无线网络接入无比便捷的时代，当你在家中访问学校的网站或收取电子邮件时，通常可以使用无线技术。现在的问题就是：以太网帧格式（数据格式）和无线上网使用的Wi-Fi（Wireless Fidelity，无线保真）帧格式不同，传输介质不同，物理地址形式也不同，如何在各种Networks存在的前提下将它们互联起来呢？

Vinton Cerf等互联网的奠基者早在40年前就为我们提出了一个技术思路：在每个网络内部使用各自的通信协议，每个网络与其他网络通信时使用TCP/IP协议族。

1.1.1 用IP实现异构网络互联

从用户的角度看，实现异构网络互联的关键点就是使各种网络类型之间的差异对自己透明。在TCP/IP协议族中，能够屏蔽底层物理网络的差异，向上提供一致

性的协议就是 IP（Internet Protocol）——互联网协议。图 1-1 示意了 IP 如何解决异构网络互联问题。IP 位于底层物理网络和高层应用之间，它定义了标准的 IP 数据报格式以及标准的 IP 地址格式。对于应用而言，它直接看到的是统一的数据形式和地址格式，而不是各不相同的底层物理网络。

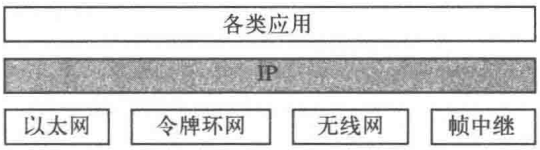

图 1-1　IP 解决异构网络互联问题示意

从用户的角度看，异构网络互联问题已经得到了解决，但从技术层面看又有另外一个现实的问题：虽然上层应用看到的都是 IP 数据报，但是数据必须要通过底层物理网络才能发送出去。在无线网与以太网互联的例子中，无线网络中传递的仍然是 Wi-Fi 帧，而以太网收到的又必须是以太网帧。要想实现二者之间的互联，必须有一个中间转化设备，这个关键设备就是路由器[⊖]。路由器在异构网络互联时所起的作用如图 1-2 所示。

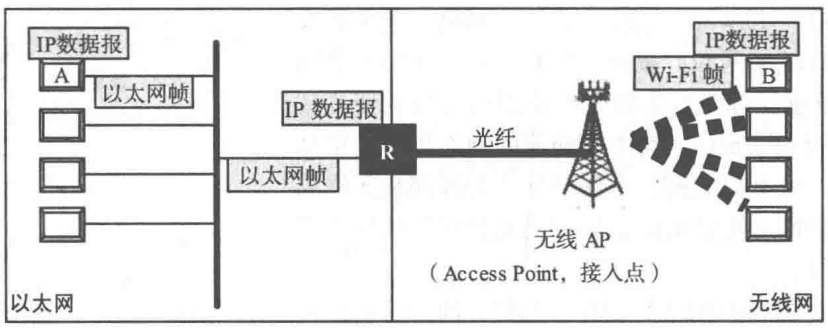

图 1-2　路由器在异构网络互联中所起的作用示意[⊜]

在这个例子中，处于以太网中的主机 A 与处于无线网络中的主机 B 进行通信。源主机 A 的高层应用首先将数据封装在 IP 数据报中。IP 数据报在投递到以太网中之前，被封装成以太网帧。这个帧到达路由器后，路由器提取其中的 IP 数据报，并把它封装成 Wi-Fi 帧，转发到无线网络中。而这个 Wi-Fi 帧到达目的主机后，IP 数据报被提取出来并被递交给上层应用。在这个过程中，主机 A 和 B 的上层应用是对等实体，虽然经过了不同的底层物理网络，但与它们直接交互的都是 IP[⊜]。

综上，从协议层面看 IP 解决了网络互联问题；从实现层面看，路由器是实现网络互联的核心设备，整个 Internet 就是由无数个用路由器互联起来的物理网络构成的，如图 1-3 所示。

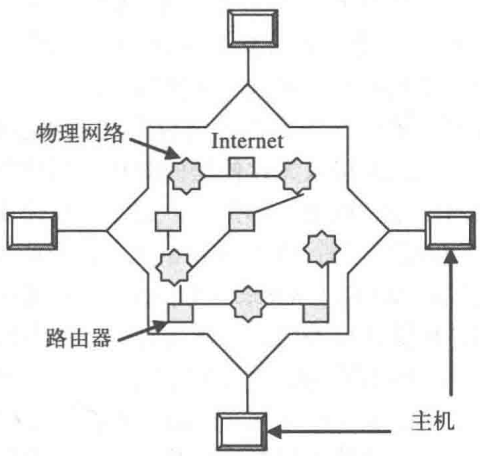

图 1-3　Internet 的构成示意

⊖ 在网络互联技术发展之初，对于“网关”“网桥”“路由器”等设备有着明确的区分，但是现在这些设备的界限已经模糊了，路由器通常具备路由、桥接等功能，所以此处使用“路由器”这个名词。

⊜ 实际中两台主机之间的通信通常需要跨越多个物理网络和路由器，此处仅阐述路由器连接异构网络的思想，因此只画出了跨越一个路由器和两个异构网络的示例。

⊜ 实际中应用和 IP 之间还有一个层次。由于此处仅讨论思想，所以暂时忽略该细节。

从 IP 的角度看，Internet 中的每个网络无论规模大小，作用如何，其地位都是同等的，类似以太网的局域网、用作主干网的广域网或者两台计算机之间的点到点链路，都可以视为一个网络。

除实现异构网络互联外，路由器的另一个重要功能就是在其所连接的多个网络之间转发 IP 数据报。每当收到一个目的地址不是自己的数据报时，路由器必须选择一条合适的路径将其转发出去，以便其能够到达目的端。

从用户的角度看，Internet 是一个单独的虚拟网络，它就是“Network of Networks”中的“Network”，因为用户能够与任意一台连接在 Internet 上的主机通信，而不管中间间隔了多少个路由器和多少个物理网络。这种观点如图 1-4 所示。

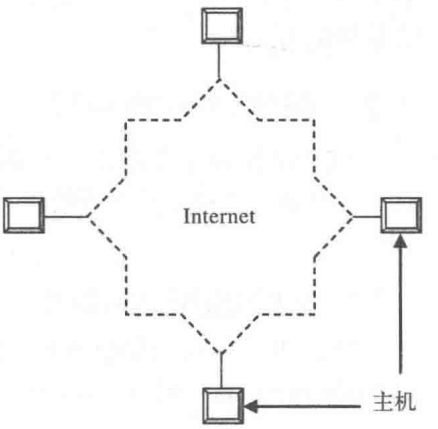

图 1-4　从用户的角度看 Internet

1.1.2　TCP/IP 协议族的引入

IP 的引入解决了异构网络互联问题，但确保一个庞大的、由异构网络组成的系统正确高效地运转却并不是一件容易的事，必须要考虑诸多问题。首先，当通信源端主机和目的主机跨越多个物理网络时，必须寻找一条能够将数据报由源端投递到目的端的路径。路由器是 IP 数据报转发的核心设备，要想实现数据报的正确转发，它必须对整个系统有准确的认识。而所有路由器对这个复杂系统的认识必须是一致的。

其次，网络通信存在不可靠性。物理线路信号可能出现噪声，而且路由设备处理能力有限。当一个路由器的处理能力达到极限时，经过其转发的数据报会被丢弃。此外，这个系统是一个分组交换系统，而且是一个图型结构，两个通信端点之间的 IP 数据报可能会经过不同的路径投递并出现乱序现象。

再次，面对这个复杂的系统，必须有适当的控制机制。比如，要能够检测其中节点的活动性，在发生拥塞时要能够进行控制。

上述这些问题如果都用 IP 这一个协议来解决，会使 IP 过于庞大。事实上，面对这样一个复杂的系统，TCP/IP 协议族的设计者采用了一种“简化问题，分而治之”的策略。对于每个问题，都引入专门的协议来解决。比如，设计了 OSPF（Open Shortest Path First，开放式最短路径优先）、RIP（Routing Information Protocol，选路信息协议）和 BGP（Border Gateway Protocol，边界网关协议）等协议用于路由信息的维护，ICMP（Internet Control Message Protocol，Internet 控制报文协议）实现网络控制，TCP（Transmission Control Protocol，传输控制协议）提高可靠性等。这种策略一方面减轻了协议设计和实现的复杂度，另一方面有利于软件的更新换代，因为即便一个问题的解决方案被替换了，也不会影响其他协议的使用。IPv6[⊖] 的出现就是一个很好的例子：IPv6 如果取代了 IPv4，其他协议都不受影响。

在上述有关网络基础设施正常高效运转的问题得以解决后，就可以基于这个基础设施构建各种应用。比如用于文件传输的 FTP（File Transfer Protocol，文件传输协议）、用于远程登录的 Telnet（Teletype network）、用于电子邮件发送的 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）等。上述所有这些协议与 IP 一起构成了 TCP/IP 协议族。

⊖ 本书不讨论 IPv6，仅讨论 IPv4，所有出现的“IP”均表示 IPv4，特殊情况下会做说明。

综上，我们对 TCP/IP 界定如下：TCP/IP 是一个被广泛采用的网际互联协议标准，它是一个协议族（protocol family）或协议套件（protocol suite），TCP 和 IP 是其中两个最重要的且必不可少的协议，故用它们作为代表命名。如果没有 TCP/IP，很难想象我们会拥有一个现在这样的 Internet。

1.2　网络协议的分层

TCP/IP 协议族中包含多个协议，它们之间并不孤立。那么这些协议之间的依赖关系如何，设计者又是按照什么样的思路来构建整个协议族的体系结构呢？这就涉及网络协议的分层问题。

1.2.1　通用的协议分层思想

网络协议分层的思想不是 TCP/IP 特有的，而是一种被广泛认可的通用思想。著名的 OSI（Open System Interconnection，开放系统互连）模型也采用了分层结构，它的协议栈包括 7 层。

网络中的通信是指在不同系统中的实体之间的通信。所谓实体，是指能发送和接收信息的任何对象，包括终端、应用软件和通信进程等。

两个系统中实体间的通信是一个十分复杂的过程，为了减少协议设计和调试过程的复杂性，大多数网络的实现都按层次的方式来组织，每一层完成一定的功能，每一层又都建立在它的下层之上。不同的网络，其层的数量、各层的名字、内容和功能不尽相同。然而，在所有的网络中，每一层都是通过层间接口向上一层提供一定的服务，同时把这种服务实现的细节对上层加以屏蔽。

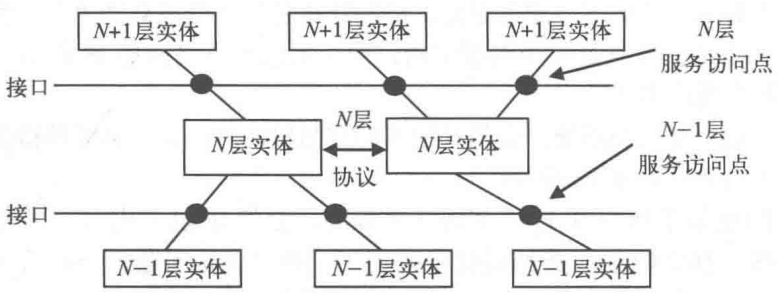

图 1-5　网络协议分层的思想示意

图 1-5 示意了这种思想，具体包括以下几个含义：

1）第 N 层实体在实现自身定义的功能时，只使用 $N-1$ 层提供的服务。

2）N 层向 $N+1$ 层提供服务，此服务不仅包括 N 层本身所具备的功能，还包括由下层服务提供的功能总和。

3）最底层只提供服务，是提供服务的基础；最高层只是用户，是使用服务的最高层；中间各层既是下一层的用户，又是上一层服务的提供者。

4）仅在相邻层间有接口，且下层服务的实现细节对上层完全透明。

N 层中的活动元素通常称为 N 层实体。不同机器上同一层的实体称为对等实体。N 层实体实现的服务为 $N+1$ 层所利用。服务是在服务访问点（Service Access Point，SAP）处提供给上层使用的。N 层 SAP 就是 $N+1$ 层可以访问 N 层服务的地方。每个 SAP 都有一个能够唯一标识它的地址。举例来说，我们可以把电话系统中的电话插孔看成是一种 SAP，而 SAP