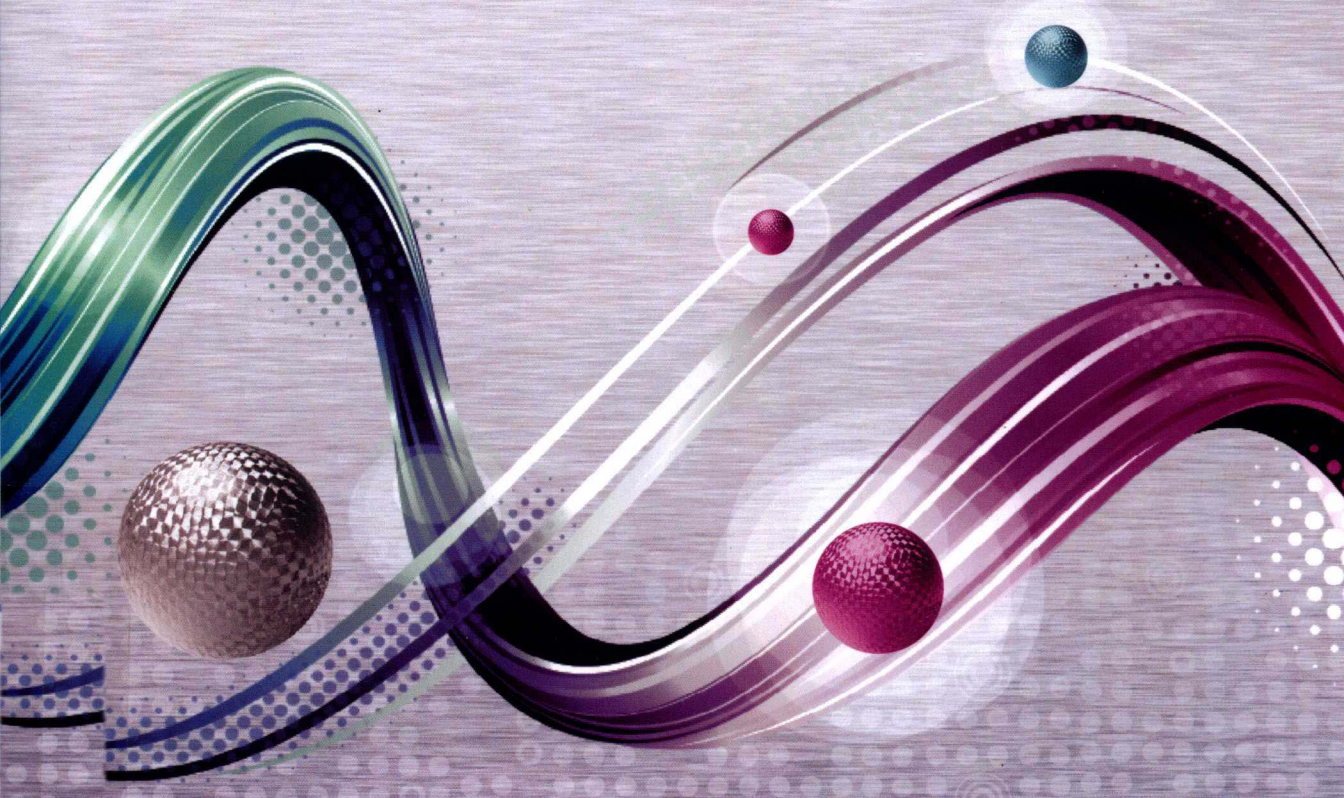
高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

网络设备安全配置与管理

林宏刚　何林波　唐远涛　编著



西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

网络设备安全配置与管理

林宏刚　何林波　唐远涛　编著

西安电子科技大学出版社

内 容 简 介

本书阐述了计算机网络基础知识，详细介绍了路由器和交换机的工作原理与基本配置，系统地讲解了路由器和交换机安全配置以及管理的相关知识和方法，并以配置操作为主详细讲解了相应操作步骤。

全书共 11 章，主要介绍了网络技术基础、以太网技术及交换机基本配置、虚拟局域网、交换机的安全配置、网络互联技术及路由器基本配置、路由协议及配置、三层交换机配置、路由器的安全配置、访问控制列表、网络地址转换等内容。

本书语言通俗易懂，内容丰富翔实，突出了以实践操作为中心的特点，理论与实践相结合，可操作性强。本书可作为高等院校信息安全、计算机科学与技术、通信工程等专业本科生的教材，也可供网络技术研究及开发人员参考。

图书在版编目(CIP)数据

网络设备安全配置与管理 / 林宏刚，何林波，唐远涛编著. —西安：西安电子科技大学出版社，2019.1
ISBN 978-7-5606-5219-1

Ⅰ. ① 网… Ⅱ. ① 林… ② 何… ③ 唐… Ⅲ. ① 计算机网络—安全技术 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2019)第 020237 号

策划编辑　李惠萍
责任编辑　闵远光　雷鸿俊
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西利达印务有限责任公司
版　　次　2019 年 1 月第 1 版　2019 年 1 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　14.25
字　　数　332 千字
印　　数　1～3000 册
定　　价　34.00 元
ISBN 978-7-5606-5219-1 / TP

XDUP 5521001-1

中国电子教育学会高教分会推荐

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

编审专家委员会名单

名誉主任：何大可（中国密码学会常务理事）

主　　任：张仕斌（成都信息工程大学信息安全学院副院长、教授）

副 主 任：李　飞（成都信息工程大学信息安全学院院长、教授）

何明星（西华大学计算机与软件工程学院院长、教授）

苗　放（成都大学计算机学院院长、教授）

赵　刚（西南石油大学计算机学院院长、教授）

李成大（成都工业学院教务处处长、教授）

宋文强（重庆邮电大学移通学院计算机科学系主任、教授）

梁金明（四川理工学院计算机学院副院长、教授）

易　勇（四川大学锦江学院计算机学院副院长、
成都大学计算机学院教授）

宁多彪（成都东软学院计算机科学与技术系主任、教授）

编审专家委员：（排名不分先后）

叶安胜　黄晓芳　黎忠文　张　洪　张　蕾　贾　浩　宁多彪

赵　攀　陈　雁　韩　斌　李享梅　曾令明　何林波　盛志伟

林宏刚　王海春　索　望　吴春旺　韩桂华　赵　军　陈　丁

秦　智　王中科　林春蔷　张金全　王祖俪　蔺　冰　王　敏

万武南　甘　刚　王　燚　闫丽丽　昌　燕　黄源源　张仕斌

李　飞　王力洪　苟智坚　何明星　苗　放　李成大　宋文强

梁金明　万国根　易　勇　吴　震　左旭辉

前　言

计算机网络是计算机技术和通信技术紧密结合的产物，它的诞生使计算机体系结构发生了巨大的变化。目前，计算机网络已广泛地应用于工业、商业、金融、政府、教育、科研及人们日常生活的各个领域，成为信息社会的基础设施，并在当今社会经济中起着非常重要的作用，对人类社会的进步做出了巨大的贡献。网络在给广大用户带来方便、快捷的同时其安全性却日益恶化。以病毒、木马、僵尸网络、间谍软件等为代表的恶意代码层出不穷，拒绝服务攻击、网络仿冒、垃圾邮件等安全事件仍十分猖獗。网络的安全以及对不良信息内容的有效控制和管理已是急需解决的问题。

在现代计算机网络中，无论是简单的小型局域网还是复杂的大型广域网，路由器、交换机都是网络中不可缺少的设备，因此网络安全就离不开路由器、交换机的各种安全机制与设备。

网络设备安全配置与管理是计算机科学与技术、信息安全等专业的一门专业必修课程。作为该课程的教材，本书阐述了计算机网络基础知识，系统地讲解了路由器和交换机的工作原理与主要配置，详细介绍了路由器和交换机安全配置以及管理的相关知识和方法。书中分章节深入阐述各种网络配置的原理，并以配置操作为重点详细讲解相应的操作步骤。本书对原理的介绍密切联系实际，力求避免枯燥的理论叙述，以实践动手操作为主，重点培养学生的实际动手能力。

本书对应课程的参考教学时间为 40～50 学时，可根据学生已掌握的知识及相关课程安排做适当裁减，建议以上机实验为主，理论讲解为辅，重点强调学生实际操作，有条件的话，可以全部在实验室完成本课程的学习。全书共 11 章，分三个部分。第一部分(第 1 章)介绍网络的基础知识，包括 TCP/IP 网络模型、IP 地址的分类以及网络协议的相关知识。第二部分(第 2～4 章)在介绍交换机的相关知识和基本配置的基础上，系统地讲解了交换机安全配置和管理的相关知识与配置方法。第三部分(第 5～11 章)在介绍路由器的相关知识和基本配置的基础上，系统地讲解了路由器安全配置和管理的相关知识与配置方法。

本书注重理论与实践的紧密结合，内容通俗易懂，图文并茂，力求实用，努力解决理论学习与实践应用相脱节的问题。本书编写组成员长期从事教学和科研工作，在计算机学科建设、课程建设、网络规划和网络工程实践上具有丰富的实践经验。本书的编写做到了内容系统、简练，实用性强，结构安排合理，论述简明清晰，适用于课程教学和实践教学。

本书在编写过程中多次得到有关领导及兄弟院校、研究所的专家、同行的热情帮助和支持，西安电子科技大学出版社为本书的出版也做了大量的工作，在此一并表示衷心的感谢。

由于编者的水平有限，书中难免会有疏漏和不妥之处，恳请各位专家和读者批评指正。本书在编写过程中参考了许多资料，在此向有关作者致以衷心的感谢。

编 者

2018 年 12 月 1 日

目　录

第 1 章　网络技术基础 1
1.1　网络的基本概念 1
1.1.1　计算机网络的发展 1
1.1.2　数据交换方式 2
1.1.3　网络的体系结构 4
1.1.4　OSI/RM 模型 5
1.1.5　TCP/IP 模型 8
1.1.6　OSI 与 TCP/IP 模型的比较 9
1.1.7　数据的封装与解封 10
1.2　网络相关术语 10
1.2.1　网络的性能指标 10
1.2.2　网络的拓扑结构 12
1.2.3　局域网 15
1.2.4　广域网 17
1.2.5　城域网 18
1.3　网络的介质 19
1.3.1　铜介质 19
1.3.2　光缆 21
1.3.3　无线传输介质 23
习题一 25
实验一 26
第 2 章　以太网技术及交换机基本配置 27
2.1　以太网的技术基础 27
2.1.1　以太网的发展 27
2.1.2　IEEE 802.3 和 OSI 模型 28
2.1.3　以太网 MAC 地址 29
2.1.4　以太网帧结构 29
2.1.5　介质访问控制方法 31
2.1.6　冲突域与广播域 31
2.1.7　以太网类型 32
2.2　二层交换机简介 34
2.2.1　交换机的处理技术 34
2.2.2　交换机的工作模式 35
2.2.3　交换机的工作原理 36
2.2.4　交换机的主要指标 37
2.3　配置二层交换机 39
2.3.1　交换机的配置方式 39
2.3.2　使用命令行接口配置交换机 43
2.3.3　交换机的基本管理配置 46
2.3.4　交换机接口的基本配置 50
2.3.5　查看交换机的系统和配置信息 52
2.4　交换机链路聚合 53
2.4.1　链路聚合概述 53
2.4.2　交换机链路聚合配置 54
2.5　生成树协议 55
2.5.1　生成树协议概述 55
2.5.2　STP 与 RSTP 协议 57
2.5.3　生成树协议配置 58
2.6　系统日志管理 59
2.6.1　启用系统日志 59
2.6.2　配置系统日志信息的发送 60
2.6.3　配置日志消息的时间戳 60
2.6.4　配置消息严重性阈值 60
2.6.5　显示记录配置 60
习题二 61
实验二 61
第 3 章　虚拟局域网(VLAN) 62
3.1　VLAN 概述 62
3.2　VLAN 在交换机上的实现方法 63
3.3　VLAN 中继协议 64
3.3.1　IEEE 802.1Q 协议 65
3.3.2　Cisco ISL 协议 66
3.4　基于端口的 VLAN 配置 66
3.4.1　单交换机的 VLAN 配置 66
3.4.2　跨交换机的 VLAN 配置 68
3.5　Cisco VTP 的 VLAN 实现 72
3.5.1　VTP 概述 72
3.5.2　VTP 工作原理 73
3.5.3　在 Cisco 交换机上配置 VTP 75

习题三 77
实验三 77
第 4 章　交换机的安全配置 78
4.1　终端访问安全 78
4.1.1　配置控制台访问口令 78
4.1.2　配置虚拟终端访问口令 79
4.1.3　登录密码设置 79
4.1.4　配置和管理 SSH 80
4.1.5　终端访问限制 81
4.1.6　配置特权等级 82
4.2　基于交换机端口的安全控制 84
4.2.1　风暴控制 84
4.2.2　端口保护控制 85
4.2.3　端口阻塞控制 85
4.2.4　端口安全性 86
4.3　绑定 IP 和 MAC 地址 90
4.4　动态 ARP 检测 90
4.4.1　在 DHCP 环境下配置动态 ARP 检测 91
4.4.2　在无 DHCP 环境下配置动态 ARP 检测 91
4.5　基于 IEEE 802.1x 的 AAA 服务 92
4.5.1　概述 92
4.5.2　基于 IEEE 802.1x 的认证配置 94
4.6　交换机访问控制列表 99
习题四 99
实验四 99
第 5 章　网络互联技术及路由器基本配置 100
5.1　TCP/IP 协议与 IP 地址 100
5.1.1　TCP/IP 中的协议 100
5.1.2　IP 地址 102
5.1.3　IP 地址的子网划分 103
5.1.4　可变长子网掩码与无类域间路由 104
5.1.5　IPv6 协议 106
5.2　路由器简介 107
5.2.1　路由器的硬件构成 108
5.2.2　路由器的软件构成 109
5.2.3　路由器的接口 109
5.3　路由和数据包转发简介 113
5.3.1　路由选择 113
5.3.2　路由表 114
5.3.3　交换与路由的比较 114
5.3.4　路由器转发 IP 包流程 115
5.4　路由器的基本配置 117
5.4.1　命令行接口 120
5.4.2　路由器的命令模式 121
5.4.3　路由器的基本配置 122
5.4.4　路由器接口配置 131
5.4.5　路由器口令配置 134
5.5　VLAN 间路由 136
5.5.1　传统 VLAN 间路由 136
5.5.2　单臂路由器 VLAN 间路由 136
习题五 138
实验五 138
第 6 章　路由协议及配置 139
6.1　路由表简介 139
6.2　静态路由与配置 140
6.2.1　静态路由配置示例 141
6.2.2　缺省路由配置示例 142
6.3　动态路由 142
6.4　RIP 协议及其配置 143
6.4.1　配置 RIP v1 145
6.4.2　配置 RIP v2 145
6.4.3　关闭路由自动汇聚 146
6.4.4　验证配置 146
6.4.5　RIP 实例 147
6.5　OSPF 协议及其配置 148
6.5.1　通配符掩码 150
6.5.2　创建 OSPF 路由进程 150
6.5.3　配置 OSPF 接口参数 151
6.5.4　验证配置 152
6.5.5　OSPF 配置示例 154
6.6　EIGRP 协议及其配置 157
6.6.1　创建 EIGRP 路由进程 157
6.6.2　验证配置 158
6.6.3　EIGRP 实例 159

习题六 163
实验六 163
第 7 章　三层交换机配置 164
7.1　三层交换机交换原理 164
7.1.1　交换原理 164
7.1.2　三层交换机与路由器 166
7.1.3　三层交换的特点 168
7.1.4　高层交换机及其发展 168
7.2　三层交换机的配置 169
7.2.1　三层交换机的基本配置 169
7.2.2　三层交换机的端口配置 171
7.3　利用三层交换机实现 VLAN 通信 172
7.3.1　VLAN 互通原理 172
7.3.2　三层交换机实现 VLAN 互通示例 173
7.4　三层交换机的路由配置 175
7.4.1　静态路由配置 175
7.4.2　RIP 协议配置 176
7.4.3　OSPF 协议配置 179
习题七 180
实验七 180
第 8 章　路由器的安全配置 181
8.1　终端访问安全配置 181
8.2　网络服务管理 181
8.3　路由协议安全 184
8.3.1　启用 RIP v2 身份验证 184
8.3.2　启用 OSPF 身份验证 186
8.3.3　启用 EIGRP 身份验证 187
8.4　使用网络加密 189
8.4.1　IPsec 协议简介 189
8.4.2　IPsec site-to-site VPN 配置 190
8.5　其他的安全配置 191
8.5.1　禁用 AUX 端口 191
8.5.2　禁止从网络启动和自动从网络下载初始配置文件 191
8.5.3　禁止未使用或空闲的端口 191
习题八 191
实验八 191
第 9 章　访问控制列表 193
9.1　访问控制列表概念 193
9.2　IP 访问控制列表 195
9.2.1　标准编号 ACL 196
9.2.2　标准命名 ACL 197
9.2.3　扩展编号 ACL 199
9.2.4　扩展命名 ACL 200
9.2.5　限制远程登录的范围 200
9.3　MAC 扩展访问控制列表 201
9.4　基于时间的访问控制列表 202
9.5　显示 ACL 配置 203
习题九 204
实验九 204
第 10 章　网络地址转换 205
10.1　网络地址转换(NAT)概述 205
10.1.1　私有地址和公有地址 205
10.1.2　相关术语 205
10.1.3　NAT 工作原理 207
10.1.4　NAT 应用 207
10.1.5　NAT 优缺点 208
10.2　静态 NAT 209
10.3　动态 NAT 209
10.4　PAT 技术 211
习题十 213
实验十 213
第 11 章　综合实例 214
11.1　案例背景 214
11.2　技术需求分析 215
11.3　实验拓扑及地址规划 215
11.4　实验设备说明 216
11.5　实验步骤与配置参考 216

第 1 章　网络技术基础

计算机网络是计算机技术与通信技术相结合的产物，随着计算机技术和通信技术的不断发展，计算机网络也经历了从简单到复杂，从单机到多机的发展历程。本章主要向读者介绍计算机网络和网络协议的基本概念。

1.1　网络的基本概念

1.1.1　计算机网络的发展

现代意义上的计算机网络是从 1969 年美国国防部高级研究计划局(DARPA)建成 ARPAnet 实验网开始的。该网络当时只有 4 个节点，以电话线路为主干网络，两年后，建成 15 个节点，进入工作阶段，此后规模不断扩大，20 世纪 70 年代后期，网络节点超过 60 个，主机 100 多台，地理范围跨越美洲大陆，连通了美国东部和西部的许多大学和研究机构，而且通过通信卫星与夏威夷和欧洲地区的计算机网络相互连通。

20 世纪 70 年代后期是通信网大发展的时期，各个发达国家的政府部门、研究机构和电报电话公司都在发展分组交换网络。这些网络都以实现计算机之间的远程数据传输和信息共享为主要目的，通信线路大多采用租用的电话线路，少数铺设了专用线路，这一时期的网络称为第二代网络，以远程大规模互联为其主要特点。

随着计算机网络技术的不断成熟，网络应用越来越广泛，网络规模增大，通信变得复杂。各大计算机公司纷纷制定了自己的网络技术标准。IBM 于 1974 年推出了系统网络结构(System Network Architecture，SNA)，为用户提供能够互联的成套通信产品；1975 年 DEC 公司宣布了自己的数字网络体系结构(Digital Network Architecture，DNA)；1976 年 UNIVAC 宣布了该公司的分布式通信体系结构(Distributed Communication Architecture，DCA)。这些网络技术标准仅在一个公司范围内有效，符合这些标准的网络通信产品能够互联，它们只是同一公司生产的系列设备。网络通信市场这种各自为政的状况使得用户在投资方向上无所适从，也不利于多厂商之间的公平竞争。针对这种情况，1977 年 ISO 组织的 TC97 信息处理系统技术委员会 SC16 分技术委员会开始着手制定开放系统互联参考模型(OSI/RM)。

OSI/RM 的出现标志着第三代计算机网络的诞生。此时的计算机网络在共同遵循 OSI 标准的基础上，形成了一个具有统一网络体系结构，并遵循国际标准的开放式和标准化的网络。OSI/RM 参考模型把网络划分为七个层次，并规定计算机之间只能在对应层之间进行通信，大大简化了网络通信原理。因此，它是公认的新一代计算机网络体系结构的基础，为普及局域网做出了贡献。

20 世纪 80 年代末，局域网技术发展日趋成熟，随着光纤及高速网络技术的发展，整个网络发展成以 Internet 为代表的因特网，就像一个对用户透明的、大的计算机系统，这就是直至现在的第四代计算机网络时期。此时计算机网络定义为“将多个具有独立工作能力的计算机系统通过通信设备和线路由功能完善的网络软件实现资源共享和数据通信的系统”。事实上，时至今日对于计算机网络也从未有过一个标准的定义。

1972 年，Xerox 公司发明了以太网，1980 年 2 月 IEEE 组织了 802 委员会，开始制定局域网标准。1985 年美国国家科学基金会(National Science Foundation)利用 ARPAnet 协议建立了用于科学研究和教育的骨干网络 NSFnet，1990 年 NSFnet 取代 ARPAnet 成为国家骨干网，并且走出了大学和研究机构，进入社会，从此网上的电子邮件、文件下载和信息传输受到人们的欢迎和广泛使用。1992 年，Internet 学会成立，该学会把 Internet 定义为“组织松散的，独立的国际合作互联网络”，“通过自主遵守计算协议和过程支持主机对主机的通信”。1993 年，伊利诺伊大学国家超级计算中心成功开发网上浏览工具 Mosaic(后来发展为 Netscape)，同年美国总统克林顿宣布正式实施国家信息基础设施(National Information Infrastructure)计划，从此在世界范围内开展了争夺信息化社会领导权和制高点的竞争。与此同时，NSF 不再向 Internet 注入资金，完全使其进入商业化运作。20 世纪 90 年代后期，Internet 以惊人的速度发展。

未来的计算机网络，即下一代计算机网络(NGN)，普遍被认为是因特网、移动通信网络、固定电话通信网络的融合，是 IP 网络和光网络的融合；是可以提供包括语音、数据和多媒体等各种业务的综合开放的网络构架；是业务驱动、业务与呼叫控制分离、呼叫与承载分离的网络；是基于统一协议的、基于分组的网络。在功能上，NGN 分为四层，即接入和传输层、媒体层、控制层、网络服务层，涉及软交换、MPLS、E-NUM 等技术。

1.1.2 数据交换方式

在通信系统中，通信大多是在多点之间进行的，数据通信时需要利用中间节点将通信双方连接起来。因此，在设计网络结构时，必须考虑采用的数据“交换”方式。所谓交换技术，就是动态地分配传输线路资源的通信技术。

常用的数据交换技术有电路交换、报文交换和分组交换三种方式。

1. 电路交换

电路交换也称为线路交换，它类似于电话系统，希望通信的计算机之间必须事先建立物理电路。整个电路交换的过程包括电路建立、数据传输和电路拆除三个阶段。

(1) 电路建立：在传输任何数据之前，要先经过呼叫过程建立一条端到端的电路。如图 1-1 所示，若 H1 站要与 H3 站连接，典型的做法是：H1 站先向与其相连的 A 节点提出请求，然后 A 节点在通向 C 节点的路径中找到下一个支路。比如 A 节点选择经 B 节点的电路，在此电路上分配一个未用的通道，并告诉 B 节点它还要连接 C 节点；B 再呼叫 C，建立电路 BC，最后，节点 C 完成到 H3 站的连接。这样

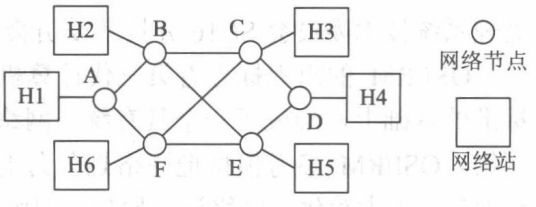


图 1-1 交换网络的拓扑结构

A 节点与 C 节点之间就有一条专用电路 ABC，用于 H1 站与 H3 站之间的数据传输。

(2) 数据传输：电路 ABC 建立以后，数据就可以从 A 节点发送到 B 节点，再由 B 节点交换到 C 节点；C 节点也可以经 B 节点向 A 节点发送数据。在整个数据传输过程中，所建立的电路必须始终保持连接状态。

(3) 电路拆除：数据传输结束后，由某一方(A 节点或 C 节点)发出拆除请求，然后逐节拆除到对方节点。

电路交换在数据传送开始之前必须先设置一条专用的通路。在线路释放之前，该通路由一对用户完全占用。其优点在于数据传输可靠、迅速，数据不会丢失且保持原来的序列。但对于猝发式的通信，电路交换效率不高。在某些情况下，电路空闲时的信道容易被浪费；在短时间数据传输时电路建立和拆除所用的时间得不偿失。因此，电路交换适用于系统间要求高质量的大量数据传输的情况。

2. 报文交换

报文交换的数据传输单位是报文，报文就是站点一次性要发送的数据块，其长度不限且可变。当某个站点要发送报文时，它将一个目的地址附加到报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。

每个节点在收到整个报文并检查无误后，就暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点。因此，端与端之间无需先通过呼叫建立连接。

一个报文在每个节点的延迟时间，等于接收报文所需的时间加上向下一个节点转发报文所需的排队延迟时间之和。

报文从源点传送到目的地采用“存储—转发”方式，在传送报文时，一个时刻仅占用一段通道。其优点如下：

(1) 线路效率较高，这是因为许多报文可以用分时方式共享一条节点到节点的通道。

(2) 不需要同时使用发送器和接收器来传输数据，网络可以在接收器可用之前暂时存储这个报文。

(3) 在线路交换网上，当通信量变得很大时，就不能接受某些呼叫。而在报文交换上却仍然可以接收报文，只是传送延迟会增加。

(4) 报文交换系统可以把一个报文发送到多个目的地。

(5) 能够建立报文的优先权。

(6) 报文交换网可以进行速度和代码的转换，因为每个站点都可以用它特有的数据传输率连接到其他站点，所以两个不同传输率的站点也可以连接，另外还可以转换传输数据的格式。

由于报文在交换节点中要进行缓冲存储，需要排队，因此报文交换不能满足实时或交互式的通信要求，报文经过网络的延迟时间长且不确定；当节点收到过多的数据而无空间存储或不能及时转发时，就不得不丢弃报文，而且发出的报文不一定会按发出的顺序到达目的地。

3. 分组交换

分组交换是报文交换的一种改进，它将报文分成若干个分组，每个分组的长度有一个上限，有限长度的分组使得每个节点所需的存储能力降低了，分组可以存储到内存中，提

高了交换速度。它适用于交互式通信，如终端与主机通信。分组交换有虚电路分组交换和数据报分组交换两种。它是计算机网络中使用最广泛的一种交换技术。

1) 虚电路分组交换

在虚电路分组交换中，为了进行数据传输，网络的源节点和目的节点之间要先建立一条逻辑通路。每个分组除了包含数据之外还包含一个虚电路标识符。在预先建好的路径上的每个节点都知道把这些分组引导到哪里去，不再需要路由选择判定。最后，由某一个站用清除请求分组来结束这次连接。它之所以是“虚”的，是因为这条电路不是专用的。

虚电路分组交换的主要特点是：在数据传送之前必须通过虚呼叫设置一条虚电路。但并不像电路交换那样有一条专用通路，分组在每个节点上仍然需要缓冲，并在线路上进行排队等待输出。

2) 数据报分组交换

在数据报分组交换中，每个分组的传送是被单独处理的。每个分组称为一个数据报，每个数据报自身携带足够的地址信息。一个节点收到一个数据报后，根据数据报中的地址信息和节点所储存的路由信息，找出一个合适的出路，把数据报原样地发送到下一节点。由于各数据报所走的路径不一定相同，因此不能保证各个数据报按顺序到达目的地，有的数据报甚至会在中途丢失。整个过程中，没有虚电路建立，但要为每个数据报做路由选择。

1.1.3 网络的体系结构

计算机网络系统是一个十分复杂的系统。将一个复杂系统分解为若干个容易处理的子系统，然后“分而治之”，这种结构化设计方法是工程设计中常见的手段。计算机网络的体系结构就是采用层次化结构来定义计算机网络系统的组成方法和系统功能，它将一个网络系统分成若干层次，并且规定了每个层次应该实现的功能以及应该向上层提供的服务，同时规定了两个网络系统的各个层次实体之间进行通信时应该遵守的协议。

1. 层次模型

计算机网络的层次结构一般以垂直分层模型来表示，如图 1-2 所示。

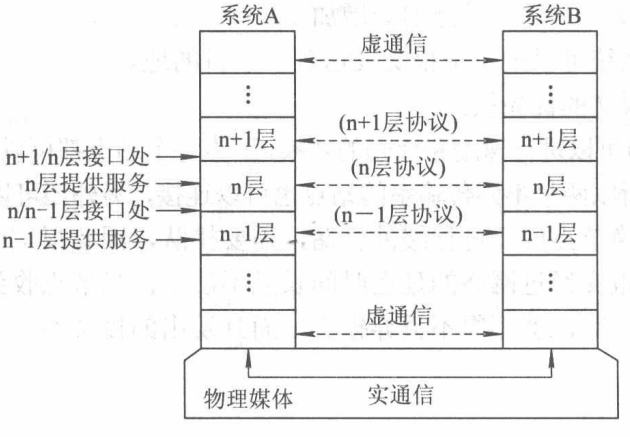


图 1-2　计算机网络的层次模型

从图 1-2 可以看出，系统 A 的某一层直接与系统 B 的同一层进行通信，当然这种通信

是逻辑上的通信，除了在物理媒体上进行的是实通信之外，其余各对等实体间进行的都是虚通信。

在这个模型中，不同系统的对等层没有直接通信的能力，它们之间的通信需要依靠下面各层的支持。在网络的分层模型中，对等层的“虚”通信必须遵循该层的协议。

在计算机网络环境中，两台计算机的两个进程直接的通信过程与邮政通信过程十分相似。网络中对等层之间的通信规则就是该层使用的协议。同一计算机的不同功能层之间的通信规则称为接口。例如第 n 层与第 n−1 层之间的接口称为 n/n−1 层接口。总之，协议是不同机器对等层之间的通信约定，而接口是同一机器相邻层之间的通信约定。

网络体系结构中层次结构划分的原则如下：

(1) 每层的功能应是明确的，并且是相互独立的。当某一层的具体实现方法更新时，只要保持上、下层的接口不变，便不会对邻居层产生影响。

(2) 层间接口必须清晰，跨越接口的信息量应尽可能少。

(3) 层数应适中。若层数太少，则造成每一层的协议太复杂；若层数太多，则体系结构过于复杂，使描述和实现各层功能变得困难。

这种分层模型的特点是：以功能作为划分层次的基础；第 n 层的实体在实现自身定义的功能时，只能使用第 n−1 层提供的服务；第 n 层在向第 n+1 层提供服务时，此服务不仅包含第 n 层本身的功能，还包含由下层服务提供的功能；仅在相邻层间有接口，且所提供服务的具体实现细节对上一层完全屏蔽。

2. 网络协议

在计算机网络系统中，为了保证通信双方能正确地、自动地进行数据通信，针对通信过程的各种情况，制定了一整套约定，这就是网络系统的通信协议。通信协议是一套语义和语法规则，用来规定有关功能部件在通信过程中的操作。

两个通信对象在进行通信时，须遵从相互接受的一组约定和规则，这些约定和规则使它们在通信内容、怎样通信以及何时通信等方面相互配合。这些约定和规则的集合称为协议。简单地说，协议是通信双方必须遵循的控制信息交换的规则的集合。

一般来说，一个网络协议主要由语法、语义和时序三大要素组成：

(1) 语法是指数据与控制信息的结构或格式，用于确定通信时采用的数据格式、编码及信号电平等，也就是“怎么讲”。

(2) 语义由通信过程的说明构成，规定了需要发出何种控制信息，完成何种动作以及做出何种应答，并对发布请求、执行动作以及返回应答予以解释，以及确定用于协调和差错处理的控制信息，也就是“讲什么”。

(3) 时序是指事件执行顺序的详细说明，指出事件的顺序以及速度匹配。

由此可见，网络协议是计算机网络不可缺少的组成部分。

1.1.4　OSI/RM 模型

OSI(Open System Interconnection)参考模型即 OSI/RM，全称为开放式系统互联参考模型，由国际标准化组织(ISO，该组织成立于 1947 年，由多个国家组成)在 1984 年发布，其目的就是要使在各种终端设备之间、计算机之间、网络之间，以及用户之间在互相交换信

息的过程中，能够逐步实现标准化，能够将复杂的网络或计算机系统划分成简单的独立组成部分，每一部分都有开放标准接口，为生产商们提供了共同遵循的国际标准。OSI 参考模型属于分层结构体系，由七层组成，从最低层到最高层依次为：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每一层由不同交换的数据单元组成，独立完成各层功能，其参考模型、交换单元如图 1-3 所示。

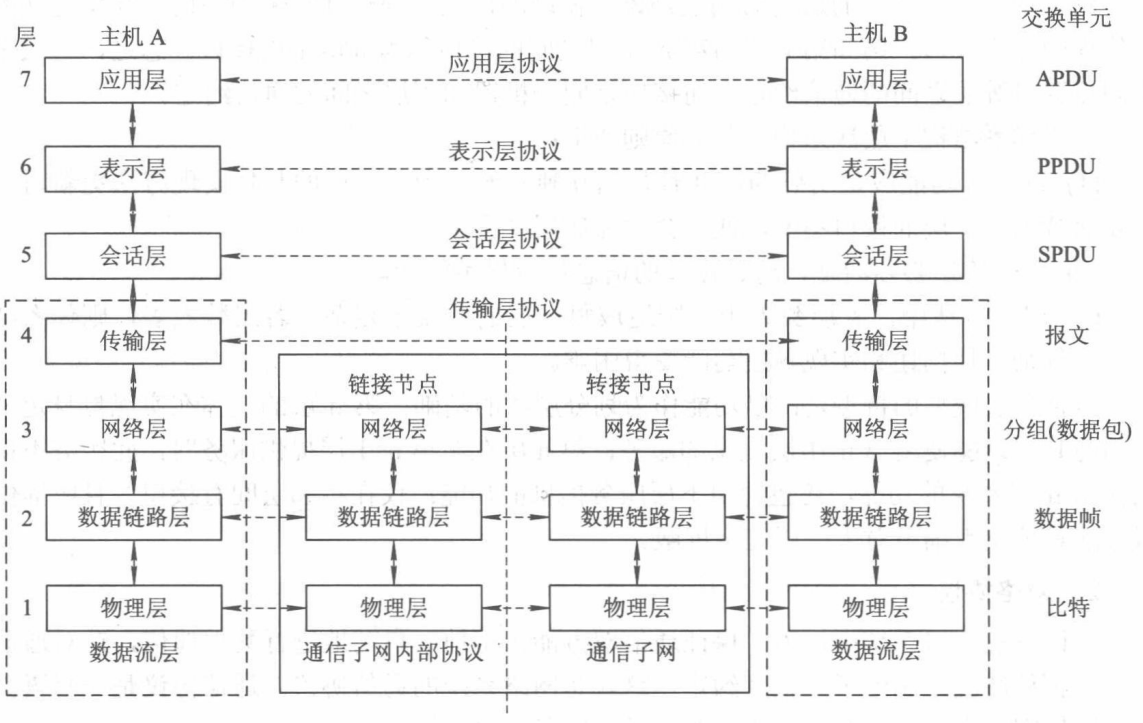


图 1-3　OSI/RM 参考模型及每层交换单元

其各层的功能如下：

1．物理层

物理层是 OSI/RM 的最低层，传输的数据单元为原始比特流。该层任务是利用传输介质(常见为光纤、双绞线等)为它的上一层(即数据链路层)提供物理连接，完成物理链路的建立、维护和拆除，体现机械的、电气的、功能的和规程的特性。比如，该层规定了电缆和接头的类型及相关规格，以及传送信号的电压值、电压变化的频率等；如果是光信号，则规定光波信号的一些属性。

物理层定义的典型规范代表包括：EIA/TIA RS-232、EIA/TIA RS-449、V.35、RJ-45 等。

局域网中常见物理层设备有集线器和中继器。

2．数据链路层

数据链路层是为网络层提供服务的，解决两个相邻节点之间的链路通信问题，即无差错地传送数据，传送的数据单元为数据帧，系统根据帧提供的信息来决定如何处理数据。该层除了将不可靠的物理链路转换成对网络层来说无差错的数据链路外，还要协调收发双方的数据传输速率，即进行流量控制，解决由于接收方因来不及处理发送方发来的高速数据而导致缓冲器溢出及线路阻塞问题。

目前，数据链路层被划分为两个子层：

(1) 介质访问控制(MAC)子层(IEEE 802.3)：MAC 子层负责指定如何通过物理线路进行传输，并定义与物理层的通信。比如，指定物理编址、网络拓扑、线路规范、错误通知、流量控制等。

(2) 逻辑链路控制(LLC)子层(IEEE 802.2)：LLC 子层负责识别协议类型，并对数据进行封装(解封)以便通过网络进行传输，具有发送帧、接收帧的功能以及帧序列控制和流量控制等功能。

数据链路层协议的代表包括：SDLC、HDLC、PPP、STP、帧中继等。

局域网中常见数据链路层设备主要有网桥、二层交换机。

3．网络层

网络层是为传输层提供服务的，传送的数据单元为数据包或分组。该层主要解决数据包如何通过各节点转发的问题，即通过路径选择算法(路由)将数据包送到目的地，网络层支持局域网(LAN)、城域网(MAN)和广域网(WAN)组建的各种物理标准，对应的网络设备主要有路由器和三层交换机。网络层通常完成如下功能：

(1) 为传输层提供服务：有面向连接的网络服务和无连接的网络服务。典型的网络层协议是 ITU-T 的 X.25 协议，它是一种面向连接的分组交换协议。

(2) 组包和拆包：包头包含了源节点地址和目标节点地址，以及相关的控制信息。

(3) 路由选择：也称为路径选择，是根据一定的原则和路由选择算法在多个节点的通信子网中选择一条最佳路径。确定路由选择的策略称为路由算法。

(4) 流量控制：流量控制的作用是控制阻塞，避免死锁。

网络层协议的代表包括：IP、IPX、RIP、OSPF 等。

4．传输层

传输层是通信子网和高三层(应用层、表示层、会话层)之间的接口层，其任务是根据通信子网的特性，最佳地利用网络资源，为两个端系统的会话层之间提供建立、维护和取消传输连接的功能，负责端到端的可靠的、透明的数据传输，包括处理差错控制和流量控制等问题。传输层传送的数据单元为段或报文，协议有 TCP、UDP、SPX 等。

5．会话层

会话层也可以称为会晤层，会话层不参与具体的传输，主要功能是管理和协调不同主机上各种进程之间的通信(对话)，即负责建立、管理和终止应用程序之间的会话。比如建立数据库服务器和用户登录之间的会话，以及退出或注销该会话。

6．表示层

表示层用于管理数据编码的方式，即处理流经节点的数据格式编码和转换问题，比如视频、图像的公用压缩编码格式的转换和对应用层数据的公用加密、公用解密。

7．应用层

应用层是 OSI/RM 的最高层，是用户与应用程序同网络访问协议之间的接口。该层通过应用程序来完成网络用户的应用需求，比如文件传输、收发电子邮件、Web 访问等。

应用层协议的代表包括：TELNET、FTP、HTTP、SNMP 等。

从图 1-3 可以得到，七层 OSI/RM 模型的下四层形成了数据流层，并规定为终端之间如何建立连接以及交换数据，并负责规定如何通过物理线路传输，经由网络互联设备到达目的终端，最终传递给应用程序。在高层中，同样也有网络互联设备，比如网关(Gateway)，它用于高层协议的转换，它也被称为协议转换器，可以是一台设备，也可以是一种协议转换软件。

1.1.5　TCP/IP 模型

TCP/IP(Transmission Control Protocol/Internet Protocol)，即传输控制协议/网际协议，是一组用于实现网络互联的通信协议集，它包括上百个各种功能的协议，如远程登录、文件传输和电子邮件等，而 TCP 协议和 IP 协议是保证数据完整传输的两个基本的重要协议。TCP/IP 协议目前是 Internet 上应用最广泛的协议，几乎所有的网络都支持该协议。

通常，将 TCP/IP 协议体系划分为四层，TCP/IP 协议体系也是基于 OSI/RM 的，但是与 OSI/RM 有所区别，图 1-4 所示的为 TCP/IP 体系结构与 OSI/RM 各层之间的对比。

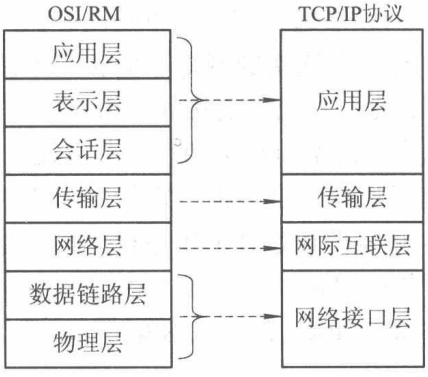


图 1-4　TCP/IP 与 OSI/RM 各层对比

TCP/IP 协议结构各层的具体任务和功能描述如下：

1．网络接口层

网络接口层与 OS/RM 中的物理层和数据链路层相对应。网络接口层定义了如何使主机通过物理网络传输数据，也定义了各种局域网(LAN)或广域网(WAN)的接口所需的协议和硬件。

网络接口层在发送端将上层的 IP 数据报封装成帧后发送到网络上；数据帧通过网络到达接收端时，该节点的网络接口层对数据帧拆封，并检查帧中包含的目的 MAC 地址。如果该地址就是本机的 MAC 地址或者是广播地址，则向上传递给网络层，否则丢弃该帧。

当使用串行线路将主机与网络相互连接，或网络与网络相互连接的时候，可以通过广域网(WAN)的连接标准 PPP(点到点协议)或帧中继来完成互联通信，例如，主机通过 Modem 和电话线接入 Internet，则需要在网络接口层运行 SLIP 或 PPP 协议。

2．网际互联层

与 OSI/RM 网络层具有相似的功能，其主要功能是解决主机到主机的通信问题，以及建立互联网络。即根据数据报所携带的目的 IP 地址，通过路由器进行路由选择，选择一条链路传送到目的主机。