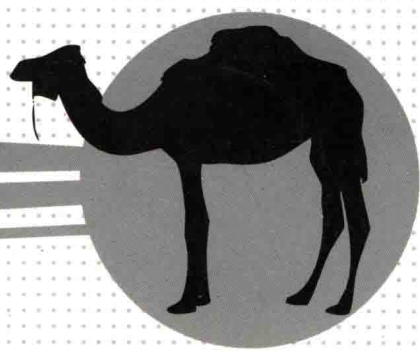


全国高等职业教育计算机类规划教材·实例与实训教程系列

局域网交换机和路由器的配置与管理

- 李建林 主 编
- 史 律 王伟林 副主编
- 聂 明 主 审



- ◆ 网络工程实例化项目演练
- ◆ 园区网实施模拟平台训练
- ◆ 网络基础知识嵌入式讲解
- ◆ 企业工程师全程参与指导



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

全国高等职业教育计算机类规划教材·实例与实训教程系列

局域网交换机和路由器的配置与管理

李建林 主编

史 律 王伟林 副主编

聂 明 主 审

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书为典型的进阶式案例化教程，共分为 3 章：第 1 章主要介绍计算机网络的基本概念、网络层次结构、网络互连设备以及思科 Packet Tracer 软件的基本使用方法；第 2 章为基本任务环节，以南京信息职业技术学院校园局域网为实际案例，介绍局域网的规划设计、所使用的技术以及园区网络中交换机与路由器的配置与管理；第 3 章为提高任务环节，介绍如何利用相关网络技术优化网络以提高网络的安全性和可靠性。全书将一个完整的网络工程案例细化成相对独立的项目，每个项目中穿插了技术原理的讲解、基本实验训练，再通过若干前后衔接的任务完成每个相对独立的项目乃至整个工程案例。

本书可以作为高职以及本科计算机网络，通信工程等专业的专业课教材，相关专业的实训课指导材料，也可以提供给广大工程技术人员参考使用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目 (CIP) 数据

局域网交换机和路由器的配置与管理 / 李建林主编. —北京：电子工业出版社，2013.9
全国高等职业教育计算机类规划教材. 实例与实训教程系列

ISBN 978-7-121-20791-4

I. ①局… II. ①李… III. ①局域网—信息交换机—高等职业教育—教材②局域网—路由选择—高等职业教育—教材 IV. ①TN915.05

中国版本图书馆 CIP 数据核字 (2013) 第 137068 号

策划编辑：程超群

责任编辑：郝黎明 文字编辑：裴 杰

印 刷：北京市李史山胶印厂

装 订：北京市李史山胶印厂

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×1 092 1/16 印张：18.75 字数：480 千字

印 次：2013 年 9 月第 1 次印刷

定 价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010) 88258888。

前言

随着微电子技术、计算机技术和通信技术的迅速发展和相互渗透，计算机网络技术已发展成为当今最热门的学科之一。在过去的二十年里，由于网络互连设备的普及，特别是由于交换机与路由器的广泛使用，使得 Internet 得到了长足的发展。金融、教育、行政、医疗等各行各业都在进行着基础网络的建设，也在不断推进着现有网络的升级和改造，随之而来的就是社会对计算机网络技术专业的人才的需求量也越来越大。

计算机网络技术专业是面向网络工程应用的计算机科学与技术类专业，旨在培养具有计算机网络技术基础知识，掌握计算机网络软硬件基本理论和技术，掌握网络工程的基本原理与实现方法，能独立完成网络工程项目并解决项目中的实际问题的专门人才。在计算机网络技术专业，特别是高等职业院校的计算机网络技术专业中，学生就业大多面向实际的网络工程师岗位，如何让学生在短期内进入行业的专业领域，让学生通过在校课程的学习就可以初步具备实际网络工程项目规划能力并能够在项目中熟练地配置交换机与路由器，是该专业课程设置以及教材编写上遇到的主要问题。目前市面上针对网络工程设备操作以及交换路由基本原理的教材和参考资料很多，但现有教材大多注重原理的讲解，注重交换机和路由器上操作的命令行，各个实验环节相互独立，无法帮助读者形成完整的基于真实网络工程项目的知识体系，学生在学习后并不能很好地在实际的项目中灵活运用所学到的知识，这正是我们筹划设计并编写本教材的原因。

本书是编者多年从事网络工程的实践经验和教学经验的积累。本书的编者经过多次商议和讨论，对于本书的编写达成了以下的共识：第一，以南京信息职业技术学院校园网的真实项目案例贯穿全书，以各子项目任务驱动完成相关网络技术学习；第二，让学生在本书的学习过程中掌握一个相对完整的项目，而不是一个个独立的实验或知识点；第三，让实际的网络工程项目在本书中占主导地位，而不是一个个基本的技术原理或一条条设备上的命令行；第四，通过一个个细分的项目任务环节，让学生在学习本书的过程中循序渐进地完成整个项目，并同时理解项目所应用的技术原理。为此，在本书的编写过程中，编者做出了长足的努力，将一个以南京信息职业技术学院校园网为例的完整的网络工程案例细化成相对独立的项目，每个项目中穿插了技术原理的讲解和基本实验训练，再通过若干前后衔接的任务完成每个独立的项目乃至整个的工程案例。考虑到初学计算机网络专业的学生的实际水平和能力，

书中的案例是经过与企业工程师商讨后简化过的案例；又考虑到并非各个学校都具备足够的相同类型的交换机和路由器提供给学生进行相关实验，在本书中我们又将简化后的案例移植到思科的 PACKET TRACER 模拟软件中实现，并保存各个任务的模拟工程文件提供给学生课后学习和参考。

本书由李建林担任主编，史律、王伟林担任副主编。其中，第 1 章由南京信息职业技术学院图文信息中心网络工程师王伟林编写，第 2 章由南京信息职业技术学院计算机与软件学院网络与信息安全教研室史律编写，第 3 章由南京信息职业技术学院计算机与软件学院副院长李建林编写，全书由李建林教授统稿。南京信息职业技术学院计算机与软件学院院长聂明教授对书稿进行审阅，南京信息职业技术学院 2010 级以及 2011 级计算机网络技术、计算机应用专业的王甜、智倩婷以及王举同学对所有基础实验环节和任务进行了测试。来自星网锐捷网络技术有限公司的网络工程师庄伟对本书的编写给予了大力的支持和帮助。

由于作水平有限，书中难免有欠妥之处，望广大读者批评指正。

编者

2013 年 8 月



第一章 网络基础知识	1
1.1 计算机网络及其体系结构	1
1.1.1 IP 协议	7
1.1.2 IP 地址的组成、分类与管理	12
1.1.3 子网与子网划分	20
1.2 局域网技术	25
1.2.1 带宽共享式以太网	27
1.2.2 交换式以太网	29
1.2.3 虚拟局域网	31
1.3 典型网络互联设备	37
1.3.1 二层交换机	37
1.3.2 路由器	43
1.3.3 三层交换机	47
1.4 网络安全设备介绍	49
1.4.1 防火墙	49
1.4.2 入侵检测系统	54
1.4.3 入侵防护系统	55
1.5 Cisco Packet Tracer 5.3 模拟器使用简介	59
1.5.1 Cisco Packet Tracer 5.3 模拟器使用方法	59
第二章 基本任务环节	64
2.1 项目一 南信院校园网的规划设计	64
2.1.1 南信校园网目前现状	64
2.1.2 南信校园网实际整体项目规划设计	64
2.1.3 任务一 “南信院” 校园网建设需求分析	65
2.1.4 任务二 规划、设计方案选择	65
2.1.5 任务三 使用 PT 模拟简化后的校园网核心层，汇聚层基本拓扑	70

2.2	项目二 科技楼接入层交换机配置	76
2.2.1	接入层的基本功能	76
2.2.2	认识接入层以太网交换机	76
2.2.3	基础实验一 交换机基本配置实验	84
2.2.4	任务一 规划设计科技楼实验室接入层网络	91
2.2.5	任务二 使用 PT 模拟科技楼实验室接入层网络的拓扑	94
2.3	项目三 校园网接入层交换机以及虚拟局域网的配置	97
2.3.1	虚拟局域网 (VLAN)	97
2.3.2	VLAN 的分类	98
2.3.3	Trunk 链路封装协议及配置	100
2.3.4	VTP 管理域	102
2.3.5	VLAN 的创建与配置步骤	104
2.3.6	基础实验一 在单台交换机下实现 VLAN	104
2.3.7	基础实验二 跨交换机实现 VLAN	106
2.3.8	基础实验三 实现交换机 Trunk 功能	108
2.3.9	任务一 配置科技楼接入层交换机 VLAN	111
2.3.10	任务二 配置科技楼汇聚层交换机 VLAN	113
2.3.11	任务三 测试科技楼内部网络的连通性	116
2.4	项目四 汇聚层与核心层三层交换机的端口 IP 地址	119
2.4.1	汇聚层以及核心层基本功能	119
2.4.2	任务一 汇聚层交换机基本端口配置	121
2.4.3	任务二 核心层交换机基本端口配置	124
2.5	项目五 通过 RIP 路由协议实现校园网的互通	125
2.5.1	路由基本原理以及动态路由协议	125
2.5.2	RIP 路由协议及其基本原理	128
2.5.3	基础实验一 静态路由以及默认路由的基本配置	134
2.5.4	基础实验二 RIP 路由协议的基本配置	136
2.5.5	任务一 应用 RIP 路由协议实现校园网的部分互通	139
2.5.6	任务二 在 RIP 路由进程中下放默认路由	144
2.6	项目六 通过 OSPF 路由协议实现校园网的互通	147
2.6.1	OSPF 路由协议及其基本原理	147
2.6.2	基础实验一 OSPF 路由协议的基本配置	152
2.6.3	任务一 应用 OSPF 路由协议实现校园网的互通	155
2.6.4	任务二 在 OSPF 路由进程中下放默认路由	160
2.6.5	任务三 校园网 RIP 与 OSPF 路由协议的重分布	162
2.7	项目七 通过 NAT 技术实现校园网对 Internet 的访问	167
2.7.1	校园网的 Internet 接入	167



2.7.2	传统串口相关封装协议 (PPP, HDLC)	168
2.7.3	NAT 的基本原理	170
2.7.4	基础实验一 PPP 串口封装协议及其认证	172
2.7.5	基础实验二 静态以及动态 NAT 的基本配置	176
2.7.6	任务一 配置动态的 NAPT 实现校园网中计算机对 Internet 的访问	178
2.7.7	任务二 配置静态的 NAPT 实现外网访问校园网中的服务器的访问	183
第三章 提高任务环节		186
3.1	项目一 通过配置生成树协议以及端口聚合提高网络的可靠性	186
3.1.1	生成树协议 (STP) 及其原理	186
3.1.2	交换机的端口聚合	189
3.1.3	基础实验一 交换机生成树协议的基本配置	191
3.1.4	基础实验二 交换机端口聚合的基本配置	194
3.1.5	任务一 配置科技楼汇聚层交换机以及接入层交换机间的生成树协议	199
3.1.6	任务二 配置服务器群组三层交换机到核心交换机间的端口聚合	203
3.2	项目二 通过配置端口安全策略提高接入层安全性	208
3.2.1	任务一 配置科技楼接入层交换机的端口安全	208
3.3	项目三 通过访问控制列表实现校园网访问控制策略	211
3.3.1	访问控制列表概述	211
3.3.2	基础实验一 标准访问控制列表的配置	216
3.3.3	基础实验二 扩展访问控制列表的配置	221
3.3.4	任务一 配置校园网中访问控制列表	225
3.3.5	任务二 南信院校园网 ACL 案例分析	227
3.4	项目四 校园网防火墙的使用	228
3.4.1	防火墙功能概述	228
3.4.2	防火墙的体系结构	229
3.4.3	防火墙的基本配置过程和基本配置思路	231
3.4.4	学院防火墙安全需求分析	232
3.4.5	防火墙接口和网络对象的定义	234
3.4.6	校园网防火墙的路由设计	238
3.4.7	防病毒与攻击的策略	241
3.4.8	网络带宽及会话管理策略	243
3.4.9	网页内容过滤策略	246
3.4.10	防火墙 VPN 功能的实现	246
3.5	项目五 通过帧中继 (FR) 实现分校区与主校区的互通	249
3.5.1	帧中继的基本原理	249
3.5.2	基础实验一 帧中继的基本配置实验	252



168	3.5.3	任务一 配置古平岗校区和仙林校区之间的帧中继连接	256
170	3.5.4	任务二 通过帧中继实现古平岗校区和仙林校区的互联	263
257	3.6	项目六 通过 IPSec VPN 实现分校区与主校区的互通	266
176	3.6.1	基础实验一 IPSec VPN 的基本配置	266
178	3.6.2	任务一 通过 IPSec VPN 实现古平岗校区和仙林校区的互联	273
181	3.6.3	任务二 通过 GRE over IPSec 实现古平岗校区和仙林校区的互联	284
186	3.7	项目七 配置 VLAN 及 VLAN 间路由	291
186	3.7.1	基础实验一 VLAN 的基本配置	291
188	3.7.2	任务一 通过 VLAN 实现部门间的隔离	291
191	3.7.3	任务二 通过 VLAN 实现部门间的互通	291
194	3.7.4	任务三 通过 VLAN 实现部门间的互通	291
199	3.7.5	任务四 通过 VLAN 实现部门间的互通	291
203	3.7.6	任务五 通过 VLAN 实现部门间的互通	291
208	3.7.7	任务六 通过 VLAN 实现部门间的互通	291
208	3.7.8	任务七 通过 VLAN 实现部门间的互通	291
211	3.7.9	任务八 通过 VLAN 实现部门间的互通	291
211	3.7.10	任务九 通过 VLAN 实现部门间的互通	291
216	3.7.11	任务十 通过 VLAN 实现部门间的互通	291
216	3.7.12	任务十一 通过 VLAN 实现部门间的互通	291
216	3.7.13	任务十二 通过 VLAN 实现部门间的互通	291
216	3.7.14	任务十三 通过 VLAN 实现部门间的互通	291
216	3.7.15	任务十四 通过 VLAN 实现部门间的互通	291
216	3.7.16	任务十五 通过 VLAN 实现部门间的互通	291
216	3.7.17	任务十六 通过 VLAN 实现部门间的互通	291
216	3.7.18	任务十七 通过 VLAN 实现部门间的互通	291
216	3.7.19	任务十八 通过 VLAN 实现部门间的互通	291
216	3.7.20	任务十九 通过 VLAN 实现部门间的互通	291
216	3.7.21	任务二十 通过 VLAN 实现部门间的互通	291
216	3.7.22	任务二十一 通过 VLAN 实现部门间的互通	291
216	3.7.23	任务二十二 通过 VLAN 实现部门间的互通	291
216	3.7.24	任务二十三 通过 VLAN 实现部门间的互通	291
216	3.7.25	任务二十四 通过 VLAN 实现部门间的互通	291
216	3.7.26	任务二十五 通过 VLAN 实现部门间的互通	291
216	3.7.27	任务二十六 通过 VLAN 实现部门间的互通	291
216	3.7.28	任务二十七 通过 VLAN 实现部门间的互通	291
216	3.7.29	任务二十八 通过 VLAN 实现部门间的互通	291
216	3.7.30	任务二十九 通过 VLAN 实现部门间的互通	291
216	3.7.31	任务三十 通过 VLAN 实现部门间的互通	291
216	3.7.32	任务三十一 通过 VLAN 实现部门间的互通	291
216	3.7.33	任务三十二 通过 VLAN 实现部门间的互通	291
216	3.7.34	任务三十三 通过 VLAN 实现部门间的互通	291
216	3.7.35	任务三十四 通过 VLAN 实现部门间的互通	291
216	3.7.36	任务三十五 通过 VLAN 实现部门间的互通	291
216	3.7.37	任务三十六 通过 VLAN 实现部门间的互通	291
216	3.7.38	任务三十七 通过 VLAN 实现部门间的互通	291
216	3.7.39	任务三十八 通过 VLAN 实现部门间的互通	291
216	3.7.40	任务三十九 通过 VLAN 实现部门间的互通	291
216	3.7.41	任务四十 通过 VLAN 实现部门间的互通	291
216	3.7.42	任务四十一 通过 VLAN 实现部门间的互通	291
216	3.7.43	任务四十二 通过 VLAN 实现部门间的互通	291
216	3.7.44	任务四十三 通过 VLAN 实现部门间的互通	291
216	3.7.45	任务四十四 通过 VLAN 实现部门间的互通	291
216	3.7.46	任务四十五 通过 VLAN 实现部门间的互通	291
216	3.7.47	任务四十六 通过 VLAN 实现部门间的互通	291
216	3.7.48	任务四十七 通过 VLAN 实现部门间的互通	291
216	3.7.49	任务四十八 通过 VLAN 实现部门间的互通	291
216	3.7.50	任务四十九 通过 VLAN 实现部门间的互通	291
216	3.7.51	任务五十 通过 VLAN 实现部门间的互通	291
216	3.7.52	任务五十一 通过 VLAN 实现部门间的互通	291
216	3.7.53	任务五十二 通过 VLAN 实现部门间的互通	291
216	3.7.54	任务五十三 通过 VLAN 实现部门间的互通	291
216	3.7.55	任务五十四 通过 VLAN 实现部门间的互通	291
216	3.7.56	任务五十五 通过 VLAN 实现部门间的互通	291
216	3.7.57	任务五十六 通过 VLAN 实现部门间的互通	291
216	3.7.58	任务五十七 通过 VLAN 实现部门间的互通	291
216	3.7.59	任务五十八 通过 VLAN 实现部门间的互通	291
216	3.7.60	任务五十九 通过 VLAN 实现部门间的互通	291
216	3.7.61	任务六十 通过 VLAN 实现部门间的互通	291
216	3.7.62	任务六十一 通过 VLAN 实现部门间的互通	291
216	3.7.63	任务六十二 通过 VLAN 实现部门间的互通	291
216	3.7.64	任务六十三 通过 VLAN 实现部门间的互通	291
216	3.7.65	任务六十四 通过 VLAN 实现部门间的互通	291
216	3.7.66	任务六十五 通过 VLAN 实现部门间的互通	291
216	3.7.67	任务六十六 通过 VLAN 实现部门间的互通	291
216	3.7.68	任务六十七 通过 VLAN 实现部门间的互通	291
216	3.7.69	任务六十八 通过 VLAN 实现部门间的互通	291
216	3.7.70	任务六十九 通过 VLAN 实现部门间的互通	291
216	3.7.71	任务七十 通过 VLAN 实现部门间的互通	291
216	3.7.72	任务七十一 通过 VLAN 实现部门间的互通	291
216	3.7.73	任务七十二 通过 VLAN 实现部门间的互通	291
216	3.7.74	任务七十三 通过 VLAN 实现部门间的互通	291
216	3.7.75	任务七十四 通过 VLAN 实现部门间的互通	291
216	3.7.76	任务七十五 通过 VLAN 实现部门间的互通	291
216	3.7.77	任务七十六 通过 VLAN 实现部门间的互通	291
216	3.7.78	任务七十七 通过 VLAN 实现部门间的互通	291
216	3.7.79	任务七十八 通过 VLAN 实现部门间的互通	291
216	3.7.80	任务七十九 通过 VLAN 实现部门间的互通	291
216	3.7.81	任务八十 通过 VLAN 实现部门间的互通	291
216	3.7.82	任务八十一 通过 VLAN 实现部门间的互通	291
216	3.7.83	任务八十二 通过 VLAN 实现部门间的互通	291
216	3.7.84	任务八十三 通过 VLAN 实现部门间的互通	291
216	3.7.85	任务八十四 通过 VLAN 实现部门间的互通	291
216	3.7.86	任务八十五 通过 VLAN 实现部门间的互通	291
216	3.7.87	任务八十六 通过 VLAN 实现部门间的互通	291
216	3.7.88	任务八十七 通过 VLAN 实现部门间的互通	291
216	3.7.89	任务八十八 通过 VLAN 实现部门间的互通	291
216	3.7.90	任务八十九 通过 VLAN 实现部门间的互通	291
216	3.7.91	任务九十 通过 VLAN 实现部门间的互通	291
216	3.7.92	任务九十一 通过 VLAN 实现部门间的互通	291
216	3.7.93	任务九十二 通过 VLAN 实现部门间的互通	291
216	3.7.94	任务九十三 通过 VLAN 实现部门间的互通	291
216	3.7.95	任务九十四 通过 VLAN 实现部门间的互通	291
216	3.7.96	任务九十五 通过 VLAN 实现部门间的互通	291
216	3.7.97	任务九十六 通过 VLAN 实现部门间的互通	291
216	3.7.98	任务九十七 通过 VLAN 实现部门间的互通	291
216	3.7.99	任务九十八 通过 VLAN 实现部门间的互通	291
216	3.7.100	任务九十九 通过 VLAN 实现部门间的互通	291
216	3.7.101	任务一百 通过 VLAN 实现部门间的互通	291

第一章 网络基础知识

1.1 计算机网络及其体系结构

1. 计算机网络的定义

关于计算机网络这一概念的描述，从不同的角度出发可以给出不同的定义。简单来说，计算机网络就是由通信线路互相连接的许多独立工作的计算机构成的集合体。这里强调构成网络的计算机是独立工作的，这是为了和多终端分时系统相区别。

从应用的角度来讲，只要将具有独立功能的多台计算机连接起来，能够实现各计算机之间信息的互相交换，并可以共享计算机资源的系统就是计算机网络。

从资源共享的角度来讲，计算机网络就是一组具有独立功能的计算机和其他设备，以允许用户相互通信和共享计算机资源的方式互联在一起的系统。

从技术角度来讲，计算机网络就是由特定类型的传输介质（如双绞线、同轴电缆和光纤等）和网络适配器互联在一起的计算机，并受网络操作系统监控的网络系统。

综上所述，可以将计算机网络这一概念系统地定义为：计算机网络就是将分布在不同地理位置上的具有独立工作能力或多台计算机、终端及其附属设备用通信设备和通信线路连接起来，并配置网络软件，以实现计算机资源共享的系统。为了能使得计算机资源共享，计算机网络必须实现数据通信功能。

计算机网络技术的应用对当今社会的经济、文化生活都产生着重要影响。当前，计算机网络的功能主要有以下几个方面。

(1) 资源共享

计算机网络最具吸引力的功能是进入计算机网络的用户可以共享网络中各种硬件和软件资源，使网络中各部分的资源互通、分工协作，从而提高系统资源的利用率。

(2) 数据传输

数据传输是计算机网络的基本功能之一，用以实现计算机与终端或计算机与计算机之间

传送各种信息，从而提高了计算机系统的整体性能，也大大方便了人们的工作和生活。

(3) 集中管理

计算机网络技术的发展和运用，已使得现代办公、经营管理等发生了很大的变化。目前，已经有了许多 MIS 系统、OA 系统等，通过这些系统可以将地理位置分散的生产单位或业务部门连接起来进行集中控制和管理，提高工作效率，增加经济效益。

(4) 分布处理

对于综合性的大型问题可以采用合适的算法，将任务分散到网络中不同的计算机上进行分布式处理，以达到均衡使用网络资源、实现分布处理的目的。

(5) 负载平衡

负载平衡是指任务被均匀地分配给网络上的各台计算机。网络控制中心负责分配和检测，当某台计算机负载过重时，系统会自动转移部分工作到负载较轻的计算机中去处理。

(6) 提高安全与可靠性

建立计算机网络后，还可减少计算机系统出现故障的概率，提高系统的可靠性。另外对于重要的资源可将它们分布在不同地方的计算机上。这样，即使某台计算机出现故障，用户在网络上可通过其他路径来访问这些资源，不影响用户对同类资源的访问。

2. 计算机网络的分类

计算机网络的分类标准有很多，可以从覆盖范围、拓扑结构、交换方式、传输介质、通信方式等方面进行分类。根据网络的覆盖范围进行分类，计算机网络可以简单地分为：局域网 (Local Area Network, LAN) 和广域网 (Wide Area Network, WAN)。这种分类方法也是目前网络工程实施过程中运用最多的一种方法。

(1) 局域网

局域网也称为局部网，是指在有限的地理范围内构成的规模相对较小的计算机网络。它具有很高的传输速率 (1~20Mb/s)，其覆盖范围一般不超过几十千米，通常将一座大楼或一个校园内分散的计算机连接起来构成局域网。它的特点是：分布距离近 (通常在 1000~2000m 范围内)；传输速度快；连接费用低；数据传输可靠；误码率低。

(2) 广域网

广域网也称为远程网，它的联网设备分布范围很广，一般从几十千米到几千千米。它所涉及的地理范围可以是市、地区、省、国家，乃至世界范围。广域网是通过卫星、微波、无线电、电话线、光纤等传输介质连接的国家网络和国际网络，它是全球计算机网络的主干网络。广域网一般具有以下几个特点：地理范围没有限制；传输介质复杂；由于长距离的传输，数据的传输速率较低，且容易出现错误，采用的技术比较复杂；是一个公共的网络，不属于任何一个机构或国家。如果从功能上对广域网加以描述，大家会对广域网这个概念有更深刻的理解，思科将广域网定义为连接各个局域网之间的网络。

现今的因特网 (Internet) 是世界上最大的计算机网络，它是由无数的局域网通过广域网联接而成的，是跨越了无数的局域网与广域网的综合型网络。

3. 计算机网络的体系结构

计算机网络实现数据通信功能是一个复杂的过程。为了减少协议设计和调试过程的复杂性,国际标准化组织(ISO)制定了一个层次化的网络通信模型,称为开放系统互联(Open System Interconnection, OSI)参考模型。OSI参考模型是一个逻辑结构,并非一个具体的计算机设备或网络,但是任何两个遵守协议的标准的系统都可以互联通信,这正是“开放”的实际意义。

OSI参考模型采用了分层的方法。所谓分层是一种构造技术,允许开放系统网络用分层次的方式进行逻辑组合。整个通信子系统划分为若干层,每层执行一种明确定义的功能,并由较低层执行附加的功能,为较高层提供服务。

计算机网络执行数据通信的功能就如同我们在生活中寄信一样,寄信这个任务的执行可以看做是在实际生活中的一种典型的层次化结构执行的例子,如图 1-1 所示。

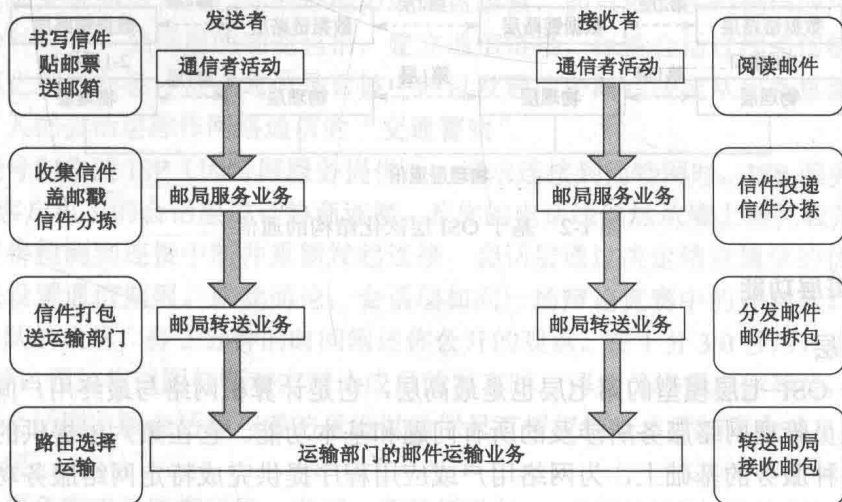


图 1-1 邮局业务分层结构图

OSI参考模型的七层由下往上分别是：第一层物理层（Physical Layer），第二层数据链路层（Data Link Layer），第三层网络层（Network Layer），第四层传输层（Transport Layer），第五层会话层（Session Layer），第六层表示层（Presentation Layer）和第七层应用层（Application Layer）。

OSI参考模型的每一层都定义了所实现的功能,完成某特定的通信任务,并只与紧邻的上层和下层进行数据的交换。图 1-2 简单示意了两个实现了 OSI 七层功能的网络设备之间是如何进行通信的。任务从主机 A 的应用层开始,按规定的格式逐层封装数据,直至数据包到达物理层,然后通过网络传输线路以及中间结点(通常包括交换机,路由器,防火墙等网络互联设备)到达主机 B。主机 B 的物理层获取数据,向上层发送数据,直到到达主机 B 的应用层。本书随后将通过校园网的实例着重介绍如何配置交换机、路由器等网络互联设备,以实现校园网的数据通信,下面简单描述 OSI 参考模型各层的功能。



图 1-2 基于 OSI 层次化结构的通信

4. OSI 每层功能

(1) 应用层

应用层是 OSI 七层模型的第七层也是最高层，它是计算机网络与最终用户间的接口，包含了系统管理员管理网络服务所涉及的所有问题和基本功能。它在第六层提供的数据传输和数据表示等各种服务的基础上，为网络用户或应用程序提供完成特定网络服务功能所需的各种应用层协议。可以简单描述为：应用层应该是用户通过应用层的协议去完成用户想要完成的任务。

例子：如果你想上网，那么你会首先打开浏览器输入网址 <http://www.cisco.com>，如果可以上网的话自动会出现网页画面，网页本身没有在本本地，那怎么可以浏览网页呢？这是因为有了应用层的超文本传输协议（HTTP）来帮助用户与远端的 Web 服务器进行连接且请求传输文件，这样用户就可以通过应用层的协议来完成用户要浏览网页的任务了。

常用的网络服务包括文件服务、电子邮件服务、打印服务、集成通信服务、目录服务、域名解析服务、网络管理、安全和路由互联服务等，如果想要完成类似这样的网络服务都必须通过应用层的协议来完成。

常用的应用层协议有以下几种。

HTTP：超文本传输协议。

FTP：文件传输协议。

TELNET：远程登录。

SNMP：简单网络管理协议。

SMTP：简单邮件传输协议。

NNTP: 网络新闻组传输协议

DNS: 域名解析协议

(2) 表示层

表示层如同应用程序和网络之间的翻译官, 在表示层, 数据将按照网络能理解的方案进行格式化, 这种格式化也因所使用网络的类型不同而不同。表示层管理数据的解密与加密, 如系统口令的处理。如果在 Internet 上查询你的银行账户, 使用的即是一种安全连接。你的账户数据在发送前被加密, 在网络的另一端, 表示层将对接收到的数据解密。除此之外, 表示层协议还对图片和文件格式信息进行解码和编码。

(3) 会话层

会话层负责在网络中的两结点之间建立、维持、终止端与端之间的通信。术语“会话”, 指在两个实体之间建立数据交换的连接, 常用于表示终端与主机之间的通信。所谓终端是指几乎不具有(如果有的话)自己的处理能力或硬盘容量, 而只依靠主机提供应用程序和数据处理服务的一种设备。会话层的功能包括: 建立通信链接, 保持会话过程通信链接的畅通, 同步两个结点之间的对话, 决定通信是否被中断以及通信中断时决定从何处重新发送。你可能常常听到有人把会话层称作网络通信的“交通警察”。

当通过拨号向你的 ISP (因特网服务提供商) 请求连接到因特网时, ISP 服务器上的会话层向你的 PC 客户机上的会话层进行协商连接。若你的电话线偶然从墙上插孔脱落时, 你终端机上的会话层将检测到连接中断并重新发起连接。会话层通过决定结点通信的优先级和通信时间的长短来设置通信期限。就此而论, 会话层如同一场辩论竞赛中的裁判员。例如, 如果你是一个辩论队的成员, 有 2 分钟的时间阐述你公开的观点, 在 1 分 30 秒后, 裁判员将通知你还剩下 30 秒。假如你试图打断对方辩论成员的发言时, 裁判员将要求你等待, 直到轮到你为止。最后, 会话层监测会话参与者的身份以确保只有授权结点才可加入会话。

(4) 传输层

传输层主要负责确保数据可靠、顺序、无差错地从 A 点到传输到 B 点 (A、B 点可能在也可能不在相同的网络段上)。因为如果没有传输层, 数据将不能被接受方验证或解释, 所以, 传输层常被认为是 OSI 模型中最重要的一层。传输协议同时进行流量控制或是基于接收方可接收数据的快慢程度规定适当的发送速率。除此之外, 传输层按照网络能处理的最大尺寸将较长的数据包进行强制分割。例如, 以太网无法接收大于 1500 字节的数据包。发送方结点的传输层将数据分割成较小的数据片, 同时对每一数据片安排一序列号, 以便数据到达接收方结点的传输层时, 能以正确的顺序重组。该过程即被称为排序。

我们再以教室为例来理解排序的过程。假设你提问题, “Jones 女士, 低级的农业耕作技术是如何影响 Dust Bowl 的?”, 但是, Jones 女士接收到信息则是“低级农业耕作技术 Jones 女士? 如何作用于 Dust Bowl? 影响”。在网络中, 传输层发送一个 (应答) 信号以通知发送方数据已被正确接收。如果数据有错, 传输层将请求发送方重新发送数据。同样, 假如数据在一给定时间段未被应答, 发送方的传输层也将认为发生了数据丢失从而重新发送它们。

(5) 网络层

网络层, 即 OSI 模型的第三层, 其主要功能是将网络地址翻译成对应的物理地址, 并决定如何将数据从发送方路由到接收方。

网络层通过综合考虑发送优先级、网络拥塞程度、服务质量以及可选路由的花费来决定从一个网络中结点 A 到另一个网络中结点 B 的最佳路径。在网络中，“路由”是基于编址方案、使用模式以及可达性来指引数据的发送。后续章节将详细解释路由器及其功能。网络层协议还能补偿数据发送、传输以及接收的设备能力的不平衡性。为完成这一任务，网络层对数据包进行分段和重组。分段即是指当数据从一个能处理较大数据单元的网络段传送到仅能处理较小数据单元的网络段时，网络层减小数据单元的大小的过程。这个过程就如同将单词分割成若干可识别的音节，给正学习阅读的儿童使用一样。重组过程即是重构被分段的数据单元。类似地，当一个孩子理解了分开的音节时，他会将所有音节组成一个单词，也就是将部分重组成一个整体。

(6) 数据链路层

数据链路层在物理层和网络层之间提供通信，建立相邻结点之间的数据链路，传送按一定格式组织起来的位组合，即数据帧。帧的格式如图 1-3 所示（以以太网帧结构为例）。本层为网络层提供可靠的信息传送机制，将数据组成适合于正确传输的帧形式。加在帧中包含应答、流控制和差错控制等信息，以实现应答、差错控制、数据流控制和发送顺序控制，确保接收数据的顺序与原发送顺序相同。

目的地址	源地址	类型	数据

图 1-3 帧的格式

(7) 物理层

物理层是 OSI 模型的底层或第一层，主要完成相邻结点之间的比特流的传输。同时本层还定义了一些有关网络的物理特性，包括物理连网媒介，如：电缆连线和连接器。物理层的协议产生并检测电压以便发送和接收携带数据的信号。在你的桌面 PC 上插入网络接口卡，你就建立了计算机连网的基础。换言之，你提供了一个物理层。尽管物理层不提供纠错服务，但它能够设定数据传输速率并监测数据出错率。网络物理问题，如电线断开，将影响物理层。同样，如果你没有将网络接口卡在计算机的电路板中正确安装，计算机也将在物理层出现网络问题。IEEE 已制定了物理层协议的标准，特别 IEEE 802 规定了以太网和令牌环网应如何处理数据。术语“第一层协议”和“物理层协议”，均是指描述电信号如何被放大及通过电线传输的标准。除了不同的传输介质自身的物理特性外，物理层还对通信设备和传输媒体之间使用的接口作了详细的规定，物理层涉及的内容还包括以下几个部分。

① 机械特性。机械特性规定了物理连接所需接插件的规格尺寸、针脚数量和排列情况等。如：EIA RS-232C 标准规定的 D 型 25 针接口，ITU-T X.21 标准规定的 15 针接口等，以太网接口用 RJ-45 水晶头等。

② 电气特性。电气特性规定了在物理信道上传输比特流时信号电平的大小、数据的编码方式、阻抗大小、传输速率和距离限制等，比如：双绞线长度不能大于 100m，RS-232 接口传输距离不大于 15m，最大速率为 19.2kbps。

③ 功能特性。功能特性定义了各个信号线的确切含义，即各个信号线的功能。比如：双绞线每根都有自己的作用。

④ 规程特性。规程特性定义利用信号线进行比特流传输的一组操作规程，是指在物理连接的建立、维护和交换信息时数据通过集线器交换数据顺序。

前面已讲述了七层协议 OSI 参考模型，但是在实际中完全遵从 OSI 参考模型的协议几乎没有。尽管如此，OSI 模型为人们考查其他协议各部分间的工作方式提供了框架和评估基础。下面讲述 TCP/IP 网络协议体系也将以 OSI 参考模型为框架对其作进一步解释。TCP/IP 出现于 20 世纪 70 年代，80 年代被确定为因特网的通信协议。

TCP/IP 体系结构是将多个网络进行无缝连接的体系结构，其结构如图 1-4 所示，其中加入了与 OSI 模型的对照。

TCP/IP 是一组通信协议的代名词，是由一系列协议组成的协议簇。它本身指两个协议集：TCP（传输控制协议）和 IP（互联网络协议）结合而成的。TCP/IP 最早由美国国防高级研究计划局（DARPM）在其 ARPANET 上实现，已有二十几年的运行经验。由于 TCP/IP 一开始用来连接异种机环境，再加上工业界很多公司都支持它，特别是在 UNIX 环境，TCP/IP 已成了其实现的一部分；由于 UNIX 用户的增长，推进了 TCP/IP 的普及。Internet 的迅速发展，使 TCP/IP 已成了事实上的网络互联标准。协议隐藏了通信底层的细节，有利于提高效率。首先程序员与高级协议抽象打交道，不必把精力放在诸如硬件配置等细节问题上；使用高层抽象编制的程序独立于机器结构或网络硬件，可以使任意一对机器进行通信。



图 1-4 TCP/IP 网络体系结构与 OSI 网络参考模型的对比

1.1.1 IP 协议

1. 基本原理

IP 是怎样实现网络互联的？各个厂家生产的网络系统和设备，如以太网、分组交换网等，它们相互之间不能互通，不能互通的主要原因是因为它们所传送数据链路层的基本数据单元（即上文中提到的“帧”）的格式不同。IP 协议实际上是一套由软件程序组成的协议软件，它用各种不同“帧”统一封装“IP 数据包”格，这种 IP 数据包的封装是因特网的一个最重要的特点，使各种计算机都能在因特网上实现互通，即具有“开放性”的特点。

那么，“数据包”是什么？它又有什么特点呢？数据包也是分组交换的一种形式，就是把所传送的数据分段打成“包”，再传送出去。但是，与传统的“连接型”分组交换不同，它属于“无连接型”，是把打成的每个“包”（分组）都作为一个“独立的报文”传送出去，所以叫做“数据包”。这样，在开始通信之前就不需要先连接好一条电路，各个数据包不一定都通过同一条路径传输，所以叫做“无连接型”。这一特点非常重要，它大大提高了网络的坚固性和安全性。

每个数据包都有报头和报文这两个部分，报头中有目的地址等必要内容，使每个数据包不经过同样的路径都能准确地到达目的地。在目的地重新组合还原成原来发送的数据。这就是 IP 具有分组打包和集合组装的功能。

在实际传送过程中，数据包还要能根据所经过网络规定的分组大小来改变数据包的长度，IP 数据包的最大长度可达 65535 字节。

IP 协议中还有一个非常重要的内容，那就是给因特网上的每台计算机和其他设备都规定了一个唯一的地址，叫做“IP 地址”。由于有这种唯一的地址，才保证了用户在连网的计算机上操作时，能够高效而且方便地从千千万万台计算机中选出自己所需的对象来。现在电信网正在与 IP 网走向融合，以 IP 为基础的新技术是热门的技术，如用 IP 网络传送语音的技术（即 VoIP）就很热门，其他如 IP over ATM、IP over SDH、IP over WDM 等，都是 IP 技术的研究重点。

2. IPv4 地址

所谓 IP 地址就是给每个连接在 Internet 上的主机分配的一个 32bit 地址。

按照 TCP/IP 协议规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，比特换算成字节，就是 4 个字节。例如一个采用二进制形式的 IP 地址是“0000101000000000000000000000 0001”，这么长的地址，人们处理起来很费劲。为了方便人们的使用，IP 地址经常被写成十进制的形式，中间使用符号“.”分开不同的字节。于是，上面的 IP 地址可以表示为“10.0.0.1”。IP 地址的这种表示法叫做“点分十进制表示法”，这显然比 1 和 0 容易记忆得多。

有人会以为，一台计算机只能有一个 IP 地址，这种观点是错误的。我们可以指定一台计算机具有多个 IP 地址，因此在访问互联网时，不要以为一个 IP 地址就是一台计算机；另外，通过特定的技术，也可以使多台服务器共用一个 IP 地址，这些服务器在用户看起来就像一台主机似的。

将 IP 地址分成网络号和主机号两部分，设计者就必须决定每部分包含多少位。网络号的位数直接决定了可以分配的网络数（计算方法 $2^{\text{网络号位数}}$ ）；主机号的位数则决定了网络中最大的主机数（计算方法 $2^{\text{主机号位数}}-2$ ）。然而，由于整个互联网所包含的网络规模可能比较大，也可能比较小，设计者最后聪明地选择了一种灵活的方案：将 IP 地址空间划分成不同的类别，每一类具有不同的网络号位数和主机号位数。

IP 地址是 IP 网络中数据传输的依据，它标识了 IP 网络中的一个连接，一台主机可以有多个 IP 地址。IP 分组中的 IP 地址在网络传输中是保持不变的。

(1) 基本地址格式 (IPv4)

现在的 IP 网络使用 32 位地址，以点分十进制表示，如 192.168.0.1。

地址格式为：

IP 地址=网络地址+主机地址 或 IP 地址=网络地址+子网地址+主机地址。

网络地址是因特网协会的 ICANN (the Internet Corporation for Assigned Names and Numbers) 分配的，下有负责北美地区的 InterNIC、负责欧洲地区的 RIPENIC 和负责亚太地区的 APNIC，目的是为了保证网络地址的全球唯一性。主机地址是由各个网络的系统管理员分配的。因此，网络地址的唯一性与网络内主机地址的唯一性确保了 IP 地址的全球唯一性。