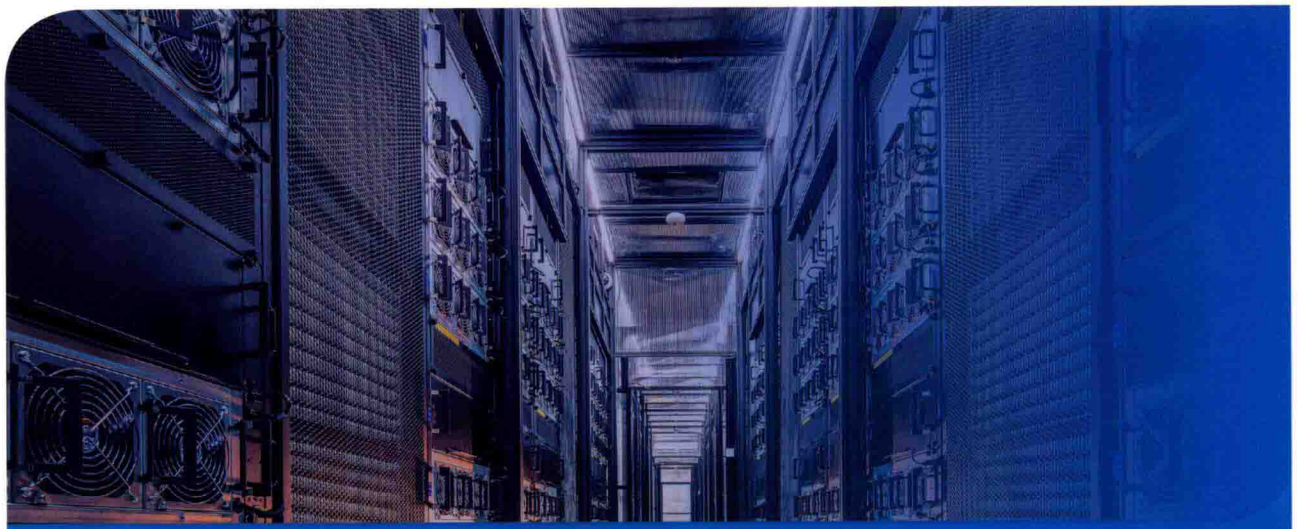
Ruijie Networks 锐捷网络学院系列教程

NETWORK
INTERCONNECTION TECHNOLOGY



网络互联技术
理论篇

汪双顶 武春岭 王津 / 主编
饶绪黎 李建林 / 副主编
余明辉 安淑梅 / 主审

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

Ruijie Networks 锐捷网络学院系列教程

NETWORK INTERCONNECTION TECHNOLOGY

网络互联技术

理论篇

汪双顶 武春岭 王津／主编
饶绪黎 李建林／副主编
余明辉 安淑梅／主审

人民邮电出版社
北京

图书在版编目（CIP）数据

网络互联技术. 理论篇 / 汪双顶, 武春岭, 王津主编. -- 北京 : 人民邮电出版社, 2017.7
锐捷网络学院系列教程
ISBN 978-7-115-43507-1

Ⅰ. ①网… Ⅱ. ①汪… ②武… ③王… Ⅲ. ①互联网络－高等学校－教材 Ⅳ. ①TP393.4

中国版本图书馆CIP数据核字(2016)第243363号

内 容 提 要

本书介绍了构建企业网络工程项目过程中涉及的以太网、交换、路由、安全及无线局域网等方面的专业技术，具体包括网络基础协议、交换机安装和调试、虚拟局域网（VLAN）、生成树、静态路由、动态路由、PPP、交换机端口安全、IP ACL、NAT、WLAN及网络规划等内容，可与《网络互联技术（实践篇）》配套使用。

本书具备专业性、实用性、易读性，不仅可以作为计算机及其相关专业学习网络组网课程的教材，还被选为锐捷网络工程师（Ruijie Certified Network Associate，RCNA）认证配套用书。同时，还可作为网络工程师、系统集成工程师相关技术人员的参考及培训用书。

◆ 主　　编　汪双顶　武春岭　王　津
副 主 编　饶绪黎　李建林
主　　审　余明辉　安淑梅
责任编辑　桑　珊
执行编辑　左仲海
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：20.5　　2017年7月第1版
字数：478千字　　2017年7月河北第1次印刷

定价：49.80元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字20170147号

前言 FOREWORD

随着全球信息化浪潮的到来，建立以网络为核心的工作、学习及生活方式，成为未来发展的趋势。小到一个家庭，大到一所高校、一个企业甚至一个集团。为了提高工作效率，都已经把很多的学习、工作、生活转移到网络这个平台上，建立以网络为核心的人际沟通交流及协作方式。统一网络平台建设，为企业网络内部各部门实现内部信息共享、协同办公提供便利条件。

建立以互联网为中心的全新生活方式，就需要构建互联互通的企业网络。企业网的业务覆盖到金融、企业、教育、政府、医疗、酒店及运营商等领域；企业网构建的技术涉及交换、路由、安全、无线网、网络出口设计及广域网接入等几大类。

● 本书目标

本书详细介绍了企业网构建过程中，所涉及的网络规划、交换、路由、安全、无线以及广域网，网络接入等领域的专业技术，包括 TCP/IP、VLAN、STP/RSTP/MSTP、RIP、OSPF、PPP、ACL、WLAN、网络出口设计等。帮助读者了解网络基础协议知识和网络建设相关技术，掌握网络设备的配置调试方法，了解网络故障的排除思路，帮助读者进行网络建议技术的积累，以便在实际工作中恰当地运用这些技术，解决实际网络建设中遇到的各种问题。

全书的每一个单元都以一个来自生活中真实网络场景开始，以来自网络厂商的一个真实的网络构建的案例为依托，描述相关技术在企业建构中发生的对应场景，绘制网络拓扑，调试设备，排除故障，以方便读者把技术和实际工作对接。为方便读者了解技术的细节，全书每一个单元都详细讲解了构建企业网中使用到的相关知识，包括技术原理、协议的细节及配置案例等。

本书在介绍理论知识和技术原理的同时，还提供了大量的网络项目配置案例，以达到理论和实践相结合的目的。每一单元末的“认证测试”试题，包括了相应章节的重点知识和主要技术点，帮助读者巩固所学的内容，并对学习情况进行测试，以便通过对应的认证考试。

● 本书结构

本书由 15 个学习单元组成，对企业网中使用到的重要技术进行了全面介绍，具体内容包括：

第 1 章　网络基础知识
第 2 章　交换技术基础
第 3 章　配置交换机设备
第 4 章　虚拟局域网
第 5 章　局域网中冗余链路
第 6 章　IP 协议及子网规划
第 7 章　三层交换技术
第 8 章　路由和静态路由技术
第 9 章　RIP 路由协议
第 10 章　OSPF 路由协议
第 11 章　DHCP 动态地址获取协议
第 12 章　保护企业网安全
第 13 章　NAT 网络地址转换技术
第 14 章　无线局域网技术
第 15 章　广域网基础

● 课程资源

为保证课程在学校的有效实施，保障课程教学资源的长期提供，如案例提供、新技术更新、新技术学习、课程技术交流和讨论等，本书的研发队伍还专门投入人力和物力，为本书搭建了专门的网络资源共享平台，以保证课程在实施过程中的项目资源的更新、疑难问题的解决、课程实施方案的讨论等一系列内容落实。读者可以访问 http://bbs.ruijie.com.cn，获得配套电子课件、认证测试答案及其他更多的教学资源。

● 课程环境

为顺利实施本课程，除需要对网络有学习的热情之外，还需要具备基本的计算机基础知识。这些基础知识为学习者提供一个良好脚手架，帮助读者理解本书中技术原理，为学习的进阶提供帮助。

为更好地实施课程中提供项目内容，还需要为本课程提供课程实施的环境，再现这些网络工程项目，包括二层交换机、三层交换机、模块化路由器、无线控制器、无线接入 AP 以及若干台测试计算机和双绞线（或制作工具）等。

虽然书中选择的工程项目来自厂商案例，但力求全部的知识诠释和技术选择都具有通用性，并遵循行业内的通用技术标准。全书关于设备的功能描述、接口的标准、技术的诠释、协议的细节分析、命令语法的解释、命令的格式、操作规程、图标和拓扑的绘制方法都使用行业内的标准。

● 职业资格认证

职业资格认证过程，是掌握与特定硬件系统、操作系统或者其他程序相关的知识学习过程，然后通过一系列考试的过程。认证考试通常由厂家或专业组织开发和管理，对于寻找就业机会的人来说，认证是最常见的就业砝码工具；对于雇主而言，职业资格认证是评估雇员工作水平的一种手段。

为提高就业竞争能力，学生在学习结束后，可以参加基于厂商的职业资格认证。证明认证者了解广泛的网络技术，比如理解协议、拓扑结构、网络硬件和具有解决网络疑难问题的能力。本课程对应的职业资格认证有网络管理员、网络工程师厂商认证。每单元学习完成后，本书都提供有一定数量测试题供读者使用，读者也可以到互联网上查找相应测试试题。

● 开发团队

本课程的开发团队主要来自锐捷网络和部分院校一线的专业教师。他们都把各自多年来在网络专业领域中积累的网络教学和技术应用的工作经验，及对网络技术的深刻理解，诠释成书，凝聚成本书的精华。

汪双顶、安淑梅等来自锐捷网络的企业工程师团队，积极发挥他们在企业拥有的项目资源优势，筛选来自厂商的工程项目和最新的技术对接课程中的技术场景和工作场景，把网络行业最新的技术引入到新认证课程中，保证课程和市场的同步。

以武春岭、王津为代表的院校团队，积极发挥其在院校的课程规划及教学一线实施的优势，筛选来自企业的技术和项目，并按照课程实施的难易度，以及学生的接受程度，进行循序渐进的规划，以适合课程方式在院校的落地实施。

在课程开发之初，开发团队工程师和教师们一起仔细研究相关厂商职业认证课程，在总结锐捷网络工程师职业认证之前几个版本内容的基础上，完成了本书的开发。

此外，在本书的编写过程中，还得到了其他一线教师、技术工程师、产品经理等的大力帮助。他们积累了多年来自工程一线工作和教学的经验，为本书的真实性、专业性及在学校教学实施提供了有力的支持。

本书规划、编辑的过程历经近两年的时间，前后经过多轮的修订，内容改革力度较大，远远超过策划者原先的估计，疏漏之处在所难免，敬请广大读者指正（wangsd@ruijie.com.cn）。本课程在使用时有任何困难，都可以通过此邮件咨询和联系。

创新网络教材编辑委员会

2017 年 4 月

使用说明

在全书关键技术解释和工程方案实施中，会涉及一些网络专业术语和词汇。为方便大家今后在工作中的应用，全书采用业界标准的技术和图形绘制方案。书中相关的符号、网络拓扑图形、命令语法规范约定如下。

- 竖线“|”表示分隔符，用于分开可选择的选项。
- 星号“*”表示可以同时选择多个选项。
- 方括号“[]”表示可选项。
- 大括号“{}”表示必选项。
- 感叹号“!”表示对该行命令解释和说明。
- 斜体字表示需要用户输入的具体值。

以下为本书中所使用的图标示例。


黑客 1


黑客 2


黑客 3


打印机


电话

IP 电话


磁带库


磁盘阵列


防火墙

VPN 网关

IDS 入侵检测系统

IPS 入侵保护系统

目录 CONTENTS

第1章 网络基础知识

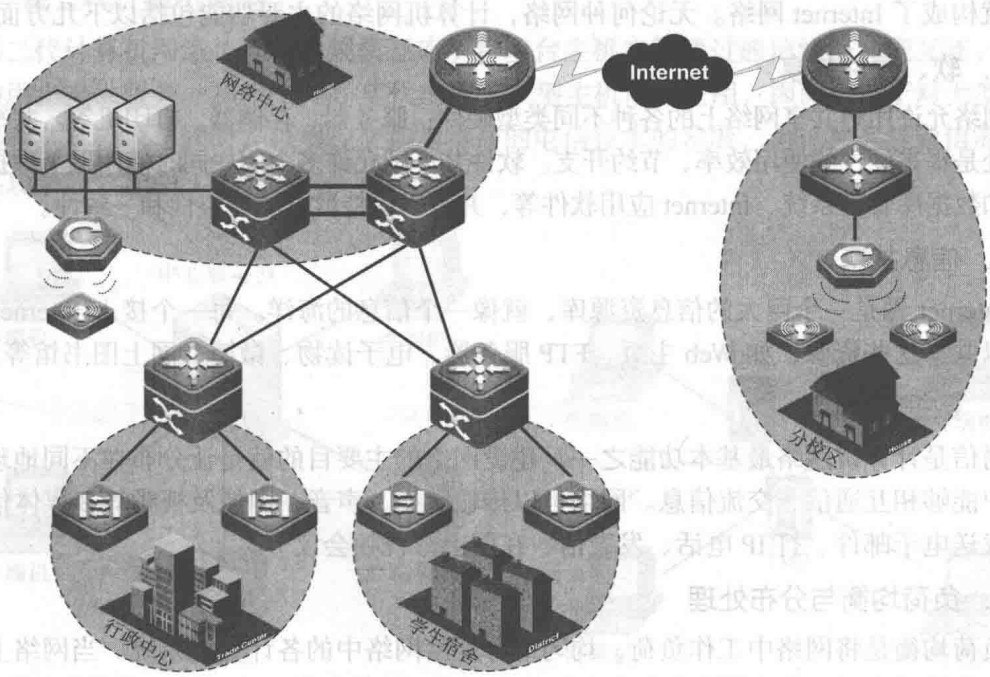
【单元背景】

晓明大学毕业分配到中山大学网络中心，从事学校的校园网管理工作。晓明想了解和学习更多的网络专业知识，但又不知道该从哪儿学起？网络中心的陈工程师告诉晓明说："网络技术学习重在实战，需要多在实际工作中学习、锻炼，但网络基础知识还必须掌握和了解。"

晓明问："哪些是必须掌握的，最基础的网络技术是哪些呢？在最短的时间中，需要掌握哪些基础知识……"

网络中心的陈工程师思索了一会儿，很快列出了以下网络专业基础知识和专业术语。

本单元知识发生在以下网络场景中。



【学习目标】

- 计算机网络发展历史
- 计算机网络分类
- 计算机网络拓扑结构

- 计算机网络体系结构
- OSI 网络体系结构
- TCP/IP 网络体系结构
- 网络组建层次模型

1.1 计算机网络基础

20 世纪 50 年代，计算机网络的诞生引起了人们极大的兴趣。其间，随着计算机技术和通信技术高速发展及相互渗透结合，计算机网络也迅速扩散到日常生活的各个领域，政府、军队、企业和个人都越来越多地将自己的重要业务依托于网络运行，越来越多的业务和信息都通过网络来传输。

在信息化社会中，计算机网络对信息的收集、传输、存储和处理起着非常重要的作用，对已经到来的信息社会都有着极其深刻的影响。

1.1.1 计算机网络概述

计算机网络通过使用双绞线、同轴电缆或光纤等有线通信介质，或使用微波、卫星等无线媒体，把地理上分散的多台计算机系统连接起来，并通过网络中的协议进行通信，实现资源共享的计算机系统集合。

两台计算机连接起来可以组成一个最简单的对等网络；通过光纤把全世界计算机连接起来就构成了 Internet 网络。无论何种网络，计算机网络的主要功能包括以下几方面。

1. 软、硬件共享

网络允许用户共享网络上的各种不同类型硬件：服务器、存储器、打印机等。共享硬件的好处是提高硬件的使用效率、节约开支。软件共享则允许多个用户同时使用网上数据和软件，如数据库管理系统、Internet 应用软件等，并可以保持数据的完整性和一致性。

2. 信息共享

Internet 网是一个巨大的信息资源库，就像一个信息的海洋。每一个接入 Internet 用户都可以共享这些资源，如 Web 主页、FTP 服务器、电子读物、微博、网上图书馆等。

3. 数据通信

通信是计算机网络最基本功能之一，建设网络的主要目的就是让分布在不同地理位置的用户能够相互通信、交流信息。网络可以传输数据、声音、图像及视频等多媒体信息，可以发送电子邮件、打 IP 电话、发微信、在网上开视频会议等。

4. 负荷均衡与分布处理

负荷均衡是将网络中工作负荷，均匀地分配给网络中的各计算机系统。当网络上某台主机的负荷过重时，通过网络应用程序的控制，可以将任务分配给网络上其他计算机处理，充分发挥网络系统上各台主机的作用。

5. 系统的安全与可靠性

网络系统可靠性对于军事、金融和工业过程控制等部门应用特别重要。计算机通过网络中冗余部件，可大大提高可靠性。例如，工作中一台机器出了故障，可以使用网络中另一台

机器替代；网络中一条通信线路出现故障，可以取道另一条线路，从而提高系统整体可靠性。

1.1.2 计算机网络发展历程

20 世纪 50 年代后期，美国半自动地面防空系统（Semi-Automatic Ground Environment，SAGE）开始了计算机技术与通信技术相结合的尝试。在 SAGE 系统中，把远程雷达和其他测控设备，由线路汇集至一台 IBM 大型计算机上进行集中的信息处理。该系统最终于 1963 年建成，被认为是计算机和通信技术结合的先驱。

随着计算机网络技术的蓬勃发展，计算机网络的发展历史大致可划分为如下几个阶段。

1. 第一代计算机网络

20 世纪 50 年代，为了使用计算机系统，将地理上分散的多台无处理能力的终端机（终端是一台计算机外部设备，包括显示器和键盘，无 CPU 和内存）通过通信线路连接到一台中心计算机上，排队等候，待系统空闲时使用计算机，科学工作者们创造了第一代计算机网络系统，如图 1-1 所示。

第一代计算机网络的主要特征是：为了增加系统的计算能力和实现资源共享，分时系统所连接的多台终端连接着中心服务器，这样就可以让多个用户同时使用中心服务器资源。当时计算机网络的定义为“以传输信息为目的而连接起来，以实现远程信息处理或进一步达到资源共享的计算机系统”。

2. 第二代计算机网络

第二代计算机网络（远程大规模互连）将多台主机之间通过通信线路实现互连，为网络中的用户提供服务。20 世纪 60 年代出现了大型主机商业应用，因而也有了对大型主机资源远程共享要求。同时，以程控交换为特征的电信技术的发展，为这种远程通信需求提供了实现手段，如图 1-2 所示。

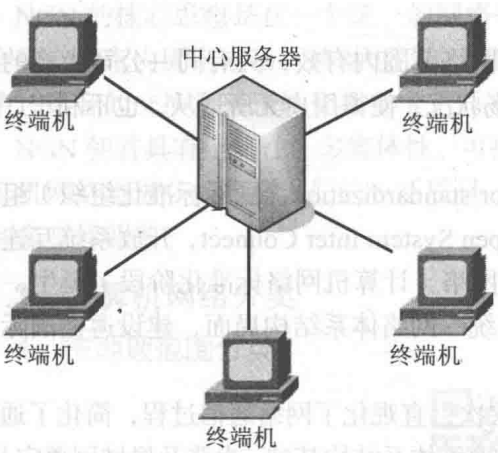


图 1-1 第一代计算机网络

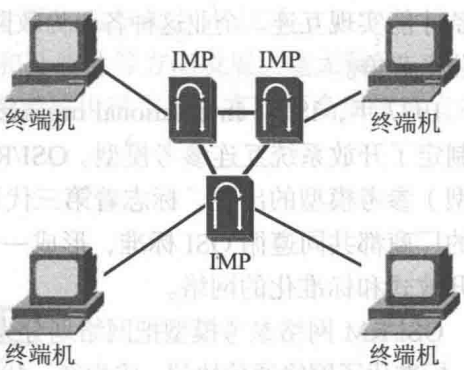


图 1-2 远程大规模互连网络

在这种网络中，主机之间不是直接用线路相连，而由接口报文处理机（Interface Message Processor，简称为 IMP，是路由器的前身）转接后实现互连。互连 IMP 机和通信线路一起负责网络中主机间的通信任务，构成通信子网。接入到通信子网中的互连主机负责运行程序，提供资源共享，组成资源子网。这个时期这种特征网络概念为“以能够相互共享资源

为目的，互连起来的具有独立功能的计算机集合体”。

1969 年，美国国防部高级研究计划局（Defense Advanced Research Projects Agency，DARPA）建成 ARPAnet 实验网。该网络就是 Internet 网的前身，当时该网络只有 4 个节点，以电话线路为主干网络。此后该网络建设的规模不断扩大，到 20 世纪 70 年代后期，网络节点已超过 60 多个，网络的范围连通了美国东部和西部许多大学和研究机构。

20 世纪 70 年代是通信网络大力发展时期，这时的网络都以实现计算机之间远程数据传输和信息共享为主要目的，通信线路大多租用电话线路，少数铺设专用线路。这一时期的网络以远程大规模互连为主要特点，称为第二代网络。

3. 第三代计算机网络

OSI 参考模型

随着计算机网络技术的成熟，网络应用领域越来越广泛，网络规模不断地增大，网络通信技术也变得更加复杂。各大计算机公司纷纷制定出自己公司的网络技术标准。

1974 年，IBM 推出了系统网络结构 SNA（System Network Architecture）标准，为用户提供互连成套通信。

1975 年，DEC（Digitul Equipment Corporation，美国数字设备公司）宣布了数字网络体系结构 DNA（Digital Network Architecture）标准。

1976 年，UNIVAC 也宣布了分布式通信体系结构 DCA（Distributed Communication Architecture）标准。

但这些网络标准都只能在一个公司建设的网络范围内有效，只有同一公司生产的网络设备才能实现互连。企业这种各自为政网络市场状况，使得用户无所适从，也不利于厂商之间公平竞争。

1977 年，ISO（International organization for standardization，国际标准化组织）组织出面制定了开放系统互连参考模型。OSI/RM（Open System Inter Connect，开放系统互连参考模型）参考模型的出现，标志着第三代计算机网络（计算机网络标准化阶段）诞生，即所有的厂商都共同遵循 OSI 标准，形成一个具有统一网络体系结构局面，建设遵循国际标准的开放式和标准化的网络。

OSI/RM 网络参考模型把网络划分为 7 个层次，直观化了网络通信过程，简化了通信原理，标准化了网络通信协议，成为新一代计算机网络体系结构基础，为普及局域网奠定基础。

4. 第四代计算机网络

20 世纪 80 年代，PC 技术、局域网技术发展成熟，出现了光纤及高速网络传输技术。网络就像一个对用户透明的大规模计算机系统，计算机网络获得高速发展。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互连在一起，