



H3C 网络学院系列教程

H3C

路由交换技术

第4卷

杭州华三通信技术有限公司 编著

清华大学出版社



H3C 网络学院系列教程

H3C

路由交换技术

第4卷

杭州华三通信技术有限公司 编著

清华大学出版社
北 京

内 容 简 介

本书详细讲解建设大规模网络所需的安全和优化技术,包括广域网体系结构、宽带接入技术、传统 VPN 技术、安全 VPN 技术、BGP/MPLS VPN、增强网络安全的技术、VoIP、服务质量及开放应用体系架构等。本书的最大特点是理论与实践紧密结合,依托 H3C 路由器和交换机等网络设备精心设计的大量实验,有助于读者迅速、全面地掌握相关的知识和技能。

本书是为网络技术领域的深入学习者编写的。对于大中专院校在校学生,本书是深入探索计算机网络技术领域的好教材;对于专业技术人员,本书是掌握计算机网络工程技术的好向导;对于普通网络技术爱好者,本书也不失为学习和了解网络技术的优秀参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

路由交换技术.第4卷/杭州华三通信技术有限公司编著. —北京:清华大学出版社,2012.5
(H3C 网络学院系列教程)
ISBN 978-7-302-28018-7

I. ①路… II. ①杭… III. ①计算机网络—路由选择—高等学校—教材 ②计算机网络—信息交换机—高等学校—教材 IV. ①TN915.05

中国版本图书馆 CIP 数据核字(2012)第 020628 号

责任编辑:刘 青

封面设计:傅瑞学

责任校对:刘 静

责任印制:王静怡

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:清华大学印刷厂

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:31.5

字 数:797 千字

版 次:2012 年 5 月第 1 版

印 次:2012 年 5 月第 1 次印刷

印 数:1~4000

定 价:80.00 元

产品编号:043792-01

随着互联网技术的广泛普及和应用,通信及电子信息产业在全球迅猛发展起来,从而也带来了网络技术人才需求量的不断增加,网络技术教育和人才培养成为高等院校一项重要的战略任务。

H3C 网络学院(HNC)主要面向高校在校学生开展网络技术培训,培训使用 H3C 网络学院系列培训教程。H3C 网络学院培训教程根据技术方向和课时分为多卷,高度强调实用性和提高学生动手操作的能力。

H3C 网络学院路由交换技术第 4 卷教程在 H3CSE-Routing & Switching 认证培训课程内容基础上进行了丰富和加强,内容覆盖面广,讲解由浅入深,包括大量与实践相关的内容,学员学习后可具备 H3CSE-Routing & Switching 的备考能力。

本书适合以下几类读者。

- 大中专院校在校生:本书既可作为 H3C 网络学院的教科书,也可作为计算机通信相关专业学生的参考书。
- 公司职员:本书能够用于公司进行网络技术的培训,帮助员工理解和熟悉各类网络应用,提升工作效率。
- 网络技术爱好者:本书可以作为所有对网络技术感兴趣的爱好者学习网络技术的自学书籍。

H3C 网络学院路由交换技术第 4 卷内容涵盖当前为多业务网络提供安全优化的网络服务所使用的主流技术,不但重视理论讲解,而且精心设计了相关实验,充分凸显了 H3C 网络学院教程的特点——专业务实、学以致用。通过对本书的学习,学员将能理解大规模、高性能、复杂多业务网络的主要需求和常用技术,掌握如何运用这些技术设计和构建可靠、安全、优化的复杂多业务网络。本课程经过精心设计,结构合理,重点突出,图文并茂,有利于学员快速完成全部内容的学习。

依托 H3C 强大的研发和生产能力,本书涉及的技术都有其对应的产品支撑,能够帮助学员更好地理解 and 掌握知识与技能。本书技术内容都遵循国际标准,从而保证良好的开放性和兼容性。

H3C 网络学院路由交换技术第 4 卷包括 9 篇共 32 章,并附 9 个课程实验。各章及附录内容简介如下。

第 1 篇 安全优化的广域网络概述

本篇共 1 章,主要概述安全优化的广域网络所涉及的主要技术。

第2篇 宽带接入技术

本篇共5章,首先介绍宽带接入技术的基本概念;然后介绍 PPPoE 基本原理及配置,PON 特别是 EPON 技术的关键技术及配置,同时,简要介绍 EPCN 技术;最后介绍 ADSL 及 ADSL2/2+ 技术。

第3篇 传统 VPN 技术

本篇共3章,首先概述 VPN 的基本概念;随后分别讲解 GRE 和 L2TP 两种 VPN 的数据封装格式、数据封装及解封装流程;最后介绍两种 VPN 的主要配置方法,并给出了常见故障的排查方法。

第4篇 安全 VPN 技术

本篇共5章,首先介绍数据安全涉及的包括加解密、完整性、PKI 等基本概念;然后讲解 IPSec VPN 和 SSL VPN 的体系结构及工作原理、IPSec VPN 的配置方法;最后介绍 IPSec 相关的高级应用。

第5篇 BGP/MPLS VPN

本篇共4章,首先介绍 MPLS 的概念、标签及标签分发等技术;然后重点讲解 BGP/MPLS VPN 私网路由及私网标签的传递中涉及的多 VRF 和 MP-BGP 技术,并详细讲解 BGP/MPLS VPN 数据转发流程,BGP/MPLS VPN 的配置和故障排除;最后介绍 BGP/MPLS VPN 的相关扩展技术。

第6篇 增强网络安全性

本篇共5章,介绍网络威胁来源、构建安全网络的关注点及构建安全网络所涉及的主要技术及管理手段。其余内容包括业务隔离、访问控制、认证与授权、攻击防范及病毒防范、事件审计、安全制度管理及设计等。

第7篇 VoIP

本篇共2章,首先介绍普通模拟电话和数字电话系统基本工作原理;然后讲解 VoIP 系统组成及基本呼叫流程;最后介绍 H.323 和 SIP 两种主要的 VoIP 信令的工作原理及配置方法。

第8篇 服务质量

本篇共6章,首先介绍 QoS 基本概念及主要的 QoS 服务模型;然后讲解 DiffServ 服务型流量监管、拥塞管理、拥塞避免等技术原理及配置方法;最后讲解 IP 头压缩、PPP 载荷压缩、LFI 等链路有效性增强技术及配置方法。

第9篇 开放应用体系架构

本篇共1章,首先介绍传统体系结构网络设备所面临的挑战和开放应用体系架构的优越性;然后深入介绍开放应用体系架构主要包括的组件及其之间的关系,详细讲解开放应用体系架构4种工作模式及主要的适用场景;最后介绍联动及管理的概念及实现方式。本篇同时概述开放应用体系架构的典型示例。

附录 课程实验

实验1 配置 GRE VPN

实验2 配置 L2TP VPN

实验3 IPSec VPN 基本配置

实验4 配置 IPSec 保护传统 VPN 数据

实验5 BGP/MPLS VPN 基础

实验6 VoIP 基本配置

实验7 配置流量监管

实验 8 配置拥塞管理

实验 9 配置链路有效性增强机制

为启发读者思考,加强学习效果,本书所附实验均为任务式实验。H3C 授权的网络学院教师可以从 H3C 网站上下载实验的教师参考资料,其中包含了所有实验内容的具体答案。

各型设备和各版本软件的命令、操作、信息输出等均可能有所差别。本书选用 H3C MSR30-20/20-20(Comware V5.20-R1718P13-Standard)路由器作为主要的教学和实验设备。书中有极少量教学内容和实验涉及交换机,选取 S3610(Comware V5.20-R5309)或 S3600V2(Comware V5.20-R2101)交换机均可。若读者采用的设备型号、软件版本等与本书不同,可参考所用设备和版本的相关手册。

由于编者水平有限,加之时间仓促,书中错漏之处在所难免,欢迎读者批评指正。来函可发到本书主编处(E-mail: zhaozhidong@h3c.com)。

H3C 培训中心

2012 年 2 月

第 1 篇 安全优化的广域网络概述

第 1 章 远程网络连接需求	2
1.1 远程连接需求分类	2
1.2 连通性需求	2
1.3 安全性需求	3
1.4 优化性需求	4
本章小结	5
习题和解答	5

第 2 篇 宽带接入技术

第 2 章 宽带接入技术概述	8
2.1 企业网的宽带接入技术需求	8
2.2 宽带接入技术关键概念	8
2.2.1 什么是宽带接入	8
2.2.2 宽带接入模型和基本概念	10
2.3 主要的宽带接入技术	11
2.3.1 宽带接入的传输介质	11
2.3.2 常见的光纤接入模式	12
2.3.3 主要的宽带接入技术及其组网	13
本章小结	14
习题和解答	14
第 3 章 以太网接入	15
3.1 以太网接入的典型应用	15
3.1.1 什么是以太网接入	15
3.1.2 大型园区接入的典型应用	16
3.2 PPPoE 原理及配置	17

3.2.1	PPPoE 原理	17
3.2.2	PPPoE 的配置	20
3.3	以太网接入的局限	22
	本章小结	23
	习题和解答	23
第 4 章	EPON	24
4.1	PON 技术简介	24
4.1.1	什么是 PON 技术	24
4.1.2	PON 的组成结构	25
4.1.3	PON 的标准化过程	26
4.1.4	主要 PON 技术对比	27
4.2	EPON 关键技术	30
4.2.1	EPON 的层次结构	30
4.2.2	EPON 系统的工作过程	31
4.3	EPON 基本配置	37
4.3.1	EPON 系统的端口类型	37
4.3.2	EPON 的基本配置步骤	37
4.3.3	OLT 端口配置	38
4.3.4	ONU 配置	38
4.3.5	UNI 端口配置	41
4.3.6	EPON 典型配置实例	41
	本章小结	42
	习题和解答	43
第 5 章	EPCN	44
5.1	有线电视网络概述	44
5.1.1	什么是 CATV	44
5.1.2	什么是 HFC	45
5.2	有线电视网络的双向传输改造	46
5.2.1	CATV 宽带数据网络需求	46
5.2.2	基于 HFC 网络的 Cable Modem 方案	47
5.2.3	基于以太网的 EoC 技术	49
5.3	EPCN 技术介绍	50
5.3.1	EPCN 系统组成	50
5.3.2	EPCN 传输原理	50
5.3.3	EPCN 的技术优势分析	51
5.3.4	EPCN 典型应用模型	52
	本章小结	54
	习题和解答	55

第 6 章 ADSL	56
6.1 DSL 技术概述	56
6.1.1 DSL 技术的起源	56
6.1.2 DSL 的基本原理	57
6.1.3 DSL 技术分类	58
6.2 ADSL 技术原理和应用	60
6.2.1 ADSL 技术的基本原理	60
6.2.2 ADSL 的上层应用	64
6.3 ADSL 基本配置	68
6.3.1 ADSL 接口的物理参数配置	68
6.3.2 ADSL 的 PPPoEoA 配置	69
6.4 ADSL2/2+ 技术简介	71
6.4.1 ADSL2	71
6.4.2 ADSL2+	76
本章小结	77
习题和解答	77
第 3 篇 传统 VPN 技术	
第 7 章 VPN 概述	80
7.1 企业网对 VPN 的需求	80
7.1.1 传统企业网面临的问题	80
7.1.2 什么是 VPN	81
7.2 VPN 主要概念术语	81
7.3 VPN 分类	82
7.3.1 不同业务用途的 VPN	82
7.3.2 不同运营模式的 VPN	83
7.3.3 按照组网模型分类	84
7.3.4 按照 OSI 参考模型的层次分类	85
7.4 主要 VPN 技术	85
本章小结	86
习题和解答	86
第 8 章 GRE VPN	88
8.1 GRE VPN 概述	88
8.2 GRE 封装格式	89
8.2.1 标准 GRE 封装	89
8.2.2 扩展 GRE 封装	91
8.2.3 IP over IP 的 GRE 封装	92
8.3 GRE 隧道工作流程	93

8.3.1	GRE 隧道构成	93
8.3.2	隧道起点路由查找	94
8.3.3	加封装	95
8.3.4	承载协议路由转发	96
8.3.5	中途转发	96
8.3.6	解封装	96
8.3.7	隧道终点路由查找	97
8.4	部署 GRE VPN 的考虑因素	98
8.4.1	地址空间和路由配置	98
8.4.2	Tunnel 接口 Keepalive	99
8.5	GRE VPN 配置	100
8.5.1	GRE VPN 基本配置	100
8.5.2	GRE VPN 高级配置	101
8.5.3	GRE VPN 信息的显示和调试	101
8.5.4	GRE VPN 配置示例一	102
8.5.5	GRE VPN 配置示例二	103
8.6	GRE VPN 的特点	104
8.6.1	GRE VPN 的优点	104
8.6.2	GRE VPN 的缺点	104
	本章小结	104
	习题和解答	104

第 9 章 L2TP VPN 106

9.1	L2TP VPN 概述	106
9.2	L2TP 工作原理	108
9.2.1	L2TP 概念和术语	108
9.2.2	L2TP 拓扑结构	109
9.2.3	L2TP 协议封装	110
9.2.4	L2TP 协议操作	111
9.2.5	L2TP 验证	113
9.2.6	典型 L2TP 工作过程	114
9.2.7	L2TP 多实例简介	115
9.3	配置独立 LAC 模式	116
9.3.1	独立 LAC 模式配置任务	116
9.3.2	L2TP 基本功能配置	116
9.3.3	LAC 基本配置命令	117
9.3.4	LNS 基本配置命令	117
9.3.5	高级配置命令	118
9.3.6	配置示例	118
9.4	用 iNode 客户端实现客户 LAC 模式	120
9.4.1	iNode 客户端介绍	120

9.4.2 客户 LAC 模式配置任务	120
9.4.3 客户 LAC 模式配置示例	120
9.5 L2TP 信息显示和调试	123
9.6 L2TP 的特点	123
本章小结	124
习题和解答	124

第 4 篇 安全 VPN 技术

第 10 章 数据安全技术基础	126
10.1 概念和术语	126
10.2 数据加解密	127
10.2.1 加解密简介	127
10.2.2 对称密钥加密	128
10.2.3 非对称密钥加密	129
10.2.4 组合加解密技术	130
10.3 数据完整性	131
10.4 数字签名	132
10.5 数字证书	133
10.6 公钥基础设施 PKI	134
10.6.1 PKI 概述	134
10.6.2 PKI 工作过程	135
10.6.3 配置 PKI	136
本章小结	138
习题和解答	138
第 11 章 IPSec 基本原理	140
11.1 IPSec VPN 概述	140
11.2 IPSec 体系结构	141
11.2.1 IPSec 体系概述	141
11.2.2 隧道模式和传输模式	141
11.2.3 IPSec SA	142
11.2.4 IPSec 包处理流程	143
11.3 AH	144
11.3.1 AH 头格式	144
11.3.2 AH 封装	145
11.3.3 AH 处理机制	145
11.4 ESP	146
11.4.1 ESP 头和尾格式	146
11.4.2 ESP 封装	147
11.4.3 ESP 处理机制	148

11.5	IKE	149
11.5.1	IKE 与 IPSec 的关系	149
11.5.2	IKE 协商的两个阶段	150
11.5.3	Cookie	150
11.5.4	IKE 主模式	150
11.5.5	IKE 野蛮模式	151
11.5.6	IKE 的优点	152
	本章小结	152
	习题和解答	153
第 12 章	配置 IPSec	154
12.1	配置前准备	154
12.2	配置 IPSec VPN	154
12.2.1	IPSec VPN 配置任务	154
12.2.2	配置安全 ACL	155
12.2.3	配置安全提议	155
12.2.4	理解安全策略	156
12.2.5	配置手工配置参数的安全策略	157
12.2.6	配置 IKE 协商参数的安全策略	158
12.2.7	在接口上应用安全策略	160
12.2.8	IPSec 的信息显示与调试维护	160
12.3	IKE 的配置	161
12.3.1	IKE 配置任务	162
12.3.2	理解 IKE 提议	162
12.3.3	配置 IKE 提议	162
12.3.4	配置 IKE 对等体	163
12.3.5	IKE 的信息显示与调试维护	165
12.4	IPSec 隧道配置示例	166
12.4.1	IPSec+IKE 预共享密钥方法配置示例	166
12.4.2	IPSec+IKE RSA 签名方法配置示例	167
12.4.3	IPSec+IKE 野蛮模式配置示例	168
	本章小结	169
	习题和解答	169
第 13 章	IPSec 高级应用	171
13.1	IPSec 隧道嵌套	171
13.2	IPSec 与传统 VPN 技术结合	172
13.2.1	GRE over IPSec	172
13.2.2	L2TP over IPSec	174
13.3	用 IPSec 保护组播	176
13.4	NAT 穿越	176

13.5	IPSec 高可靠性	179
13.5.1	IPSec 的黑洞问题	179
13.5.2	IKE Keepalive 机制	180
13.5.3	配置 IKE Keepalive	180
13.5.4	DPD 机制	181
13.5.5	配置 DPD	182
	本章小结	182
	习题和解答	182
第 14 章	SSL VPN	184
14.1	SSL 协议简介	184
14.1.1	协议概述	184
14.1.2	记录层	185
14.1.3	握手层	186
14.1.4	握手过程	187
14.2	SSL VPN 概述	190
14.2.1	SSL 与 SSL VPN	190
14.2.2	SSL VPN 运作流程	191
14.3	SSL VPN 功能与实现	193
14.3.1	SSL VPN 系统结构	193
14.3.2	接入方式	193
14.3.3	访问控制	196
14.3.4	静态授权	196
14.3.5	动态授权	197
14.3.6	缓存清除	199
14.4	部署 SSL VPN	199
	本章小结	200
	习题和解答	200

第 5 篇 BGP/MPLS VPN

第 15 章	MPLS 技术基础	202
15.1	MPLS 起源	202
15.2	MPLS 网络组成	203
15.3	MPLS 标签	204
15.3.1	MPLS 标签基本概念	204
15.3.2	MPLS 标签分配协议分类	205
15.3.3	LDP 消息类型	206
15.3.4	标签分配过程	207
15.3.5	标签分配和管理方式	209
15.4	MPLS 转发实现	212

15.5 MPLS 应用与发展	214
本章小结	214
习题和解答	214
第 16 章 BGP/MPLS VPN 基本原理	216
16.1 BGP/MPLS VPN 技术背景	216
16.1.1 传统 VPN 的缺陷	216
16.1.2 BGP/MPLS VPN 的优点	217
16.2 MPLS 隧道技术	217
16.2.1 隧道技术与 MPLS	217
16.2.2 MPLS 隧道技术应用	218
16.2.3 MPLS 倒数第二跳弹出	220
16.3 多 VRF 技术	221
16.3.1 优化 VPN 组网结构	221
16.3.2 多 VRF 技术实现原理	222
16.4 MP-BGP 技术	225
16.4.1 MP-BGP 技术实现	225
16.4.2 Route Target 属性	227
16.4.3 RD 前缀	229
16.4.4 MPLS 私网 Label	230
16.5 BGP/MPLS VPN 基本原理	230
16.5.1 公网隧道建立	230
16.5.2 本地 VPN 的建立	231
16.5.3 私网路由的学习	232
16.5.4 私网数据的传递	234
本章小结	236
习题和解答	236
第 17 章 BGP/MPLS VPN 配置与故障排除	238
17.1 BGP/MPLS VPN 的配置思路	238
17.2 BGP/MPLS VPN 配置命令	238
17.2.1 配置公网隧道	238
17.2.2 配置本地 VPN	239
17.2.3 配置 MP-BGP	239
17.3 BGP/MPLS VPN 配置示例	239
17.3.1 网络环境和需求	239
17.3.2 配置 BGP/MPLS VPN 公网隧道	240
17.3.3 配置 BGP/MPLS VPN 本地 VPN	241
17.3.4 配置 MP-BGP	243
17.4 BGP/MPLS VPN 故障排查	245
17.4.1 BGP/MPLS VPN 故障排查思路	245

17.4.2 BGP/MPLS VPN 故障排查步骤	245
17.4.3 排查本地 VPN 故障的步骤	247
17.4.4 排查 MP-BGP 故障的步骤	248
本章小结	249
习题和解答	249
第 18 章 BGP/MPLS VPN 技术扩展	251
18.1 BGP/MPLS VPN 基本组网的缺陷	251
18.2 MCE	252
18.3 HOPE	255
18.4 BGP/MPLS VPN 技术扩展	259
本章小结	259
习题和解答	260
 第 6 篇 增强网络安全性	
第 19 章 网络安全概述	262
19.1 网络安全威胁的来源	262
19.2 网络安全范围	264
19.3 安全网络构成	266
本章小结	267
习题和解答	268
第 20 章 业务隔离与访问控制	269
20.1 业务隔离	269
20.1.1 局域网业务隔离	269
20.1.2 广域网业务隔离	269
20.2 访问控制	270
20.3 防火墙技术	271
20.3.1 防火墙技术原理简介	271
20.3.2 状态检测防火墙的常用配置	273
本章小结	275
习题和解答	275
第 21 章 认证与授权	277
21.1 AAA 体系结构	277
21.2 认证授权应用	278
本章小结	279
习题和解答	279
第 22 章 传输安全与安全防护	281
22.1 传输安全	281

22.2	使用 NAT 进行安全防护	282
22.3	网络攻击与防御	282
22.4	病毒防范	285
22.5	设备安全加固	285
	本章小结	286
	习题和解答	287
第 23 章	安全管理	288
23.1	安全管理概述	288
23.2	用户行为管理	288
23.3	安全事件管理	289
23.4	流量管理	290
23.5	安全制度管理	291
	本章小结	291
	习题和解答	292
 第 7 篇 VoIP 		
第 24 章	语音技术基础	294
24.1	电话系统简介	294
24.1.1	基本模拟电话系统组成	294
24.1.2	电话机	295
24.1.3	本地环路	295
24.1.4	PBX 及中继	296
24.1.5	模拟语音接口	296
24.2	呼叫流程及信令	297
24.2.1	呼叫流程	297
24.2.2	信令	298
24.3	模/数转换简介	299
24.4	数字语音传输	300
	本章小结	301
	习题和解答	301
第 25 章	VoIP 基础	302
25.1	VoIP 系统介绍	302
25.1.1	什么是 VoIP	302
25.1.2	VoIP 信令简介	303
25.1.3	语音模/数信号转换	304
25.1.4	主要编码方式	305
25.1.5	封装 IP 语音包	305
25.1.6	语音实体	307

25.1.7	VoIP 基本呼叫过程	307
25.2	H.323 基础	308
25.2.1	H.323 组件	308
25.2.2	H.323 协议族	309
25.2.3	H.225 RAS	310
25.2.4	H.225 呼叫信令	311
25.2.5	H.245 控制信令	311
25.2.6	H.323 呼叫流程	312
25.2.7	H.323 配置示例	314
25.3	SIP 基础	316
25.3.1	SIP 组件	316
25.3.2	SIP 消息	317
25.3.3	SIP 注册及呼叫流程	318
25.3.4	SIP 配置示例	320
本章小结		322
习题和解答		322

第 8 篇 服务质量

第 26 章	QoS 概述	324
26.1	新一代网络面临的服务质量问题	324
26.2	服务质量的衡量标准	324
26.2.1	带宽	324
26.2.2	延迟	325
26.2.3	抖动	325
26.2.4	丢包率	326
26.2.5	常规应用对网络服务质量的要求	327
26.3	QoS 的功能	328
26.3.1	提高服务质量的方法	328
26.3.2	QoS 功能	329
26.4	Best-Effort 模型	329
26.5	DiffServ 模型	329
26.5.1	DiffServ 模型体系结构	330
26.5.2	边界行为	331
26.5.3	无突发令牌桶算法	332
26.5.4	带突发的双令牌桶算法	332
26.5.5	主要标记方法	334
26.5.6	IP Precedence	334
26.5.7	DSCP	335
26.5.8	802.1p CoS	336
26.5.9	MPLS EXP	336