

H3C

H3C 网络学院系列教程

H3C 认证培训指定教材



H3C Comware V7 网络操作系统

路由交换技术

详解与实践 第4卷

新华三大学 / 编著



清华大学出版社

H3C 网络学院系列教程



路由交换技术

详解与实践 第4卷

新华三大学 / 编著

清华大学出版社
北京

内 容 简 介

H3C 网络学院系列教程《路由交换技术详解与实践 第4卷》教材详细讨论了建设大规模网络所需的安全和优化技术,包括安全优化的广域网络概述、宽带接入技术、传统 VPN 技术、安全 VPN 技术、BGP/MPLS VPN、增强网络安全性、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籍。

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

路由交换技术详解与实践. 第4卷/新华三大学编著. —北京:清华大学出版社,2018
(H3C 网络学院系列教程)
ISBN 978-7-302-50515-0

I. ①路… II. ①新… 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(2018)第 138930 号

责任编辑:田在儒
封面设计:王跃宇
责任校对:赵琳爽
责任印制:刘海龙

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 装 者:北京泽宇印刷有限公司

经 销:全国新华书店

开 本:185mm×260mm

印 张:29.75

字 数:779千字

版 次:2018年7月第1版

印 次:2018年7月第1次印刷

定 价:79.00元

产品编号:078671-01

新华三大学培训开发委员会

顾 问 于英涛 尤学军 黄智辉
主 任 李 涛
副主任 李劲松 陈 喆 邹双根 解麟猛

认证培训编委会

陈 喆 曲文娟 张东亮 赵国卫 刘小嘉 陈永波
朱嗣子 酉海华 孙 玥

本书编审人员

主 编 张东亮
参编人员 金 山 翟运波 王继尧 纪合宝
马文斌 张智奇

版权声明

© 2003 2018 新华三技术有限公司(简称新华三)版权所有

本书所有内容受版权法的保护,所有版权由新华三拥有,但注明引用其他方的内容除外。未经新华三事先书面许可,任何人不得将本书的任何内容以任何方式进行复制、经销、翻印、存储于信息检索系统或者其他任何商业目的的使用。

版权所有,侵权必究。

H3C 网络学院系列教程

路由交换技术详解与实践 第4卷

新华三大学 编著

2018年7月印刷

伴随着时代的快速发展,IT 技术已经与人们的日常生活密不可分,在越来越多的人依托网络进行沟通的同时,IT 技术本身也演变成了服务、需求的创造和消费平台,这种新的平台逐渐创造了一种新的生产力和一股新的力量。

新华三是全球领先的新 IT 解决方案领导者,致力于新 IT 解决方案和产品的研发、生产、咨询、销售及服务,拥有 H3C® 品牌的全系列服务器、存储、网络、安全、超融合系统和 IT 管理系统等产品,能够提供包括大互联、大安全、云计算、大数据和 IT 咨询服务在内的一站式、全方位 IT 解决方案。同时,新华三也是 HPE® 品牌的服务器、存储和技术服务的中国独家提供商。

以技术创新为核心引擎,新华三 50% 的员工为研发人员,专利申请总量超过 7200 件,其中 90% 以上是发明专利。2016 年新华三申请专利超过 800 件,平均每个工作日超过 3 件。

2004 年 10 月,新华三的前身——杭州华三通信技术有限公司(简称华三)出版了自己的第一本网络学院教材,开创了业界相关培训教材正式出版的先河,极大地推动了 IT 技术在业界的普及;在后续的几年间,华三陆续出版了《路由交换技术 第 1 卷》《路由交换技术 第 2 卷》《路由交换技术 第 3 卷》《路由交换技术 第 4 卷》等网络学院教材系列书籍,以及《H3C 以太网交换机典型配置指导》《H3C 路由器典型配置指导》《根叔的云图——网络故障大排查》等网络学院参考书系列书籍。

作为 H3C 网络学院技术和认证的继承者,新华三会适时推出新的 H3C 网络学院系列教程,以继续回馈广大 IT 技术爱好者。《路由交换技术详解与实践 第 4 卷》是新华三所推出 H3C 网络学院系列教程的新版本。

相较于以前的 H3C 网络学院系列教程,本次新华三对教材进行了内容更新,以更加贴近业界潮流和技术趋势;另外,本书中的所有实验、案例都可以在新华三所开发的功能强大的图形化全真网络设备模拟软件(HCL)上配置和实践。

新华三希望通过这种形式,探索出一条理论和实践相结合的教育方法,以顺应国家提倡的“学以致用、工学结合”教育方向,培养更多实用型的 IT 技术人员。

希望在 IT 技术领域,这一系列教材能成为一股新的力量,回馈广大 IT 技术爱好者,为推进中国 IT 技术发展尽绵薄之力,同时也希望读者对我们提出宝贵的意见。

新华三大学

培训开发委员会认证培训编委会

2018 年 1 月

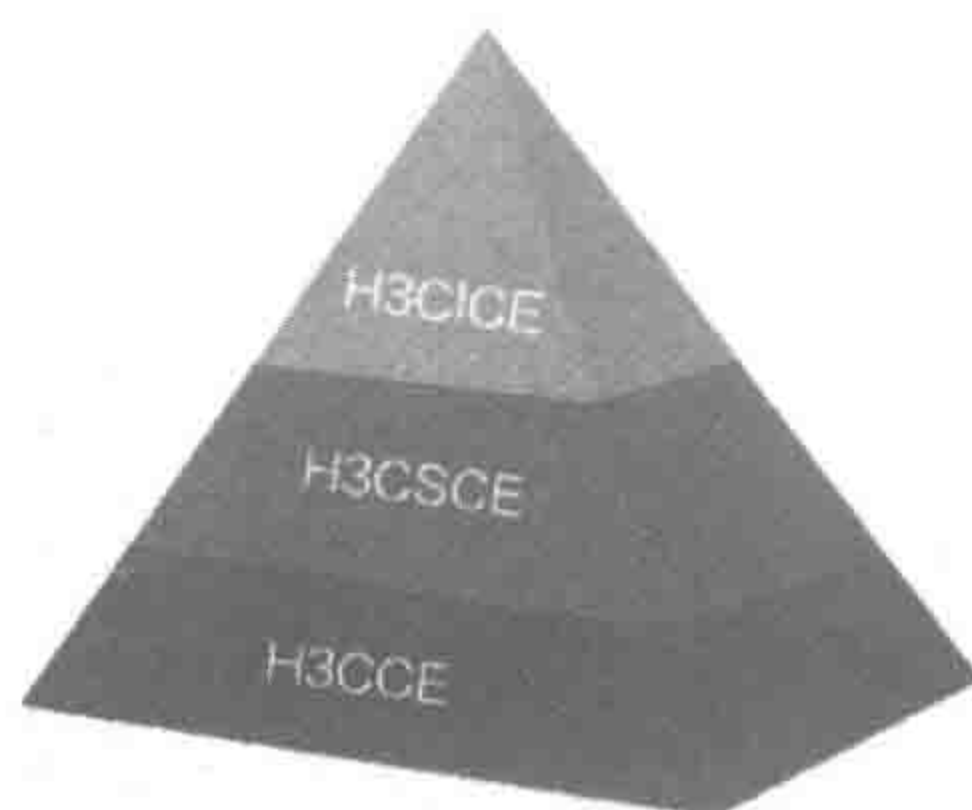
H3C认证简介

H3C 认证培训体系是中国第一家建立国际规范的完整的网络技术认证体系，H3C 认证是中国第一个走向国际市场的 IT 厂商认证。新华三致力于行业的长期增长，通过培训实现知识转移，着力培养高业绩的缔造者。目前在全球拥有 21 家授权培训中心和 450 余家网络学院。截至 2016 年年底，已有 40 多个国家和地区的 25 万人接受过培训，13 万人获得各类认证证书。H3C 认证将秉承“专业务实，学以致用”的理念，快速响应客户需求的变化，提供丰富的标准化培训认证方案及定制化培训解决方案，帮助你实现梦想、制胜未来。

按照技术应用场合的不同，同时充分考虑客户不同层次的需求，新华三为客户提供了从网络助理工程师到网络专家的四级网络认证体系和应运而生的云计算认证体系。



网络认证体系



云计算认证体系

H3C 认证将秉承“专业务实，学以致用”的理念，与各行各业建立更紧密的合作关系，认真研究各类客户不同层次的需求，不断完善认证体系，提升认证的含金量，使 H3C 认证能有效证明你所具备的网络技术知识和实践技能，帮助你在竞争激烈的职业生涯中保持强有力的竞争实力！

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 网络学院的《路由交换技术详解与实践》第 2、3、4 卷教材在 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知识,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:本书可以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《路由交换技术详解与实践 第 4 卷》教材详细讨论了建设大规模网络所需的安全和优化技术,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。本书经过精心设计,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。

依托新华三集团强大的研发和生产能力,教材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。教材技术内容都遵循国际标准,从而保证了良好的开放性和兼容性。

H3C 网络学院《路由交换技术详解与实践 第 4 卷》教材包括 8 篇共 30 章,并附 7 个实验。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,主要概述了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,首先介绍了宽带接入技术的基本概念,其次介绍了 PPPoE 基本原理及配置, PON 特别是 EPON 技术的关键原理及配置,同时,简要介绍了 EPCN 技术。最后介绍了 ADSL 及 ADSL2 /2+ 技术。

第3篇 传统VPN技术

本篇共3章,首先概述了VPN的基本概念,其次分别讲解了GRE和L2TP两种VPN的数据封装格式、数据封装及解封装流程,最后介绍了两种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,首先介绍了数据安全涉及的包括加解密、完整性、PKI等基本概念;其次讲解了IPSec VPN和SSL VPN体系结构及工作原理,IPSec VPN的配置方法;最后介绍了IPSec相关的高级应用。

第5篇 BGP/MPLS VPN技术

本篇共4章,首先介绍了MPLS的概念,标签及标签分发等技术;其次重点讲解了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,并详细讲解了BGP/MPLS VPN数据转发流程,BGP/MPLS VPN的配置和故障排除;最后介绍了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,介绍了网络威胁来源及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。内容包括业务隔离、访问控制、认证授权、攻击防范及防病毒、事件审计、安全制度管理及设计等。

第7篇 服务质量

本篇共6章,首先介绍了QoS基本概念及主要的QoS服务模型,其次讲解了DiffServ服务模型流量监管、拥塞管理、拥塞避免等技术原理及配置方法,最后讲解了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8篇 开放应用体系架构

本篇共1章,首先介绍了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,其次深入介绍了开放应用体系架构主要包括的组件及其之间的关系,再次详细讲解了开放应用体系架构四种工作模式及主要的适用场景,最后介绍了联动和管理的概念及实现方式。本篇同时概述了开放应用体系架构的典型用例。

附录实验

- 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 配置流量监管
- 实验7 配置拥塞管理

为启发读者思考,加强学习效果,本书所附实验为任务式实验。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,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。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。

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 本章目标	2
1.2 远程连接需求分类	2
1.3 连通性需求	2
1.4 安全性需求	3
1.5 优化性需求	4
1.6 本章总结	5
1.7 习题和答案	5
1.7.1 习题	5
1.7.2 习题答案	5

第 2 篇 宽带接入技术

第 2 章 宽带接入技术概述	8
2.1 本章目标	8
2.2 企业网的宽带接入技术需求	8
2.3 宽带接入技术关键概念	9
2.3.1 什么是宽带接入	9
2.3.2 宽带接入模型和基本概念	10
2.4 主要的宽带接入技术	11
2.4.1 宽带接入的传输介质	11
2.4.2 常见的光纤接入模式	12
2.4.3 主要的宽带接入技术及其组网	13
2.5 本章总结	14
2.6 习题和答案	14
2.6.1 习题	14
2.6.2 习题答案	14

第 3 章 以太网接入	15
3.1 本章目标	15
3.2 以太网接入的典型应用	15
3.2.1 什么是以太网接入	15
3.2.2 大型园区接入的典型应用	16
3.3 PPPoE 原理及配置	17
3.3.1 PPPoE 原理	17
3.3.2 PPPoE 的配置	20
3.4 以太网接入的局限	22
3.5 本章总结	22
3.6 习题和答案	23
3.6.1 习题	23
3.6.2 习题答案	23
第 4 章 EPON 技术	24
4.1 本章目标	24
4.2 PON 技术简介	24
4.2.1 什么是 PON 技术	24
4.2.2 PON 的组成结构	25
4.2.3 PON 的标准化过程	26
4.2.4 主要 PON 技术对比	27
4.3 EPON 关键技术	30
4.3.1 EPON 的层次结构	30
4.3.2 EPON 系统的工作过程	31
4.4 EPON 基本配置	37
4.4.1 EPON 系统的端口类型	37
4.4.2 EPON 的基本配置步骤	37
4.4.3 OLT 端口配置	38
4.4.4 ONU 配置	38
4.4.5 UNI 端口配置	41
4.4.6 EPON 典型配置	41
4.5 本章总结	43
4.6 习题和答案	43
4.6.1 习题	43
4.6.2 习题答案	43
第 5 章 EPCN 技术	44
5.1 本章目标	44
5.2 有线电视网络概述	44
5.2.1 什么是 CATV	44

5.2.2	什么是 HFC	45
5.3	有线电视网络的双向传输改造	46
5.3.1	CATV 宽带数据网络需求	46
5.3.2	基于 HFC 网络的 Cable Modem 方案	47
5.3.3	基于以太网的 EoC 技术	49
5.4	EPCN 技术介绍	50
5.4.1	EPCN 系统组成	50
5.4.2	EPCN 传输原理	50
5.4.3	EPCN 的技术优势分析	51
5.4.4	EPCN 典型应用模型	52
5.5	本章总结	54
5.6	习题和答案	55
5.6.1	习题	55
5.6.2	习题答案	55
第 6 章	ADSL 技术	56
6.1	本章目标	56
6.2	DSL 技术概述	56
6.2.1	DSL 技术的起源	56
6.2.2	DSL 的基本原理	57
6.2.3	DSL 技术分类	58
6.3	ADSL 技术原理和应用	60
6.3.1	ADSL 技术的基本原理	60
6.3.2	ADSL 的上层应用	64
6.4	ADSL 基本配置	68
6.4.1	ADSL 接口的物理参数配置	68
6.4.2	ADSL 的 PPPoEoA 配置	69
6.5	ADSL2/2+ 技术简介	71
6.5.1	ADSL2	72
6.5.2	ADSL2+	76
6.6	本章总结	77
6.7	习题和答案	77
6.7.1	习题	77
6.7.2	习题答案	78

第 3 篇 传统 VPN 技术

第 7 章	VPN 概述	80
7.1	本章目标	80
7.2	企业网对 VPN 的需求	80
7.2.1	传统企业网面临的问题	80

7.2.2	什么是 VPN	81
7.3	VPN 主要概念术语	81
7.4	VPN 分类	82
7.4.1	不同业务用途的 VPN	82
7.4.2	不同运营模式的 VPN	83
7.4.3	按照组网模型分类	84
7.4.4	按照 OSI 参考模型的层次分类	85
7.5	主要 VPN 技术	85
7.6	本章总结	86
7.7	习题和答案	86
7.7.1	习题	86
7.7.2	习题答案	87
第 8 章	GRE VPN 技术	88
8.1	本章目标	88
8.2	GRE VPN 概述	88
8.3	GRE 封装格式	89
8.3.1	标准 GRE 封装	89
8.3.2	扩展 GRE 封装	92
8.3.3	IP over IP 的 GRE 封装	92
8.4	GRE 隧道工作流程	93
8.4.1	GRE 隧道构成	93
8.4.2	隧道起点路由查找	95
8.4.3	加封装	95
8.4.4	承载协议路由转发	96
8.4.5	中途转发	96
8.4.6	解封装	97
8.4.7	隧道终点路由查找	97
8.5	部署 GRE VPN 的考虑因素	98
8.5.1	地址空间和路由配置	98
8.5.2	Tunnel 接口 Keepalive	99
8.6	GRE VPN 配置	100
8.6.1	GRE VPN 基本配置	100
8.6.2	GRE VPN 高级配置	101
8.6.3	GRE VPN 信息的显示和调试	101
8.6.4	GRE VPN 配置示例一	102
8.6.5	GRE VPN 配置示例二	103
8.7	GRE VPN 的特点	104
8.7.1	GRE VPN 的优点	104
8.7.2	GRE VPN 的缺点	104
8.8	本章总结	105

8.9	习题和答案	105
8.9.1	习题	105
8.9.2	习题答案	105
第 9 章	L2TP VPN 技术	106
9.1	本章目标	106
9.2	L2TP VPN 概述	106
9.3	L2TP 工作原理	108
9.3.1	L2TP 概念术语	108
9.3.2	L2TP 拓扑结构	109
9.3.3	L2TP 协议封装	110
9.3.4	L2TP 协议操作	111
9.3.5	L2TP 验证	114
9.3.6	典型 L2TP 工作过程	114
9.4	配置独立 LAC 模式	116
9.4.1	独立 LAC 模式配置任务	116
9.4.2	L2TP 基本功能配置	116
9.4.3	LAC 基本配置命令	117
9.4.4	LNS 基本配置命令	117
9.4.5	高级配置命令	118
9.4.6	配置示例	119
9.5	用 iNode 客户端实现客户 LAC 模式	120
9.5.1	iNode 客户端介绍	120
9.5.2	客户 LAC 模式配置任务	121
9.5.3	客户 LAC 模式配置示例	121
9.6	L2TP 信息显示和调试	123
9.7	L2TP 的特点	124
9.8	本章总结	125
9.9	习题和答案	125
9.9.1	习题	125
9.9.2	习题答案	125
第 4 篇 安全 VPN 技术		
第 10 章	数据安全技术基础	128
10.1	本章目标	128
10.2	概念和术语	128
10.3	数据加解密	129
10.3.1	加解密简介	129
10.3.2	对称密钥加密	130
10.3.3	非对称密钥加密	131

10.3.4	组合加解密技术	132
10.4	数据完整性	133
10.5	数字签名	134
10.6	数字证书	135
10.7	公钥基础设施 PKI	136
10.7.1	PKI 概述	136
10.7.2	PKI 工作过程	137
10.7.3	配置 PKI	138
10.8	本章总结	140
10.9	习题和答案	140
10.9.1	习题	140
10.9.2	习题答案	140
第 11 章	IPSec 基本原理	142
11.1	本章目标	142
11.2	IPSec VPN 概述	142
11.3	IPSec 体系结构	143
11.3.1	IPSec 体系概述	143
11.3.2	隧道模式和传输模式	143
11.3.3	IPSec SA	144
11.3.4	IPSec 包处理流程	145
11.4	AH	146
11.4.1	AH 头格式	146
11.4.2	AH 封装	147
11.4.3	AH 处理机制	147
11.5	ESP	148
11.5.1	ESP 头和尾格式	148
11.5.2	ESP 封装	149
11.5.3	ESP 处理机制	150
11.6	IKE	151
11.6.1	IKE 与 IPSec 的关系	151
11.6.2	IKE 协商的两个阶段	152
11.6.3	Cookie	152
11.6.4	IKE 主模式	152
11.6.5	IKE 野蛮模式	153
11.6.6	IKE 的优点	154
11.7	本章总结	154
11.8	习题和答案	155
11.8.1	习题	155
11.8.2	习题答案	155

第 12 章 配置 IPsec	156
12.1 本章目标	156
12.2 配置前准备	156
12.3 配置 IPsec VPN	157
12.3.1 IPsec VPN 配置任务	157
12.3.2 配置安全 ACL	157
12.3.3 配置安全提议	157
12.3.4 理解安全策略	158
12.3.5 配置手工配置参数的安全策略	160
12.3.6 配置 IKE 协商参数的安全策略	161
12.3.7 在接口上应用安全策略	162
12.3.8 IPsec 的信息显示与调试维护	163
12.4 IKE 的配置	164
12.4.1 IKE 配置任务	164
12.4.2 理解 IKE 提议	165
12.4.3 配置 IKE 提议	165
12.4.4 配置 IKE keychain	166
12.4.5 配置本端身份信息	167
12.4.6 配置 IKE profile	167
12.4.7 IKE 的显示信息与调试维护命令	168
12.5 IPsec 隧道配置示例	169
12.5.1 IPsec+IKE 预共享密钥方法配置示例	169
12.5.2 IPsec+IKE RSA 签名方法配置示例	171
12.5.3 IPsec+IKE 野蛮模式配置示例	173
12.6 本章总结	175
12.7 习题和答案	175
12.7.1 习题	175
12.7.2 习题答案	175
第 13 章 IPsec 高级应用	176
13.1 本章目标	176
13.2 IPsec 隧道嵌套	176
13.3 IPsec 与传统 VPN 技术结合	177
13.3.1 GRE over IPsec	177
13.3.2 L2TP over IPsec	180
13.4 用 IPsec 保护组播	182
13.5 NAT 穿越	183
13.6 IPsec 高可靠性	186
13.6.1 IPsec 的黑洞问题	186

13.6.2	IKE Keepalive 机制	187
13.6.3	配置 IKE Keepalive	187
13.6.4	DPD 机制	188
13.6.5	配置 DPD	189
13.7	本章总结	189
13.8	习题和答案	189
13.8.1	习题	189
13.8.2	习题答案	190
第 14 章	SSL VPN 技术	191
14.1	本章目标	191
14.2	SSL 协议简介	191
14.2.1	协议概述	191
14.2.2	记录层	192
14.2.3	握手层	193
14.2.4	握手过程	194
14.3	SSL VPN 概述	197
14.3.1	SSL 与 SSL VPN	197
14.3.2	SSL VPN 运作流程	198
14.4	SSL VPN 功能与实现	200
14.4.1	SSL VPN 系统结构	200
14.4.2	接入方式	200
14.4.3	访问控制	203
14.4.4	静态授权	204
14.4.5	动态授权	204
14.4.6	缓存清除	206
14.5	部署 SSL VPN	206
14.6	本章总结	207
14.7	习题和答案	207
14.7.1	习题	207
14.7.2	习题答案	207

第 5 篇 BGP / MPLS VPN 技术

第 15 章	MPLS 技术基础	210
15.1	本章目标	210
15.2	MPLS 起源	210
15.3	MPLS 网络组成	211
15.4	MPLS 标签	212