



MPLS和VPN 体系结构 (修订版)

MPLS and VPN Architectures

A practical guide to understanding,
designing, and deploying MPLS and MPLS-enabled VPNs

[美] **Ivan Pepelnjak**, CCIE #1354
Jim Guichard, CCIE #2069

著

田果, CCIE #19036
刘丹宁, CCIE #19920
沈铮, CCIE #18738

译

MPLS和VPN 体系结构 (修订版)

MPLS and VPN Architectures

[美] Ivan Pepelnjak, CCIE #1354 著
Jim Guichard, CCIE #2069
田果, CCIE #19036
刘丹宁, CCIE #19920 译
沈铮, CCIE #18738

人民邮电出版社
北 京

图书在版编目 (C I P) 数据

MPLS和VPN体系结构 / (美) 佩佩恩亚克 (Pepelnjak, I.), (美) 吉查德 (Guichard, J.) 著; 田果, 刘丹宁, 沈铮译. -- 2版 (修订本). -- 北京: 人民邮电出版社, 2015. 2

ISBN 978-7-115-38337-2

I. ①M… II. ①佩… ②吉… ③田… ④刘… ⑤沈…
III. ①宽带通信系统—综合业务通信网②虚拟网络—用户通信网 IV. ①TN915.142②TP393.01

中国版本图书馆CIP数据核字 (2015) 第007123号

版 权 声 明

Jim Guichard, Ivan Pepelnjak: MPLS and VPN Architectures, (ISBN: 1587050021)

Copyright © 2001 Cisco Systems, Inc.

Authorized translation from the English language edition published by Cisco Press.

All rights reserved.

本书中文简体字版由美国 Cisco Press 授权人民邮电出版社出版。未经出版者书面许可, 对本书任何部分不得以任何方式复制或抄袭。

版权所有, 侵权必究。

-
- ◆ 著 [美] Ivan Pepelnjak Jim Guichard
译 田 果 刘丹宁 沈 铮
责任编辑 傅道坤
责任印制 张佳莹 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: 800×1000 1/16
印张: 22.25
字数: 479 千字 2015 年 2 月第 2 版
印数: 7 801—10 800 册 2015 年 2 月河北第 1 次印刷

著作权合同登记号 图字: 01-2009-7288 号

定价: 59.00 元

读者服务热线: (010) 81055410 印装质量热线: (010) 81055316

反盗版热线: (010) 81055315

内容提要

本书详细地介绍了 MPLS 技术架构,涵盖了有关 MPLS 的基础理论、拓扑设计、案例研究以及具体配置等多方面的内容,并重点讨论了 MPLS 的一项主要应用:基于 MPLS 的 VPN。书中通过配置案例、推荐的设计方案、部署指南以及案例研究,介绍了 MPLS/VPN 体系结构及其相关机制。

本书分为两个部分,共 15 章。第 1 部分(第 1~第 6 章)介绍了 MPLS 技术的基本概念及其相关配置,包括帧模式 MPLS 操作、信元模式 MPLS 操作、在交换 WAN 媒介中运行帧模式 MPLS、高级 MPLS 主题、MPLS 迁移与配置实例等;第 2 部分(第 7~第 15 章)介绍了基于 MPLS 的 VPN(虚拟专用网),包括实施 VPN 的方式、MPLS/VPN 技术架构、提供商边缘(PE)到客户边缘(CE)的连接方式、高级 MPLS/VPN 拓扑、高级 MPLS/VPN 主题、MPLS/VPN 部署指南、“运营商的运营商”VPN 以及提供商之间的 VPN 解决方案、IP 隧道技术到 MPLS/VPN 解决方案的迁移案例研究等。

本书是学习、设计以及部署 MPLS 和 MPLS/VPN 的技术指导,从架构的角度为 MPLS/VPN 的实施提出深入的问题,并提供相应的解决方案。对于初步接触 MPLS/VPN 的工程师,本书能够为你提供全面而详细的理论讲解;对于 MPLS/VPN 资深工程师而言,本书能够为你的部署工作提供深入而精辟的指导方针。

关于作者

Jim Guichard, Cisco Systems 全球解决方案工程部的资深网络设计顾问。在供职 Cisco 的几年时间里,他参与了多个大型 WAN 和 LAN 网络的设计、实施和规划工作。由于他在设计复杂的网络互连架构方面,拥有广博的专业知识、丰富的实践经验及对技术的深入理解,因此,在面对 MPLS 技术及其部署工作时,他总是能够展现出细致入微的洞察力。读者可以通过以下邮箱与他取得联系: jguichar@cisco.com。

Ivan Pepelnjak, CCIE, NIL 数据通信公司 (<http://www.nil.si>) 技术部的执行理事。NIL 是一家高科技数据通信公司,它主要的业务是在服务提供商技术领域为客户提供优质的服务。

Ivan 拥有 10 年以上的设计、安装、排错及操作大型服务提供商网络、大型企业的 LAN 和 WAN 网络方面的经验。而在上述他参与的网络项目中,有许多都部署了 MPLS/VPN。他还主持设计并成功开发了多项高级 IP 课程,课程的内容涵盖 MPLS/VPN、BGP、OSPF 以及 IP QoS 等。另外,他还撰写了《EIGRP Network Design Solutions》一书,该书已由 Cisco Press 出版发行。

关于技术审稿人

Stefano Previdi，在网络领域打拼 10 年后加盟 Cisco。起初，在技术支持中心担任路由协议领域的专家，后调任 IP 骨干网技术领域的咨询工程师，负责的领域有路由协议及 MPLS 等。自 2000 年起，调 IOS 工程组任 IS-IS 协议的开发工程师。

Dan Tappan，Cisco 公司的著名工程师。在互联网领域有 20 年的工作经验，起初，在 BBN（Bolt、Beranek 和 Newman 公司）负责将 ARPANET 的网络核心协议从 NCP 转换到 TCP。在过去几年，一直担任 Cisco 公司实施 MPLS（标记交换）和 MPLS/VPN 的技术负责人。

Emmanuel Gillain，自 1997 年起供职于 Cisco。于 1998 年获得 CCIE 认证，现任 EMEA 全球电信组（Global Telcom Team）的系统工程师，负责担任全球服务提供商的售前和技术审计负责人。他协助公司从技术的角度判断商业契机，并提供售前和技术支持方面的工作。他于 1995 年获得了五年制电子工程学位，并在法国电信/Global One 公司任职两年。

献辞

愿将本书献给我们的家庭成员。在我们写作本书的时间里，他们无时无刻不在给予我们支持和鼓励。

致谢

在此我们要特别感谢 Cisco Systems 的 Stefano Previdi。他是 MPLS 领域的先驱，正是他向我们介绍了纷繁复杂的 MPLS 架构及其在 Cisco IOS 上的实施方法。他甚至还亲自充当了本书第一版的技术审校，以确保本书不仅通顺正确，而且能够涵盖与 MPLS 相关的各方面内容。

每一个重要的工程都是团队协作的结晶，本书当然也不例外。我们谨在此感谢所有在我们漫长写作过程中向我们提供了帮助的同仁，如本书的开发编辑 Allison Johnson 帮助我们克服了写作过程中的困难；Cisco Press 编辑组的其他成员也为我们提供了帮助；特别需要感谢我们的技术审校 Stefano Previdi、Dan Tappan、Emmanuel Guilan。他们不仅帮助我们修正了错误和疏漏，而且还结合他们在 MPLS 设计实施领域的经验，为我们提出了很多宝贵意见。

最后，如果没有我们家庭成员不断的支持和关爱，本书永无问世之日，其中尤其需要感谢的，是我们两人的妻子，Sadie 和 Karmen。

译者序

MPLS 属于第三代网络架构。但在这个技术日新月异的时代，一个有着十几岁“高龄”的技术却实难被划分进“新技术”的范畴。而这本书写自 MPLS 技术创始之初的前三年，于是，有朋友说，这本书老了。而我本人也曾支持这样的看法。

不过，在翻译过程中，我发现这本以“架构”为名的书实在是老当益壮。它想向读者传递的，更多的是一种理念，而这种理念本身超越了技术的范畴。

技术类书籍，由于旨在解决现实中的问题，因此写作方式总以先抑后扬为主，沿着提出问题、分析问题、解决问题的思路展开叙述。而本书，则将这种方式发挥到了极致。

综观本书，留给我印象最深的，无外乎“although”一词。书中每解决一个问题，便看到一个让步状语从句，立刻提出这种解决方案的缺陷，引出新技术的需求，然后再解决新的问题。其实，这就是“技术”的特点。套用英语中的一句谚语“Where there is a will, there is a way”。而这本书，可以同时为读者呈现 MPLS 环境中的“wills and ways”。

于是，无论是其中提到的方案、问题还是缺陷，都可以在设计、实施服务提供商网络时给读者提供一种思路，一种方法。毕竟，技术都会面临更新换代，即使沿着 IETF、RFC 文档追寻下去，也无外乎是一条解决问题的线索，而这本书则给与 MPLS/VPN 相关的线索套上了服务提供商的实际环境。

而服务提供商的技术，在各种网络技术中更新换代得最慢，这大致是因为主干网必须维持相对的稳定性。前些天，人民邮电出版社的同仁对我说，根据他们从 Jeff Doyle 先生那里得到的回复，他暂时没有更新《TCP/IP 路由技术》（第二卷）的打算，这成就了人民邮电出版社重译第一版的动力。

其实，我个人认为，即使是技术类的书籍，只要不是一本配置大全，更新换代的速度就会相对较慢，介绍“架构”的书尤其如此。对于这类书籍，其实既无法，也不必随技术更新时时更新版本，它传递的信息质量才是最关键的。

佛家《大慧语录》卷二十中言道：“古人云，见月休观指，归家罢问程……归到家了，自然不问程途；见真月了，自然不看指头矣。”

月亮时时在天空中流转盈亏，手指却既不会随动，指月也难以精确。如果人们顺着它的大致方向看到了真月，那么接下来，手指是否还继续随着月亮移动，对于望月人来说，还重要吗？

最后，对人民邮电出版社相关人员的信任表示感谢，尽管他们知道我们对于服务提供商领域并没有太多造诣，依然出于对我们翻译质量和水平的肯定，邀请我们翻译这本 Cisco 技术书籍的经典之作。

译者

2009年5月

目 录

第 1 部分 MPLS 技术和配置

第 1 章 多协议标签交换 (MPLS) 架构

概述3

1.1 基于 IP 转发的扩展性与灵活性3

1.1.1 网络层路由选择范例4

1.1.2 基于 IP 转发的扩展性与 灵活性6

1.1.3 独立转发与控制8

1.1.4 外部路由信息转发8

1.2 多协议标签交换 (MPLS) 入门8

1.2.1 MPLS 架构中的设备分类10

1.2.2 在网络边缘压入标签12

1.2.3 MPLS 数据包转发与标签交换 路径14

1.3 MPLS 的其他应用15

1.4 总结16

第 2 章 帧模式 MPLS 操作19

2.1 帧模式 MPLS 数据层操作21

2.1.1 MPLS 标签栈头部22

2.1.2 帧模式 MPLS 的标签交换24

2.2 帧模式 MPLS 的标签绑定与转发26

2.2.1 LDP/TDP 会话的建立27

2.2.2 标签的绑定与分发29

2.2.3 帧模式 MPLS 网络的收敛31

2.3 倒数第二跳弹出 (PHP, Penultimate Hop Popping)34

2.4 MPLS 与边界网关协议 (BGP) 的 互动36

2.5 总结38

第 3 章 信元模式 MPLS 操作41

3.1 通过 LC-ATM 接口实现控制层的 连通43

3.1.1 在 Cisco IOS 软件中实现 MPLS 控制层的连通性44

3.1.2 在 ATM 交换机上实施控制层45

3.2 在 ATM-LSR 域中转发带标签的 数据包46

3.3 在 ATM-LSR 域中执行标签分配和 分发47

3.3.1 VC 聚合49

3.3.2 ATM 域的收敛51

3.4 总结52

第 4 章 在交换 WAN 媒介中运行帧模式 MPLS55

4.1 帧中继网络中帧模式 MPLS 的 操作55

4.2 通过 ATM PVC 实现帧模式 MPLS 的 操作57

4.3 总结60

第 5 章 高级 MPLS 主题63

5.1 控制标签映射的分发63

5.2 通过以太网封装 MPLS66

5.2.1 IP MTU 路径发现67

5.2.2 以太网交换机及 MPLS MTU69

5.3 MPLS 环路检测与防范	69	6.1 将主干网迁移到帧模式 MPLS 的 解决方案	83
5.3.1 帧模式 MPLS 中的环路检测 和防范	70	6.2 在预迁移阶段对架构进行检查	85
5.3.2 信元模式 MPLS 中的环路检测 和防范	71	6.3 处理内部 BGP 结构	86
5.4 在启用了 MPLS 的网络中进行路由 追踪	75	6.4 将内部链路迁移到 MPLS	88
5.5 启用了 MPLS 网络中的路由汇总	79	6.5 移除多余的 BGP 对等会话	90
5.6 总结	80	6.6 从基于 ATM 的主干网迁移到帧 模式 MPLS	91
第 6 章 MPLS 迁移与配置实例	83	6.7 总结	94

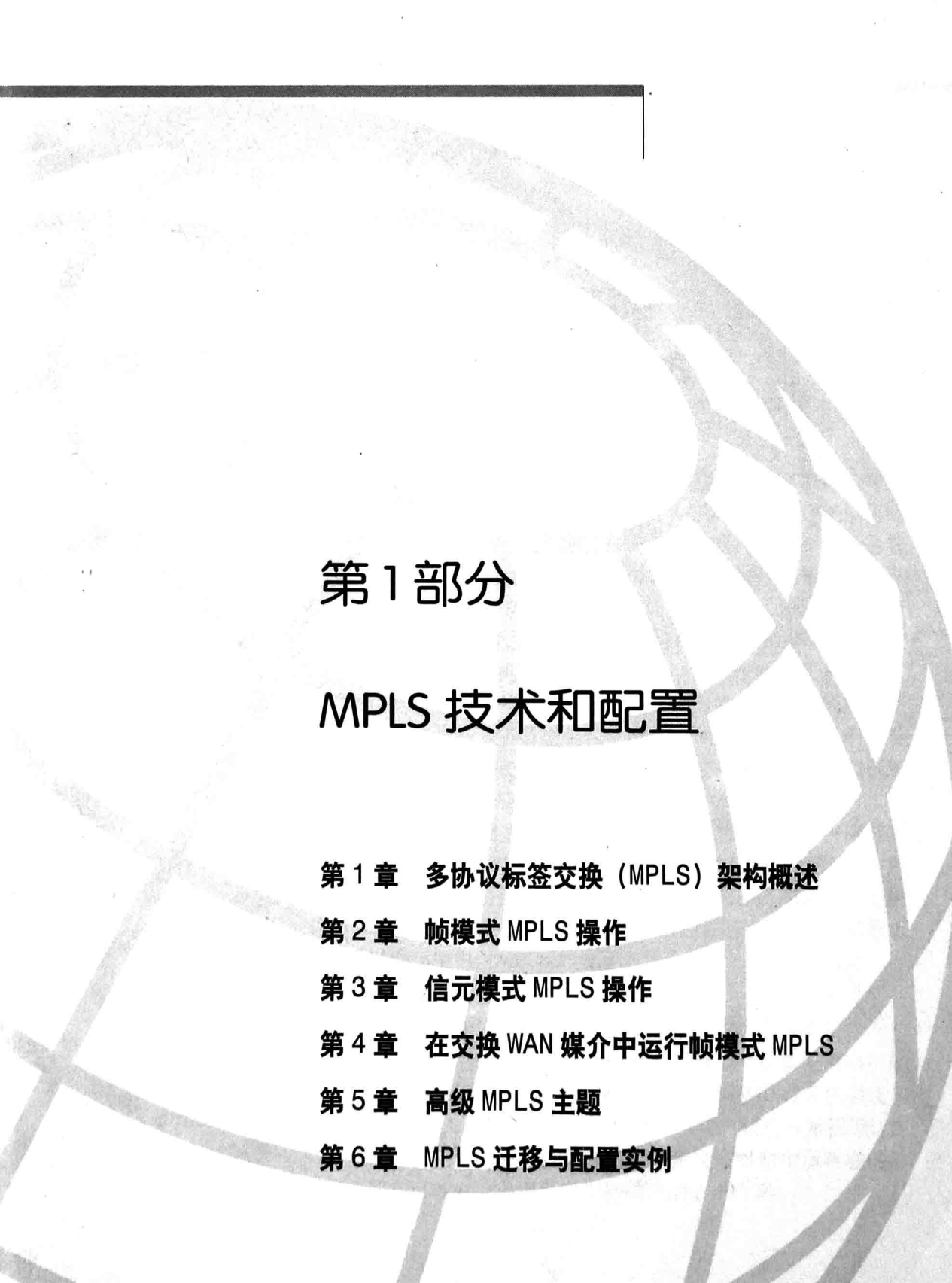
第 2 部分 基于 MPLS 的虚拟专用网

第 7 章 虚拟专用网 (VPN) 实施方案 选项	99	8.3 重叠的虚拟专用网	130
7.1 虚拟专用网的演变	99	8.4 路由目标	133
7.2 基于商业问题的 VPN 分类	102	8.5 提供商网络中 VPN 路由信息的 传递	134
7.3 覆盖 VPN 模型和对等 VPN 模型	103	8.6 VPN 数据包转发	138
7.3.1 覆盖 VPN 模型	104	8.7 总结	140
7.3.2 对等 VPN 模型	106	第 9 章 MPLS/VPN 技术架构的运作 方式	143
7.4 典型 VPN 网络拓扑	110	9.1 案例研究: 基本 MPLS/VPN 内部 网络服务	144
7.4.1 星型拓扑	111	9.2 VRF 配置	145
7.4.2 部分互连或全互连拓扑	113	9.3 路由区别符和 VPN-IPv4 地址 前缀	146
7.4.3 混合拓扑	115	9.4 BGP 扩展团体属性	151
7.4.4 简单企业外部网拓扑	116	9.4.1 路由目标 BGP 扩展团体属性	152
7.4.5 中心服务型企业外部网	117	9.4.2 源站点 BGP 扩展团体属性	154
7.4.6 VPDN 拓扑	119	9.4.3 BGP 扩展团体属性的格式	156
7.4.7 托管网络 VPN 拓扑	120	9.5 基本的 PE 到 CE 链路配置	157
7.5 总结	121	9.5.1 PE 到 CE 链路配置——静态 路由	157
第 8 章 MPLS/VPN 技术架构概述	125		
8.1 案例学习: Supercom 服务提供商 网络中的虚拟专用网	126		
8.2 VPN 路由和转发表	128		

9.5.2 PE 到 CE 链路配置——RIP 版本 2	158	10.8.1 将在其网络中使用 iBGP 的客户 迁移至 MPLS/VPN 服务	196
9.6 接口与 VRF 的关联	160	10.8.2 自治系统号覆盖	198
9.7 多协议 BGP 的使用与部署	160	10.9 总结	199
9.7.1 多协议 BGP 的配置	163	第 11 章 高级 MPLS/VPN 拓扑	203
9.7.2 VPN-IPv4 前缀的增强型 BGP 决策过程	166	11.1 内部网与外部网的集成	203
9.8 出向路由过滤 (ORF) 和路由刷 新特性	168	11.2 中心服务型拓扑	205
9.8.1 PE 路由器上的自动路由 过滤	168	11.3 MPLS/VPN 星型拓扑	208
9.8.2 刷新 PE 路由器之间的路由 信息	169	11.4 总结	211
9.8.3 PE 路由器的 ORF	172	第 12 章 高级 MPLS/VPN 主题	213
9.9 MPLS/VPN 数据层——数据包 转发	173	12.1 MPLS/VPN: 扩展解决方案	214
9.10 总结	174	12.2 MPLS/VPN 网络中的路由收敛	215
第 10 章 提供商边缘 (PE) 到客户边缘 (CE) 的连通性选项	177	12.2.1 服务提供商主干网内的 收敛	216
10.1 将 VPN 客户连接到 MPLS/VPN 主 干网中	177	12.2.2 VPN 站点间的收敛	218
10.2 服务提供商与客户网络之间的 BGP-4	178	12.3 穿越主干网通告路由	222
10.3 PE 路由器与 CE 路由器之间的 OSPF	181	12.3.1 负责承载 VPN-IPv4 和 IPv4 路由信息的 BGP	222
10.4 独立的 VPN 客户路由信息	183	12.3.2 PE 路由器 MP-iBGP 全互连	226
10.5 MPLS/VPN 主干网中 OSPF 路由的 传播	185	12.3.3 分离 PE 路由器之间的 MP-iBGP 会话	227
10.6 PE 到 CE 连通性——使用 OSPF 站点区域 0	188	12.4 使用路由反射器层级	228
10.7 PE 到 CE 连通性——不使用 OSPF 站点区域 0	191	12.4.1 使用 PE 路由的路由反射来 扩展网络	231
10.8 VPN 客户连通性——MPLS/VPN 设计	193	12.4.2 路由反射器分区	231
		12.4.3 在 PE 路由器执行标准的 团体属性过滤	233
		12.4.4 路由反射器上基于属性的路由 目标过滤	236
		12.4.5 路由反射与 ORF 功能	237
		12.5 部署 BGP 联盟	238
		12.5.1 BGP 联盟——单 IGP 环境	243

12.5.2 BGP 联盟——多 IGP 环境	244	13.6 在 MPLS/VPN 主干网中使用 路由跟踪	297
12.6 PE 路由器的规则与扩展	247	13.7 总结	300
12.7 其他连通性需求——Internet 接入	249	第 14 章 运营商的运营商以及提供商 之间的 VPN 解决方案	303
12.8 通过防火墙与 Internet 连接	250	14.1 运营商的运营商解决方案 概述	304
12.9 Internet 接入——静态默认路由	251	14.2 运营商的运营商技术架构—— 拓扑	307
12.10 PE 和 CE 路由器之间分离的 BGP 会话	255	14.2.1 POP 站点中未部署 MPLS 的 ISP	307
12.11 通过动态默认路由建立 Internet 连通性	262	14.2.2 POP 站点中部署 MPLS 的 ISP	312
12.11.1 动态默认路由——路由 目标分配	262	14.3 层级式虚拟专用网	315
12.11.2 将全局路由表与 VRF 进行 关联	264	14.4 提供商之间的 VPN 解决方案	318
12.12 全局路由表中的补充查找 (Additional Lookup)	267	14.4.1 提供商之间的 VPN——跨边界 交换 VPN-IPv4	319
12.13 通过不同服务提供商实现 Internet 连通性	268	14.4.2 提供商之间的 VPN——客户 站点之间的 eBGP 多跳	325
12.14 总结	268	14.5 总结	327
第 13 章 MPLS/VPN 部署指南	271	第 15 章 IP 隧道技术到 MPLS/VPN 的 迁移案例研究	329
13.1 MPLS/VPN 部署简介	271	15.1 现有的 VPN 解决方案部署环境—— IP 隧道技术	330
13.2 客户路由从 IGP 到 BGP 的迁移	271	15.2 为 PE 路由器定义 VPN 和路由 策略	331
13.3 MPLS/VPN 主干网中的多协议 BGP 部署	275	15.3 主干网中的 VRF 定义	332
13.3.1 VPN 路由和下一跳转发	276	15.4 SampleNet VPN 站点的 VRF 和路由 策略	333
13.3.2 PE 路由器环回接口地址 配置	278	15.5 SampleNet Internet 接入的 VRF 和 路由策略	334
13.4 在 LAN 接口部署 MPLS/VPN	284	15.6 Internet 接入客户的 VRF 和路由 策略	335
13.5 客户链路的网络管理	286		
13.5.1 用不同的扩展团体属性通告 路由	287		
13.5.2 使用标准 BGP 团体属性过滤 路由	290		
13.5.3 使用输出映射表以不同的路由 目标通告路由	294		

15.7	MPLS/VPN 迁移——步骤和 实施	335	15.10	将 VPN 站点迁移到 MPLS/VPN 解决方案	341
15.8	BGP 路由反射器上的 MP-iBGP 配置	338	15.11	总结	341
15.9	TransitNet PE 路由器上的 MP-iBGP 配置	340			



第 1 部分

MPLS 技术和配置

第 1 章 多协议标签交换 (MPLS) 架构概述

第 2 章 帧模式 MPLS 操作

第 3 章 信元模式 MPLS 操作

第 4 章 在交换 WAN 媒介中运行帧模式 MPLS

第 5 章 高级 MPLS 主题

第 6 章 MPLS 迁移与配置实例



第 1 章

多协议标签交换 (MPLS) 架构概述

在数据包从源去往目的地的过程中，传统的 IP 数据包转发机制会分析包含在每个数据包网络层头部的目的 IP 地址。网络中每一跳的路由器都会对目的 IP 地址进行独立的分析。无论管理员选择使用动态路由协议还是静态配置，目的都是为了建立一个用来分析目的 IP 地址的数据库（路由表）。因此，人们所实施的传统 IP 路由进程被称为基于目的地的逐跳单播路由。

尽管这种网络机制大获成功并得到了广泛的部署和应用，但它仍然存在着一些限制，这些限制时而进入人们的视野，并且它们的存在降低了数据包转发网络的灵活性。因此人们需要利用一些新的技术来解决这些问题，并对基于 IP 的网络架构所具有的功能进行扩展。

本书第 1 章将着重介绍这些限制，并由此引出一种叫做多协议标签交换 (MPLS) 的全新架构，这种架构可以解除 IP 架构中的一些限制。接下来的章节将会首先关注在纯路由环境中 MPLS 架构的技术细节，然后再对由路由器和 ATM 交换机所组成的混合环境中，MPLS 的技术进行介绍。

1.1 基于 IP 转发的扩展性与灵活性

为使读者理解在传统 IP 数据包转发网络中，影响网络扩展性和灵活性的各类因素，有必要首先对基本的 IP 转发机制及其与下层架构 (LAN 或 WAN) 之间的交互方式进行一番回顾。在搞清楚这些问题之后，读者就可以发现现有机制中所存在的缺陷，并有可能就此得出针对这些缺陷的改进方案。