第一图书网, tushu007.com

<<MPLS和VPN体系结构>>

图书基本信息

书名：<<MPLS和VPN体系结构>>

13位ISBN编号：9787115290533

10位ISBN编号：7115290539

出版时间：2012-10

出版时间：人民邮电出版社

作者：（美）佩佩恩雅克，（美）吉查德，（美）爱普卡　著，孙余强　译

页数：471

字数：665000

译者：孙余强

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

《MPLS和VPN体系结构》(第2版·修订版)在《MPLS和VPN体系结构》(第1卷)的基础上讨论MPLS
VPN技术的最新发展及高级应用。
全书分为4个部分，共9章。
第1部分是引言，简要回顾了MPLS
VPN体系结构；第2部分讲述PE-CE高级互连技术，包括MPLS
VPN远程访问、PE-CE路由协议的增强和高级特性、虚拟路由器组网技术；第3部分讨论了MPLS VPN技术的高级应用，包括MPLS
VPN骨干网安全防护、大规模路由选择技术和多家服务提供商之间的连网技术、多播VPN技术、跨MPLS骨干网传输IPv6流量技术；第4部分探讨了MPLS和MPLS
VPN网络中的故障排除技术。
《MPLS和VPN体系结构》(第2版·修订版)面向中、高级网络技术人员。
对于需要参与高级、大规模MPLS或MPLS
VPN网络的设计、维护与应用的人来说，本书是必读书籍。

作者简介

Ivan Pepelnjak，CCIE
#1354，拥有10年以上设计、安装、维护大型服务商提供网络、大型企业的LAN和WAN网络的经验。
他目前是NIL数据通信公司（www.NIL.si）的首席技术顾问和董事会成员。
他还是许多大获成功的高级IP技术教程的编写者或主要开发者，这些IP技术教程涵盖MPLS/VPN、BGP、OSFP以及IP
QoS技术等。
Jim Guichard，CCIE#2069，Cisco公司Internet技术部门（Internet
Technologies
Division）的第2任技术负责人。
在IBM和Cisco效力的6年里，Jim参加过多项WAN/LAN项目的设计、实施和规划工作。
凭借着广博的专业知识、丰富的项目经验，以及对复杂的Internet网络体系结构的理解，Jim为Cisco的许多大型服务提供商客户提供过有价值的帮助。

Jeff Apcar，Cisco公司亚太地区高级服务团队的高级设计咨询工程师。

他是Cisco公司MPLS技术专家组成员之一，曾为亚太地区的多家服务提供商设计过基于数据包和信元的MPLS网络。
Jeff还设计并维护过500+节点的大型IP路由网络，他对各种网络通信技术都有深入的研究。

书籍目录

第1部分　引言
第1章　MPLS VPN体系结构概述
1.1　MPLS VPN术语
1.2　面向连接型VPN
1.3　无连接型VPN
1.4　基于MPLS的VPN
1.4.1　MPLS术语
1.4.2　MPLS VPN术语
1.5　MPLS VPN的新发展
1.5.1　与MPLS VPN紧密集成的各种接入技术
1.5.2　新路由协议选项
1.5.3　在MPLS上传输的第3层新协议
1.6　小结
第2部分　PE-CE高级互连技术
第2章　MPLS VPN远程访问
2.1　MPLS VPN远程访问增强特性
2.2　接入协议和规程概述
2.2.1　PPP
2.2.2　L2TP
2.2.3　VPDN
2.2.4　RADIUS
2.2.5　DHCP
2.3　拨入MPLS VPN网络
2.3.1　用L2TP VPDN拨入MPLS VPN网络
2.3.2　ISDN直接拨号访问
2.4　通过LSDO提供拨出访问
2.4.1　配置SuperCom San Jose VHG/PE路由器
2.4.2　配置SuperCom San Jose LAC/NAS
2.4.3　SuperCom RADIUS属性
2.4.4　验证VRF感知的LSDO操作
2.4.5　从AAA服务器下载VRF静态路由
2.5　提供非LSDO拨出访问(通过ISDN直接拨号)
2.6　为接入MPLS VPN网络的主用链路，提供拨号备份链路
2.7　通过DSL接入MPLS VPN网络
2.7.1　用RFC 1483 routed(路由式)封装的DSL接入
2.7.2　用RFC 1483 Bridged(桥接式)封装的DSL接入
2.7.3　用PPPoA(ATM上的PPP)封装的DSL接入
2.7.4　通过PPPoE(以太网上的PPP)封装的DSL接入
2.7.5　使用PPPoX和VPDN(L2TP)的DSL访问
2.8　通过Cable(有线电视网)接入MPLS VPN网络
2.8.1　配置SuperCom前置PE路由器
2.8.2　验证Cable接入的运行效果
2.9　MPLS VPN远程访问高级特性
2.9.1　ODAP特性
2.9.2　per-VRF AAA

2.9.3　支持VPN的DHCP中继特性(DHCP Relay: VPN Support)
2.10　小结
第3章　PE-CE路由协议的增强和高级特性
3.1　PE-CE路由协议：OSPF
3.1.1　PE-CE间运行OSPF的需求
3.1.2　PE和CE路由器间OSPF的基本运作方式
3.1.3　更改OSPF router-id
3.1.4　在VRF内监控OSPF的运行情况
3.1.5　用来传递OSPF路由的BGP扩展团体属性
3.1.6　掌控由PE路由器生成的LSA的类型
3.1.7　OSPF站点间的环路预防
3.1.8　VPN客户站点间后门链路
3.2　PE-CE路由协议：集成的IS-IS
3.2.1　PE-CE间运行IS-IS的需求
3.2.2　隔离IS-IS VPN路由信息
3.2.3　通过多协议BGP传播IS-IS路由
3.2.4　在PE-CE路由器间运行level 1-2模式
3.2.5　在PE-CE路由器间运行level 2模式
3.2.6　在PE-CE路由器间运行level 1模式
3.2.7　预防IS-IS站点间的路由环路
3.3　PE-CE路由协议：EIGRP
3.3.1　在PE-CE间运行EIGRP的需求
3.3.2　隔离EIGRP VPN路由信息
3.3.3　用多协议BGP传播EIGRP路由
3.3.4　EIGRP路由BGP扩展团体属性
3.3.5　EIGRP-VRF路由类型
3.4　小结
第4章　虚拟路由器组网技术
4.1　CE路由器上虚拟路由器的配置
4.1.1　在虚拟路由器场景中运行OSPF
4.1.2　在虚拟路由器场景中运行BGP
4.1.3　复杂的虚拟路由器设置
4.2　将虚拟路由器连接至MPLS VPN骨干网
4.2.1　重温GRE
4.2.2　MPLS VPN网络中的GRE隧道
4.2.3　通过GRE隧道将multi-VRF CE路由器接入MPLS VPN骨干网
4.2.4　在EuroBank European站点内部署GRE隧道，实现multi-VRF功能
4.3　根据源IP地址选择VRF
4.3.1　VRF选择特性在EuroBank网络中的应用
4.3.2　规划VPN流量的回程路径
4.4　虚拟路由器网络环境中NAT的应用
4.4.1　重温NAT
4.4.2　PE路由器的NAT配置
4.4.3　用PE-NAT实现公共服务的访问
4.4.4　在共享防火墙的网络环境中启用PE-NAT功能
4.5　小结
第3部分　高级部署场景

第一图书网, tushu007.com

第5章　MPLS VPN骨干网安全防护
5.1　MPLS与生俱来的安全能力
5.1.1　地址空间隔离
5.1.2　屏蔽核心网络
5.1.3　防标签欺骗
5.2　邻居认证
5.2.1　PE和CE间认证
5.2.2　PE间认证
5.2.3　P网络认证
5.3　CE间认证
5.4　严控注入VRF的路由
5.4.1　使用RIPv2作为PE/CE路由协议
5.4.2　用多协议BGP交换VPNv4路由
5.4.3　用eBGP作为PE/CE路由协议
5.4.4　用OSPF作为PE/CE路由协议
5.5　PE与CE互连电路
5.6　外联网访问
5.7　Internet访问
5.7.1　遵循默认路由的共享式Internet访问模式
5.7.2　防火墙托管(Co-Location)
5.7.3　遵循全局路由表的hub-and-spoke(中心和分支)型Internet访问模式
5.7.4　部署具备防火墙功能的CE路由器
5.8　MPLS上的IPSec
5.9　小结
第6章　大型网络路由选择技术和多家服务提供商之间的连网方式
6.1　大型网络路由选择：运营商的运营商解决方案概述
6.2　运营商(Carrier)骨干网连通性
6.2.1　在VPN站点间交换内部路由
6.2.2　CSC PE和CE路由器间路由信息的交换方式
6.2.3　VPN站点间外部路由的交换方式
6.3　在PE/CE链路上运行标签分发协议
6.3.1　LDP发现：传输地址的用法
6.3.2　CSC PE和CE路由器之间的标签分发
6.3.3　CSC CE路由器上静态默认路由的配置
6.4　在PE/CE路由器之间运行BGP-4
6.5　分层VPN：运营商的运营商MPLS VPN
6.6　接入多家服务提供商的VPN间的连通性
6.6.1　提供商间的连通性要求
6.6.2　背靠背VRF解决方案
6.6.3　跨ASBR-ASBR链路通告路由
6.6.4　外部多协议BGP
6.6.5　外部MP-BGP VPNv4路由交换
6.6.6　用来交换VPNv4前缀的多跳多协议eBGP
6.6.7　路由反射器间的多跳多协议eBGP
6.6.8　在路由反射器上更改BGP路由的下一跳
6.6.9　用来交换BGP路由下一跳的IPv4+标签能力
6.7　小结

第一图书网, tushu007.com

第7章　多播VPN
7.1　IP多播概述
7.1.1　源树
7.1.2　共享树
7.1.3　多播转发
7.1.4　RPF
7.1.5　PIM
7.2　在服务提供商网络环境中开展企业网多播业务
7.2.1　mVPN体系结构
7.2.2　多播域概述
7.2.3　多播VRF
7.2.4　PIM邻接关系
7.3　MDT
7.3.1　默认MDT
7.3.2　数据MDT
7.3.3　MTI
7.3.4　RPF检查
7.3.5　多协议BGP MDT更新消息及SSM
7.3.6　mVPN的多播状态标志
7.3.7　mVPN多播流量的转发
7.4　SuperCom网络mVPN业务实例研究
7.4.1　PIM SM之于SuperCom网络
7.4.2　在VRF内启用多播功能
7.4.3　多播隧道接口
7.4.4　多播分发树
7.4.5　mVRF PIM邻接关系
7.4.6　mVRF多播路由表项
7.4.7　数据MDT操作
7.4.8　SSM之于SuperCom核心网络
7.5　小结
第8章　跨MPLS骨干网传输IPv6流量
8.1　IPv6的商业驱动
8.2　在现有网络中IPv6的部署
8.3　IPv6简介
8.3.1　IPv6编址
8.3.2　IPv6邻居发现
8.3.3　IPv6路由选择
8.3.4　Cisco IOS的IPv6配置
8.4　探究6PE的运作方式和配置方法
8.4.1　在PE和CE路由器间交换IPv6路由
8.4.2　建立MP-BGP会话/执行路由重分发
8.4.3　被标记的IPv6 MP-BGP前缀
8.4.4　穿越MPLS骨干网，转发IPv6流量
8.5　复杂的6PE部署场景
8.5.1　BGP路由反射器
8.5.2　在启用了BGP联盟的网络中部署6PE
8.5.3　自治系统间(inter-AS)的6PE部署

8.6　小结
第4部分　故障排除
第9章　排除MPLS网络故障
9.1　排除MPLS网络故障
9.1.1　客户网络的控制平面操作
9.1.2　服务提供商网络的控制平面操作
9.1.3　数据平面的操作
9.2　排除MPLS骨干网故障
9.3　其他快速诊断方法
9.4　排除MPLS控制平面的故障
9.4.1　验证本机TDP/LDP运行参数
9.4.2　验证TDP/LDP Hello协议的运行情况
9.4.3　检查TDP/LDP会话
9.4.4　检查标签交换
9.5　排除MPLS数据平面的故障
9.5.1　在接口级别(interface-level)监控CEF的运行情况
9.5.2　超大数据包问题
9.6　排除MPLS VPN故障
9.6.1　快速诊断MPLS VPN故障
9.6.2　CE路由器间的ping操作
9.6.3　检查LSR的CEF交换功能
9.7　深入排除MPLS VPN故障
9.7.1　出站方向上CE-PE间的路由交换
9.7.2　路由导出
9.7.3　传播MPLS VPN路由
9.7.4　路由导入(Route Import)
9.7.5　MPLS VPN路由的重分发，以及入站方向上PE-CE间的路由交换
9.8　小结

章节摘录

版权页： 插图： 步骤5 若认证比对失败，CE路由器会生成一条告警消息，以提示需要人工干预。
另一种可选手段是，让CE路由器完全退出VPN，直到问题解决。
具备卓越的灵活性，支持重叠型（外联网）VPN，是基于令牌的CE间认证的优点之一。
其缺点是客户不但要自行操刀，执行额外的配置，还得维护以下两种协议之一：VPN令牌传播协议或运行于PE／CE互连电路之间的BGP协议。
虽然能够很容易地扩展BGP协议，令其支持令牌的传播，但对运行在PE／CE互连电路上的其他路由协议（如RIP、OSPF、ISIS、EIGRP或静态路由）进行改进（使其支持令牌的传播）恐怕就不是那么简单的事儿了。
相形之下，运行单独的VPN令牌分发（传播）协议，可以不受PE—cE路由协议的约束。
不过，如此一来，对客户站点来说，除了需要“操心”CE路由器之间的认证之外，还得维护已投入运行的PE／CE路由协议（假定不用BGP传播VPN令牌）。
draft—behringer—mpls—vpn.auth是另一份当前还在商议中的草案。
该草案提出的解决办法既不用开发新的协议，也无需对cE路由器进行软件升级，更不必在客户网络中执行额外的配置。
其主旨围绕这样一个前提：在PE／CE电路上，已经运行了MD5邻居认证（如前所述）。
使用该解决办法时，发送于PE路由器间的BGP UPDATE消息会包含一种新的BGP属性，名为“UPDATEauthenticator（更新认证者）”。
此UPDATE authenticator属性会携带两类信息：其一，生成此消息的路由器IP地址（generator value）；其二，由generator value生成的HMAC MD5加密签名。
使用generatorvalue，运行VPN专用的MD5密钥，便能生成generator value签名，而相关VPN的路由则由上面提到的那种包含UPDATE authenticator属性的BGP UPDATE消息承载。
收到包含UPDATE authenticator属性的BGP UPDATE消息之后，接收UPDATE消息的PE路由器会利用VPN MD5密钥的本地拷贝，根据包含在此属性中的9eneratorvalue，生成一个HMAC MD5签名。
若计算出的HMAC MD5签名结果与随UPDATEauthenticator属性传输而来的MD5签名值不同，PE路由器会丢弃UPDATE消息，并生成一条告警日志。
该草案所提解决办法也有其局限性，如下所列。

编辑推荐

Cisco权威出品MPLS领域的经典巨著，畅销10年深入分析MPLS架构通过扩展案例学习实践应用

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com