

基于 MPLS 的 VPN 技术探究

江晓峰, 高兴锁, 周海涛

(中国地质大学 计算机科学与技术系, 湖北 武汉 430074)

摘要:目前各种形式的网络应用已深入到千家万户的日常生活中,人们对骨干网络互连设备的性能、网络安全性以及稳定性的期望值越来越高。MPLS VPN 是一新兴的网络技术,它具有安全性高、可管理性好、可扩展性强、QoS 保障等特点。文中就这种新兴的网络技术,介绍了其重要的组成部分,以及 MPLS VPN 的基本框架结构,提出了地域级 MPLS VPN 解决方案,从而来提高网络的利用率与效益并大大改善整个网络结构的弹性与可扩展性。

关键词:多协议标签交换;虚拟专用网;虚拟路由转发表;标签分配协议

中图分类号:TP393.03

文献标识码:A

文章编号:1005-3751(2006)03-0053-03

Inquisition of Technique of Virtual Private Network Based on Multi Protocol Label Switching

JIANG Xiao-feng, GAO Xing-suo, ZHOU Hai-tao

(Department of Computer Science & Technology of China University of Geosciences, Wuhan 430074, China)

Abstract:Presently various network applications have penetrated millions of families and institutions, and there have always been higher expectations for the performance, security and stability of backbone network interconnection devices, among which MPLS VPN is a newly developed network technology, with characteristics of higher security, better manageability, larger extensibility and QoS guarantee. This paper introduces key components and essential frame structures of MPLS VPN, and proposed a resolution for regional MPLS VPN, thus promoting the utilization and efficiency, as well as improving the flexibility and extensibility of network structures.

Key words:multi protocol label switching; virtual private network; virtual routing forwarding; label distribution protocol

0 引言

MPLS 这个名称基于一个事实,即简单标签交换是作为底层转发机制。它是指 MPLS 位于传统的第二层与第三层协议之间,其上层与下层协议可以是当前网络存在的各种协议^[1]。伴随着经营观念和管理模式的转变,虚拟网的研究受到越来越多的重视。能为地理位置分布在不同地区的核心企业及其主要合作伙伴、用户建立一个安全可靠、高性能的通信环境, MPLS VPN 技术孕育而生。不少企业组网已经开始考虑将 MPLS VPN 作为主流的选择。

1 MPLS VPN 技术的工作原理

1.1 MPLS VPN 的重要组成部分

·用户边缘设备(Custom Edge Router-CE)。

用户边缘(CE)设备通过连接至一个或多个业务提供商边缘(PE)路由器的数据链路为用户提供对服务商的接入^[2]。通常情况下,CE 设备是一台 IP 路由器,它与直连

的 PE 路由器建立邻接关系。建立邻接关系后,CE 路由器将站点的本地路由广播给 PE 路由器。并从该 PE 路由器学习到远端 VPN 路由。

·提供商边缘路由器(Provider Edge Router-PE)。

PE 路由器使用静态路由、RIPv2、OSPF 或 EIGRP 与 CE 路由器交换路由信息。对于 PE 路由器来说,它只需要维护与其直接相连的那些 VPN 的 VPN 路由信息。每个 PE 路由器为其直连的站点维持一个虚拟路由转发表(VRF)^[2]。每个用户链接被映射至一个特定的 VRF。这里需要注意的是,一个 PE 路由器上的多个端口可与一个 VRF 相联系。PE 路由器具有维护多个转发表的能力以支持每个 VPN 间路由信息的隔离。

·提供商路由器(Provider-P)。

提供商(P)路由器是提供商网络中不连接任何 CE 设备的路由器。由于数据在 MPLS 骨干网中被转发时使用了双层标签堆栈,P 路由器只需维护到达提供商 PE 路由器的路由,它们并不需要为每个用户站点维护特定的 VPN 路由信息。

·用户域(site)。

在一个限定的地理范围内的用户子网。例如企业总部的专业网、分支机构的办公室网络等等。用户域内的所

收稿日期:2005-06-31

作者简介:江晓峰(1980—),男,湖北武汉人,硕士研究生,研究方向为基于电子商务、电子政务的信息安全技术;高兴锁,教授,研究方向为计算机网络、信息安全、基于互联网的 MIS、三维可视化。

有通信设施由用户自己管理。

1.2 基于 MPLS 的第二层与第三层 VPN 解决方案

(1) 第二层 MPLS VPN。

第二层 MPLS VPN, 也称作透明 LAN 业务 (TLS) 或虚拟私有 LAN (VPLS), 它的目的是扩展而不是代替现有的第二层 VPN 业务^[3]。对于第二层 MPLS VPN 来说, 最重要的是在 MPLS 网络上建立简单的点到点的隧道, 这样就能处理各种二层数据流。

(2) 第三层 MPLS VPN。

BGP/MPLS VPN 定义了运营商的 IP 骨干网上为用户提供 MPLS VPN 服务的一种机制。因为 BGP 被用来在运营商骨干网中发布每个 VPN 路由信息, 在路由器和交换机上建立和储存每个 VPN 的路由表, 而 MPLS 被用来将 VPN 业务从一个 VPN 站点转发至另一个站点。每个 VPN 实际上是私有 IP 网络, 在每个 PE 路由器上有私有的 IP 地址。

第二层和第三层 MPLS VPN 的主要区别是: 在一个第三层 MPLS VPN 里, PE 路由器和 CE 路由器建立了对等关系, 并且维护独立的路由表, 而不是在 CE 路由器之间建立对等关系。如图 1 所示。图中 IGP 为内部网关协议。CE 路由器向 PE 路由器提供私有网络的路由信息。反过来, PE 路由器必须能够存储多个私有路由表, 每个 VPN 连接一个私有路由表及到 Internet 的路由信息。

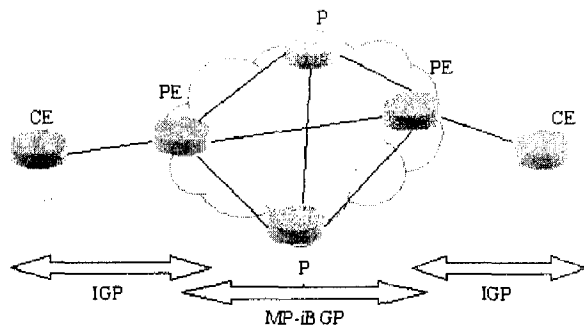


图 1 BGP/MPLS VPN 网络构成图

第三层 MPLS VPN 可以与 IP 网络很好地融合, 支持多种二层协议, 可以构建在多种传输网络上, 它具有很强的自动路由发现功能。它也受到一些条件限制。目前, 只有高端路由器可以支持多个私有路由表。即使如此, 复杂的路由结构使设备仍然存在超负荷的可能性。

2 基于 MPLS 的 VPN 地域级解决方案设计与研究

2.1 设计原理

(1) 层次结构。

在 MPLS VPN 的设计上, 笔者坚持三层结构的设计思想, 一般将 P 路由器定义到核心层, 将 PE 路由器定义到分布层, 而将 CE 路由器定义到接入层。

(2) 核心层设计。

核心层由 P 路由器组成, 主要负责网络骨干流量的传输和与 PE 路由器的连接。P 路由器之间应该网状或部分网状连接, 以保证可靠性。P 路由器不可以直接接入有主机系统或应用系统的网段, 否则会影响核心层的划分和 VPN 的规划。P 路由器主要放在电信大楼和部分主要的、流量大的分局或县局。

(3) 分布层设计。

分布层由 PE 路由器组成, 主要负责与 P 路由器、CE 路由器的连接。PE 路由器拥有并维护与其直接相连 CE 路由信息, 由 PE 路由器来负责定义和划分 VPN, PE 负责给数据包打 VPN 标签和 IGP 标签两层标签。PE 路由器放在电信大楼内和各主要接入节点 (分局、县局)。

(4) 接入层设计。

接入层由 CE 路由器和交换机组成, 提供各应用子系统的接入。此时 CE 路由器和交换机的配置与普通的配置没有什么区别。

2.2 网络拓扑结构图及关键技术

(1) 路由信息及标签信息的发布和维护。

图 2 中, 站点武汉某学校 A 校园网与某学校 B 校园网组成一个 VPN (此 VPN 的客户站点是由武汉某地区的所有大学校园网组成), 站点武汉某建工集团局域网与某煤工集团局域网构成一个 VPN (此 VPN 的客户站点是由武汉某地区的所有建筑公司局域网组成)。这里需要说明的是, 这两个 VPN 是相互独立的、不能互通的, 它们的地址空间存在交叠。

传统路由协议分布虚拟网路由信息遇到的一个问题就是 IPv4 地址空间重叠。一个简单的解决方法是采用 VPN-IPv4 地址来表示每个 VPN 地址空间, 以达到扩充地址空间的目的^[4]。

(2) MPLS VPN 中的数据转发。

PE 路由器除了维护针对 CE 连接的 VRF 以外, 还和 P 路由器一样需要维护一个用于骨干网转发的标签交换

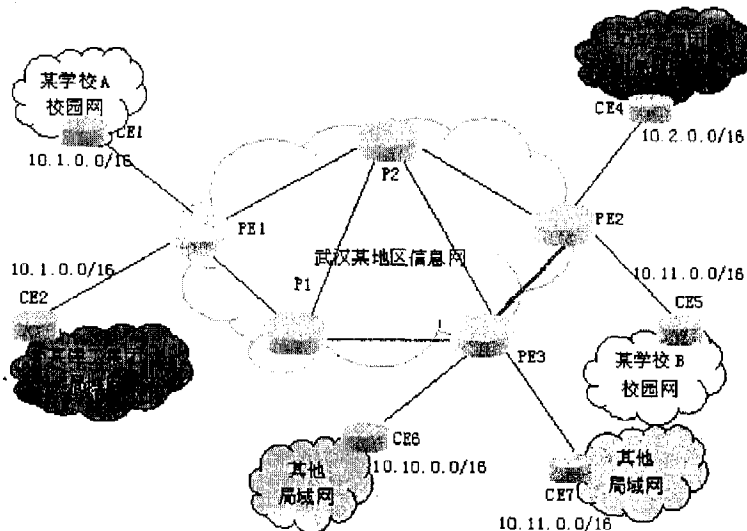


图 2 武汉某地区宽带城域网中基于 MPLS 的 VPN 网络拓扑结构图

转发表。在骨干网上,PE 到 PE 之间的 LSP 可以看成是一条下层的 LSP 隧道。PE 和 PE 互为 LDP 对等节点,同时 PE 与相连的 P 也是 LDP 对等关系,在 MPLS 骨干的入节点 PE 上,先将出节点 PE 发布的标签(外部标签)加入标签栈,然后将这个数据包“转发”给自己,再将下一跳 P 路由器发布的标签(内部标签)入栈,然后再将加入了两个标签的数据包向下一跳 P 路由器转发。图 3 为 MPLS VPN 数据包转发示意图。

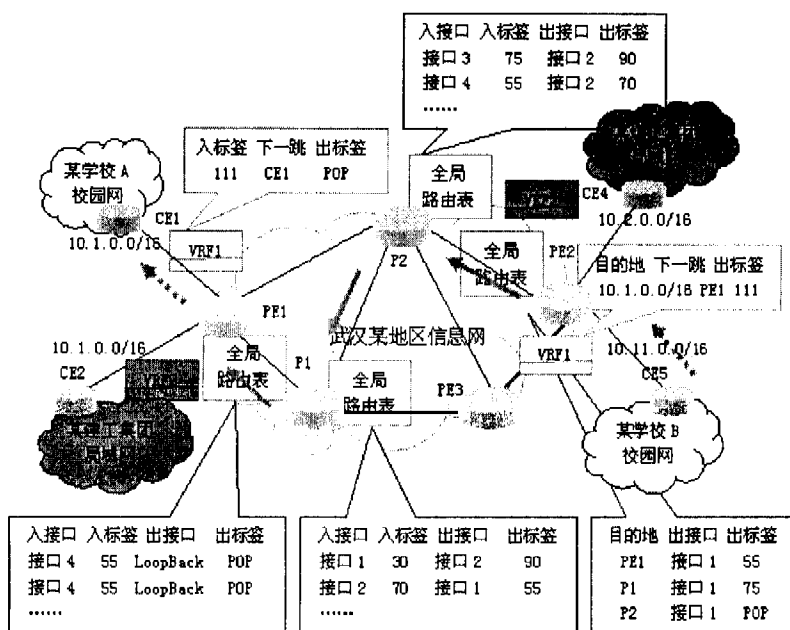


图 3 武汉某地区 MPLS VPN 数据包转发示意

如图 3 所示,站点武汉某学校 B 校园网中的某个主机(目的地址:10.1.1.2)的数据转发到它的默认网关。当一个数据包到达 CE5 时,它执行最长匹配路由查询,并将 IPv4 数据包转发给 PE2。PE2 接受到该数据包,在 VRF1 中执行路由查询,并获得如下信息:由 PE1 连同该路由一起通告给 PE2 的 MPLS 标签(标签=111),该路由的 BGP 下一跳为 PE1,从 PE2 至 PE1 的 LSP 输出子接口,从 PE2 至 PE1 的 LSP 的初始 MPLS 标签。用户业务数据包包含两个标签的标签栈从 PE2 向 PE1 转发。对于这个数据流,PE2 为 LSP 的入口 LSR,而 PE1 为此 LSP 的出口 LSR。首先,PE2 给数据包加上从 PE1 得到的标签 111,然后再向标签栈中压入从 P2 获得的内部标签 55,然后向

P2 转发。在 MPLS 骨干内部的 P 路由器根据标签栈顶部的标签进行转发(PE1 发布给 PE2 的标签不位于标签栈顶),直到出节点 PE。当 PE1 接受到数据包时,将骨干 LSP 的内部标签出栈,并使用下一层标签(111)确定到达 10.1.0.0/16 的下一跳,然后将外部标签出栈。最后,PE1 将原来的 IPv4 数据包转发给 CE1,CE1 将把数据包转发给站点武汉某学校 A 校园网中的服务器 10.1.1.2。

3 结束语

MPLS VPN 非常适合于具有相对简单的网络用户。它允许用户将路由管理的复杂性外包给它们的 VPN 服务提供商,将管理站点的全网状连接的复杂性从用户 CE 路由器转移到 PE 路由器,允许提供商使用其共享的 MPLS 基础结构对私有及公共数据进行传输。MPLS VPN 具有较好的可扩展性,通常与覆盖型网络联系在一起的 N 平方可扩展性问题不会出现^[5]。

当然,MPLS VPN 目前也存在着一些难以解决的问题,例如在 VPN 中难以实现多点播送支持。但无论如何,MPLS 技术的应用确实使现有的 VPN 性能在原有的基础上有了大幅度的提高,而 MPLS VPN 必将成为未来 VPN 的主流。

参考文献:

- [1] 朱 斌,徐 林.MPLS 技术在 VPN 中的研究与应用[J].计算机与数字工程,2005,34(4):83-85.
- [2] 刘广宇.基于 MPLS 的 VPN 技术原理[J].信息技术,2005(4):106-107.
- [3] 冯 径.多协议标签交换技术[M].北京:人民邮电出版社,2002.
- [4] 吴 伟.下一代 IP 网络技术保障——多协议标签交换[M].北京:清华大学出版社,2002.
- [5] 谢希仁.计算机网络(第3版)[M].大连:大连理工大学出版社,2000.

(上接第 52 页)

息,把 BookServer.dll 部署在服务器端以提供远程数据服务。在安装 .NET Framework 的客户端只需拷贝 Interface.dll 和 WinClient.exe,即可实现网络环境下的分布式应用。由此可见,.NET Remoting 远程处理架构是一种基于 HTTP(或 TCP/IP)协议的分布式开发模型,大大简化了分布式对象处理的软件开发过程。

参考文献:

- [1] 梁普选,张宝华,李国昌..NET 远程处理架构及分布式对

象处理[J].河北工业科技,2004,21(6):35-38.

- [2] BARNABY T..NET 分布式编程 C# 篇[M].黎 媛,王小锋,等译.北京:清华大学出版社,2004.
- [3] 陈 琨,陈福民.基于 .NET Remoting 利用软件方法实现网络教学的探索[J].计算机应用,2003,23(8):130-132.
- [4] McLean S,Naftel J,Williams K.Microsoft.NET Remoting 权威指南[M].张昆琪等译.北京:机械工业出版社,2003.
- [5] 李念强,张焕春,经亚枝.分布式应用集成模型——.NET 远程框架[J].计算机工程,2002,28(3):267-269.