基于MPLS的二、三层VPN研究

罗恒洋
(安徽财经大学 信息工程学院 计算机系,安徽 蚌埠 233041)

摘 要:传统的IP VPN采用封装技术在IP主干网上建立隧道,发送数据分组,MPLS采用在数据分组头部增加转发标签的技术,完成数据分组在IP主干网的转发。基于MPLS的VPN有两种实现方式,就是基于MPLS的二、三层VPN实现方案。文中阐述了MPLS网络的基本工作原理和MPLS主干网的结构,分析了基于MPLS技术的二、三层VPN的拓扑结构和工作机制,总结了MPLS二、三层VPN的工作特点,提出了要根据VPN网络设计性能和目标,合理选择基于MPLS技术的VPN方案组建用户所需要的VPN。

关键词:MPLS;隧道技术;二层VPN;三层VPN;拓扑结构
中图分类号:TP393.02 **文献标识码**:A **文章编号**:1673-629X(2009)01-0063-04

Research on L2 and L3 VPN Based on MPLS

LUO Heng-yang
(Department of Computer, School of Information and Engineering, Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: The conventional forwards data packages by tunnel which is set up over IP backbone via encapsulated technology. MPLS makes use of labels added in the header of datagram to forward the data packets over IP backboe. There are two ways to realize the VPN based on MPLS, that is, the methods of layer2 and layer3 VPN based on MPLS. States the main principle of MPLS technology and the structure of MPLS backbone. Analyzes the mechanism and topology of layer2 and layer3 VPN based on MPLS. Summarizes the characteristics which are possesd by layer2 and layer3 VPN. Proposes that on the basis of the property and target of network design a plan may be reasonably choosed to construct the MPLS VPN needed by customers.

Key words: MPLS; tunnel technology; layer2 VPN; layer3 VPN; topology

0 引 言

VPN(Virtual Private Net)技术的核心是在公共的数据通信网络上建立隧道,连接两个距离相当远的企业专用网络,为企业提供服务[1]。早期的VPN使用某种专门的隧道协议完成VPN功能,使用的是传统的IP交换技术,制约了VPN的性能,随着MPLS技术在IP骨干网上的应用[2],其与生俱来的对VPN支持能力充分显示出来,成为首选的组建VPN技术。

1 MPLS工作原理及网络结构

限制IP分组交换网发展的因素主要有两个:一是传输物理链路带宽;二是路由器转发速率。随着高带宽传输媒介的应用,低带宽的传输介质在骨干网上逐渐被高带宽的传输介质取代,物理链路的带宽大大提高。传统的IP分组转发中,无连接网络层协议的分组从一个路由器传输到下一个路由器,每个路由器都要独立分析分组头,执行网络层路由算法,对路由作出选择,确定分组的下一跳,分组在路由器中时延较大,网络规模不断扩大的情况下,路由器能否实现线速转发成了网络的主要瓶颈,MPLS技术最初产生的原因就是要解决分组转发速率问题[3,4]。MPLS将所有进入网络的分组划分成转发等价类FEC[1~4](Forwarding Equivalence Class),并将每个特定FEC映射到下一跳,即进入网络的每一特定分组都被指定到某个特定的FEC中,每个FEC都被编码为一个短而定长的值,这个值称为标签(Label)。标签加在分组前,使分组成为标签分组,再转发到下一跳,在后续的每一跳上,不再需要分析分组头,而是用标签作为指针,指向下一跳的输出端口和一个新的标签,标签分组使用新标签代替旧标签后,从指定的输出端口转发出去。根据固定长度的标签检索目的地址,要比传统的最长匹配IP地址

收稿日期:2008-05-16
基金项目:安徽省自然科学研究项目(KJ2007C302ZC)
作者简介:罗恒洋(1970—),男,山东滕州人,讲师,硕士,研究方向为计算机网络与信息安全。

方式快很多,减小了分组在路由器中的时延,能实现路由器的高速转发。

MPLS 技术把传统的三层路由选择技术和二层虚电路交换技术结合起来,提高了路由器的能力,采用 MPLS 技术的 IP 主干网结构主要由标签交换路由器(LSR)构成的 MPLS 域组成,互相连接的标签交换路由器(LSR)构成了 MPLS 域,局域网通过用户边缘路由器(CE)和主干网边缘路由器(PE)接入 IP 主干网。IP 主干网(MPLS 域)内的标签交换路由器之间建立标签交换路径(LSP)形成一个贯穿主干网的隧道,数据流沿着标签交换路径构成的隧道从一端流向另一端。当采用 MPLS 技术组建 VPN 时,要使用双层标签技术实现隧道[1],内层标签由边缘设备完成与用户站点的映射,标识着本标签报文需要哪个边缘设备处理,外层标签完成在由核心层设备构成的 MPLS 域中转发分组,核心层的设备不需要知道内层标签的存在,只是按照标签路径转发分组。

2 MPLS 二层 VPN 的实现与分析

传统 IP VPN 中,虚拟点对点连接通过隧道实现,而在 MPLS 域中,任意两个端点之间可以建立标签交换路径(LSP),这个 LSP 就称作 LSP 隧道。因此,可以设计出 MPLS 二层隧道的 VPN 拓扑结构,如图 1 所示。

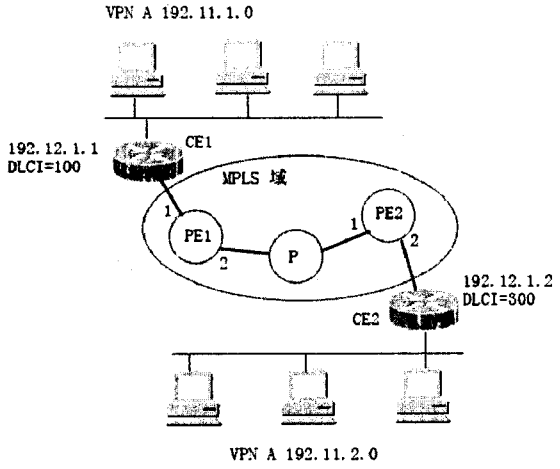

图 1 基于 MPLS 第二层 VPN

图 1 中,CE 为用户边缘路由器,PE 为 MPLS 域的边缘路由器[2],CE 通过 PE 接入 MPLS 域。一个 PE 可以接入多个 VPN,对于同一 VPN,各个 CE 接入 PE 的方式必须相同,文中以帧中继[5]接入方式进行分析。VPN A 中的 CE1 用帧中继接口接入 PE1,VPN A 中的 CE2 也通过帧中继接口接入本地的 PE2,在 MPLS 域中 PE1 和 PE2 之间必须建立 LSP,这些 LSP 的建立和 VPN 没有关系,通过 LDP 或 RSVP 建立 LSP。图 1 中 LAN1 通过 CE1 用帧中继接口接入本地 PE1,PE1 就必须为帧中继接入电路分配数据链路连接标识符,同时在 CE1 中建立路由表,如表 1 所示。

表 1 CE1 中有关 192.11.2.0 子网的路由项

目的 IP 地址	目的地址掩码	输出接口	输出接口类型	虚电路 DLCI	下一跳路由地址
192.11.2.0	255.255.255.0	FR1	FR	100	192.12.1.2

对于 CE1 来说,MPLS 域就象一个帧中继网络,通过 DLCI=100 的虚电路和 VPN A CE2 点对点相连,只要把送往 192.11.2.0 子网的 IP 报文封装成 LAPF(核心)帧,帧首部 DLCI 字段值置为 100,然后将封装后的 LAPF(核心)帧从相应帧中继接口(FR1)输出,就一定能够到达 VPN A CE2。

由于 MPLS 域中的 LSP 隧道是单向隧道,为了在 VPN A 中实现各个子网的双向数据传输,要在 PE1 和 PE2 上建立两条不同方向的 LSP 隧道。表 2 给出 PE1 中,PE1→P→PE2 LSP 隧道转发表,表 3 给出 PE2 中,PE1→P→PE2 LSP 隧道转发表,PE1 和 PE2 中逆方向的 LSP 隧道转发表文中略去,不影响分组在隧道中的转发分析。

表 2 PE1 中 PE1→P→PE2 LSP 转发表

输入 DLCI	VPN 标识标签	LSP 输出标签	LSP 输出接口
100	202	505	2

表 3 PE2 中 PE1→P→PE2 LSP 转发表

LSP 输入标签	LSP 输入接口	VPN 标识标签	对应 DLCI	对应 FR 端口
-	1	202	300	FR2

从表 2 中可以看出,PE1 必须根据接收到的 LAPF(核心)帧首部 DLCI 字段值确定 VPN 标识标签,选定对应的 LSP,这个 LSP 可以通过 PE1 内 LSP 转发表的输出标签和输出接口确定。LSP 的 VPN 标识标签和输出标签功能是不同的,输出标签是隧道标签,PE1 的 LSP 输出标签和 LSP 输出接口确定了 LSP 隧道,保证能够经过指定的 LSP 隧道将 MPLS 分组送到 PE2。如果 PE2 接入了多个不同 VPN 时,无法从标识 LSP 的标签字段中确定对应的 CE 来转发 LAPF(核心)帧,因此使用 VPN 标识标签,作为内层标签,让 LSP 末端 PE2 用 VPN 标识标签确定 LAPF(核心)帧的目的 CE 及相应的 DLCI。

假设有 IP 分组从 VPN A 中的 IP 子网地址为 192.11.1.0 的 LAN1 中终端发送到 VPN A 中 IP 子网地址为 192.11.2.0 的 LAN2 中终端,分析 IP 分组传送过程如下:LAN1 中终端首先把 IP 分组转发给用户边缘路由器 CE1,CE1 根据报文目的 IP 地址确定下一跳路由器的 IP 地址为 192.11.1.2,连接方式为帧中继,DLCI=100,输出端口为帧中继端口 2(FR2),CE1

将 IP 分组封装成 LAPF 帧,帧首部 DLCI 字段值为 100,从指定输出端口将 LAPF 帧转发出去,PE1 收到 LAPF 帧,根据 DLCI = 100,查找 PE1 转发表,确定 VPN 标识标签 202 和 LSP,LSP 输出标签 505,LSP 输出端口为 2,将 LAPF 帧封装成 MPLS 分组从端口 2 转发出去,MPLS 标签堆栈栈底标签为 202,栈顶标签为 505,中间路由器 P 根据栈顶标签进行标签交换转发,图 1 中的 P 已是 LSP 上倒数第二跳 LSR,只进行弹出、交换操作,不再压入输出标签,到达 PE2 的 MPLS 分组所携带的标签只是栈底 VPN 标识标签,不是 LSP 输入标签,PE2 根据栈底 VPN 标识标签,查找 PE2 转发表,确定帧中继输出端口和输出 DLCI,对 LAPF 帧的 DLCI 字段进行置换,DLCI = 300,将 LAPF 帧转发给 CE2,CE2 从 LAPF 帧中剥离出 IP 分组,根据 IP 分组的目的 IP 地址,将 IP 分组转发给 IP 子网地址为 192.11.2.0 的 LAN2。从 CE 角度看,IP 主干网(MPLS 域)很象一个提供二层连接的公共传输网络[6]。

3　MPLS 三层 VPN 的实现与分析

采用 MPLS 技术的三层 VPN 的网络拓扑结构如图 2 所示。图 2 中,CE1 和 CE2 作为用户边缘路由器[2]不需要知道属于同一 VPN 的其他子网的分布情况,CE1 和 CE2 只需配置直接和其相连的 LAN 的路由情况。将 PE1 和 PE2 设置为 BGP 的邻接路由器,同时,PE1 和 VPN A CE1,PE2 和 VPN A CE2 可以设置为 RIP、OSPF,或 BGP 的邻接路由器。MPLS 域通过 LDP 或 RSVP 在 PE1 和 PE2 之间建立 PE1→PE2 和 PE2→PE1 的 LSP,PE1 和 VPN A CE1 交换路由信息,PE2 和 VPN A CE2 交换路由信息。

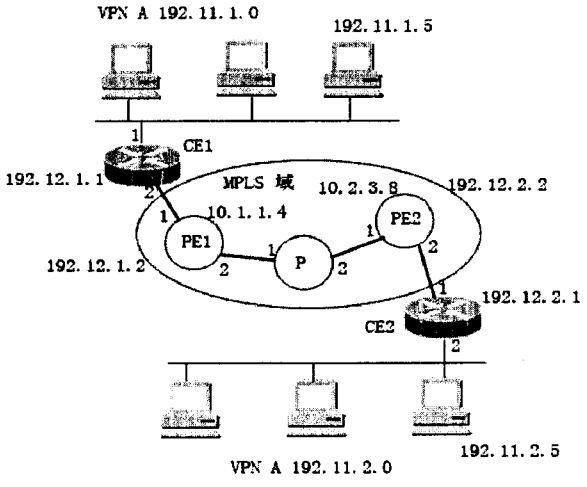

图 2　基于 MPLS 第三层 VPN

PE1 和 PE2 通过 BGP 公告信息,PE1 和 PE2 为 VPN A 最终建立的路由表如表 4 和表 5 所示。

表 4　PE1 为 VPN A 最终建立的路由表

目的 IP 地址	目的地址掩码	下一跳路由器	输出端口	距离	VPN 标识标签
192.11.1.0	255.255.255.0	192.12.1.1	1	2	1001
192.11.2.0	255.255.255.0	10.2.3.8	2	n	2002

表 5　PE2 为 VPN A 最终建立的路由表

目的 IP 地址	目的地址掩码	下一跳路由器	输出端口	距离	VPN 标识标签
192.11.2.0	255.255.255.0	192.12.2.1	2	2	2002
192.11.1.0	255.255.255.0	10.1.1.4	1	n	1001

对于 PE1,目的地址 192.11.2.0/255.255.255.0 的下一跳路由器为 PE2,给出的 PE2 IP 地址为 MPLS 域内的全局 IP 地址,对于 PE2,目的地址 192.11.1.0/255.255.255.0 的下一跳路由器为 PE1,给出的 PE1 IP 地址同样为 MPLS 域内的全局 IP 地址。VPN 标识标签是用来标识 IP 分组所属 VPN 的,由于 PE 可能连接多个属于不同 VPN 的 LAN,这些属于不同 VPN 的 LAN 所分配的 IP 地址可以相同(专用地址),因此,PE 必须为属于不同 VPN 的 LAN 建立单独的路由表。当有到达 PE 的分组时,PE 无法从 IP 分组的目的 IP 地址确定 IP 分组所属 VPN,必须给分组携带用于区分分组所属 VPN 的标识标签,PE1 和 PE2 通过 BGP 公告消息将 VPN 标识标签公告给对方。PE1→PE2 的 LSP 路径如表 6 所示。

表 6　PE1→P→PE2 的 LSP

	PE1		P		PE2	
FEC	输入标签及端口	输出标签、端口	输入标签及端口	输出标签及端口	输入标签及端口	输出标签及端口
10.2.3.8/32	—	100,2	100,1	200,2	200,1	—

假定图 2 中有 IP 地址为 192.11.1.5 的终端,向 IP 地址为 192.11.2.5 的终端传输 IP 分组,分析分组传输过程如下:目的地址为 192.11.2.5 的 IP 分组首先被传送到 CE1,CE1 通过检索路由表发现 IP 分组的下一跳路由为 PE1,通过输出端口 2 将 IP 分组转发给 PE1,PE1 通过检索路由表,发现 IP 分组的下一跳路由器为 PE2,同时指定该分组的 VPN 标识标签为 2002,PE1 为 VPN A 生成独立的路由表,必须指定 PE1 端口 1 连接 VPN A,所有从端口 1 接收到的分组均去检索为 VPN A 生成的路由表。由于 PE1 的端口 2 使能了 MPLS,可以确定从 PE1 到 PE2 的传输路径是 LSP,PE1→P→PE2 的 LSP 如表 6 所示,PE1 将 IP 分组封装成 MPLS 分组,在标签堆栈中压入 VPN 标识标签后,将 MPLS 分组交转发部件转发。转发部件根据 FEC(10.2.3.8/255.255.255.255)去匹配转发表,确定 MPLS 分组的输出标签为 100,输出端口为 2,PE1 在 MPLS 报文的标签堆栈中压入用于指定 LSP 的输出标签 100,从端口 2 转发出 MPLS 分组。当 P 从端

口 1 接收到 MPLS 分组，根据输入端口 1 和输入标签（MPLS 分组栈顶标签 100）匹配转发表，找到输出端口 2 和输出标签 200，但由于 P 已是 LSP 的倒数第二跳 LSR，P 不再将输出标签 200 压入标签堆栈，而是直接将弹出栈顶标签后的 MPLS 分组转发给 PE2，PE2 根据 MPLS 分组所携带的标识标签 2002 确定 IP 分组属于 VPN A，从 MPLS 分组中剥离出 IP 分组，根据 IP 分组的目的地址查找 PE2 为 VPN A 所生成的路由表，找到路由项，并根据路由项将 IP 分组转发给 CE2，CE2 再根据路由表将 IP 分组转发给 IP 地址为 192.11.2.5 的终端。由此可以看出，在基于 MPLS 第三层 VPN 中，VPN A CE1 和 VPN A CE2 接入 MPLS 域的方式可以不同[2,6]。

4 两种设计方案的总结

MPLS 二层 VPN 把 MPLS 域作为提供第二层连接的公共传输网络，作为第二层连接两端的用户设备，要采用同一种方式接入 MPLS 域，MPLS 域不参与用户 VPN 的路由过程，由用户负责解决同一 VPN 内各 LAN 之间的路由问题，这就要求用户全面了解 VPN 中各 LAN 的分布及配置，对用户的网络设计及配置知识有较高的要求；基于 MPLS 第三层的 VPN 只要求用户配置有关直接相连的 LAN 路由信息和接入 MPLS 域的 PE，并不需要知道属于同一 VPN 的其它 LAN 的情况，这就降低了对用户网络设计、配置知识的要求，VPN 的管理由网络服务提供者来进行管理，方便了 VPN 用户。

MPLS 二层 VPN 中，PE 只需要和 CE 建立链路层连接，一旦某个 CE 故障，只影响 PE 连接的故障 CE 接口，而在基于 MPLS 第三层 VPN 中，某个 CE 故障可能导致错误的路由信息，因而影响 PE 甚至整个服务提供者的稳定性。基于 MPLS 二层的 VPN 中，每个 PE 仅保持每个 CE 有关的信息，并不保存 CE 所连接的多个 VPN 信息，即多个 VPN 能够复用 MPLS 域内的一条隧道，在基于 MPLS 的三层 VPN 中，PE 要为一个 CE 连接的多个 VPN 都要保留单独的 VPN 路由信息，这对 MPLS 域内的 PE 性能要求有某些限制。从用户角度看，MPLS 二层 VPN 和传统的二层 VPN 很相似，组建 VPN 时容易从传统的二层 VPN 升级到基于 MPLS 的二层 VPN。采用 MPLS 组建三层 VPN 时，难度较大一些，对网络服务提供者有更高的要求。MPLS 二层 VPN 中，网络服务提供者不参与用户路由信息，保证了用户路由的专用性，而 MPLS 三层 VPN 中，CE 和 PE 是两个对等的网络设备，相互交换路由信息，PE 中要保留所有用户 VPN 的路由信息，无法保证用户路由的专用性。基于 MPLS 二层 VPN 用户其网络层以上可以运行多种协议，而 MPLS 三层 VPN 用户的网络层以上要运行相同的协议。MPLS 二、三层 VPN 在 MPLS 域内都是利用标签隧道完成报文分组的快速转发，从用户和网络服务提供者的角度看，两种方案主要在 CE 与 PE 路由器的作用和配置上有很大不同，设计 VPN 时要根据 VPN 的性能和目标进行取舍。

5 结束语

采用基于 MPLS 第二层组建的 VPN 对用户要求较高[1,2]，但从安全的角度来看，只使用骨干网提供的链路层服务，VPN 的专用性较强，因为服务提供者并不了解用户的 VPN 结构，而 MPLS 第三层 VPN 组网中，服务提供者的 PE 了解所有 VPN 信息，容易造成 VPN 专用信息的泄漏。MPLS 三层 VPN 是 RFC2547 中提出的 VPN 结构，从网络服务提供者角度来看易于管理、扩充性好、有 QoS 保证、安全性较好。MPLS 二、三层 VPN 各有特点，网络实施者可以根据网络设计目标选择一种合适方案，创建所需要的 VPN。

参考文献：

[1] 何宝宏. IP 虚拟专用网技术[M]. 北京：人民邮电出版社，2002.

[2] 沈鑫剡. IP 交换网原理、技术及实现[M]. 北京：人民邮电出版社，2003.

[3] 谢希仁. 计算机网络[M]. 第 4 版. 北京：电子工业出版社，2003.

[4] Tanenbaum A S. Computer Network[M]. 3rd Edition. 北京：清华大学出版社，1996.

[5] Stallings W. Data and Computer Communication[M]. 5th edition. 北京：清华大学出版社，1997.

[6] Finlayson M, Herrison J, Sugarman R. VPN Technologies a Comparison[R]. [s.l.]: Data Connection Limited, 2003.

（上接第 62 页）

481 - 492.

[8] 邓乃扬，田英杰. 数据挖掘中的新方法——支持向量机[M]. 北京：科学出版社，2006.

[9] 章毓晋. 图像工作[M]. 第 2 版. 北京：清华大学出版社，2007.

[10] 郭 勇. 基于支持向量机的图像处理方法研究[D]. 西安：西安理工大学，2006.