文章编号:1674-7070(2010)06-0567-06

MPLS VPN 的实现机制及其配置

傅德胜[1]　肖洁芩[1]

摘要

讨论了 MPLS VPN 的实现方式、组件及其功能、工作原理、数据转发过程,给出了 MPLS VPN 配置实例,同时对 MPLS VPN 安全性进行了剖析.

关键词

MPLS VPN;实现机制;配置;边界网关协议;虚拟路由转发

中图分类号 TP393.2

文献标志码 A

0　引言

Introduction

MPLS(Multi-Protocols Label Switching)是一项用绑定在包中的标记(或叫标签)通过网络进行数据包转发的技术,它将网络第 2 层的交换和第 3 层的路由技术很好地结合起来,以简洁的方式完成信息的传送,把路由选择和数据转发分开由标签来规定一个分组通过网络的路径.

VPN(Virtual Private Network)虚拟专用网是利用网络来传输私有信息而形成的逻辑网络,用来在通用的网络结构上标识闭合的用户组.通过对网络数据的封包和加密传输,在一个公用网络(通常是因特网)建立一个临时的、安全的连接,从而实现在公网上完整、保密地传输私有数据.

MPLS VPN(Multi-Protocol Label Switching Virtual Private Network)为利用多协议标签交换技术组建的虚拟专用网,其利用运营商的网络,降低企业内部网络的建设成本,极大地提高用户网络运营和管理的灵活性,同时满足用户对信息传输的安全性、实时性、高速性、便捷性的需要.当前,MPLS VPN 业务开始大范围服务于各个行业中,它与传统数据通信服务之间不是简单的业务更替关系,通过它不仅能够以更优质的服务满足企业客户需要,而且还可以在其基础上开发各种增值应用.

本文将讨论 MPLS VPN 实现方式、组件及其功能、工作原理、数据转发过程,并给出 MPLS VPN 配置实例.

1　MPLS VPN 实现方式

MPLS VPN realization modes

MPLS VPN 的实现方式有 2 种:

1)重叠 VPN:X.25、帧中继和 ATM 等 2 层重叠 VPN 以及 GRE 隧道和 IPSec 等 3 层重叠 VPN.

2)对等互连 VPN:使用 ACL 在共享的服务提供商网络设施上实现的 VPN,为每个客户提供独立的路由器.

MPLS VPN 同时汲取了重叠 VPN 和对等互连 VPN 的优点.从本质上看,MPLS VPN 属于对等互连 VPN,它利用每个客户唯一的 RD(Router Distinguisher,路由区分符)来实现每个客户的路由信息完全

收稿日期 2010-06-24

作者简介

傅德胜,男,教授,主要研究图像处理与模式识别、信息安全.000501@nuist.edu.cn

肖洁芩(通讯作者),女,硕士生,主要研究信息安全.xiaojieqin@qq.com

1　南京信息工程大学　计算机与软件学院,南京,210044

独立,确保路由信息的安全性,而且利用 RD,服务提供商可以为每个客户提供一个逻辑独立的 PE 路由器,但一般不是物理独立的[1].

每个客户的路由信息都由一个与 RD 绑定的特定路由协议实例来维护,由该路由协议实例构建的路由表称为 VRF(Virtual Routing and Forwarding,虚拟路由转发)表.

2 MPLS VPN 组件及其功能
MPLS VPN components and functions

MPLS VPN 由以下几部分组成[2]:

1) C 网络:客户控制的内部网络.

2) CE 路由器:客户端路由器,连接在 PE 路由器上. CE 路由器无需支持 MPLS,也不属于 MPLS 体系架构,只是负责发送和接收客户的路由信息. 提供商的 MPLS P 路由器对 CE 路由器是不可见的.

3)LSP:标签交换数据包通过 P 网络传输特定目的地时用到的路径.

4) P 网络:服务提供商控制的由核心路由器组成的内部网络,通过提供商的骨干网提供转送能力,但不携带客户的路由信息.

5) P 路由器:服务提供商的 MPLS 核心路由器或骨干路由器,无面向客户的接口,不携带 VPN 路由,也不参与 MPLS 路由,它们仅提供 PE 路由器之间的流量传送功能. P 路由器与 PE 路由器相连,负责将 BGP(Border Gateway Protocol,边界网关协议)对等信息传送到远端 PE 路由器.

6) PE 路由器:服务提供商控制的路由器,与 CE 路由器互连并交换路由信息. PE 路由器虽然是单台设备,但是却运行多个路由协议实例,以维护与特定客户相关的路由器并负责将它们重分发到全局 IP 路由表中,如图 1 所示.

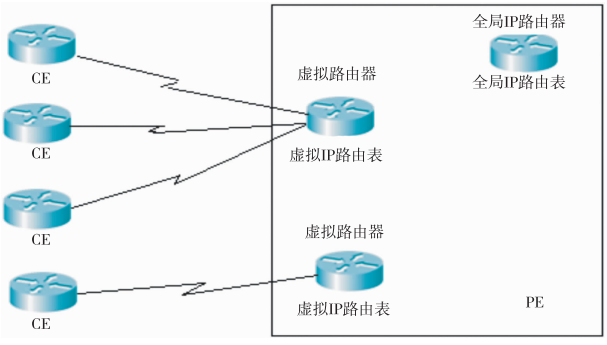

图 1 PE 路由器中创建的虚拟路由器

Fig. 1 Established virtual routers in a PE router

7) RD:一个 64 bit 标识符,附加在 IPv4 地址前就可以组成一个全球唯一的 VPNv4 地址. 这样可以使不同客户使用相同私网地址的子网相互共存. PE 路由器上的这些 VPNv4 地址在 BGP 对等体之间进行宣告. 支持 IPv4 之外地址族的 BGP 实现称为 MBGP(Multiprotocol BGP,多协议 BGP). 本地环路中运行 IGP(Interior Gateway Protocol,内部网关协议),在 PE 和 CE 路由器之间直接通过 IBGP(Interior BGP,内部 BGP)对等连接建立对等关系,以便交换路由. 邻居 PE 从其对等体接收到 VPNv4 信息之后,移除 RD,这样路由器就可以被重发布回 IGP,并发送给 CE 路由器,从而到达目的网络. RD 的功能仅仅是允许路由选择体系能处理重叠的地址空间[3].

8) VRF 表:与客户相关的路由表实例. RD 和 VRF 之间存在唯一的映射关系. 一个 VPN 对应一个 VRF 可以保证对于接收到的 VPN 数据包只有当路由的目标站点与源站点的 VPN 标识符相同时,才进行数据包的转发.

9) RT:某个站点同时加入多个 VPN,将若干个 VPN 标识符都与某台路由器相关联,以表示成员关系. RT 是一个附加在 VPNv4 BGP 路由上表示 VPN 成员关系的额外属性.

3 MPLS VPN 工作原理
MPLS VPN working principle

3.1 VPN 路由信息的传播

基于 PE 路由器之间的 VPN 路由信息传播主要有 2 种方法:

1) 对于每个 VPN,PE 路由器可以运行不同的路由选择算法. 服务提供商网络中包含大量 VPN 时,这种方案面临挑战.

2) PE 路由器运行单个路由协议来交换所有的 VPN 路由. 为了支持 VPN 客户地址空间重叠的情况,必须在 VPN 客户使用的地址空间加入额外的信息,使之唯一.

当构建大型的 MPLS VPN 网络时,将采用第 2 种方法. 在 CE 路由器通告给 PE 路由器的 IP 子网中附加一个 RD 的 64 位前缀,使 BGP 在 PE 路由器之间交换得到 96 位地址[4].

选择 BGP 作为路由协议传输 VPN 路由主要基于以下考虑:

1) 网络中的 VPN 路由的数目可能非常庞大,BGP 是唯一一种支持大量路由的路由协议.

2) BGP、EIGRP 和 IS-IS 可用于多协议的路由协议. 然而,IS-IS 和 EIGRP 不能扩展到 BGP 那么多的路由数量,并且,BGP 具有在不直接相连的路由器之间交换信息这一特性,使得 P 路由中无需包含 VPN 路由选择信息.

3) BGP 可以运载附加在路由后面的任何信息,将其作为一种可选的 BGP 属性. BGP 这种特性使得在 PE 路由器之间传播路由目标非常简单[5].

3.2 VPNv4 路由传播

如图 2 所示,用户的 VPN 路由由于在每一个 IPv4 前缀上都添加了 RD 后变成 VPNv4 路由而使得其具有唯一性,所以所有的用户路由都可以很安全地在 MPLS VPN 的网络中进行传播. 端到端的路由流向大致为:

1) PE 路由器从 CE 路由器那里通过内部网关协议(IGP)或者外部 BGP 接收到 IPv4 的路由;

2) 将这些路由加入相应的 VRF 中,这个 VRF 通常配置在 PE 路由器指向 CE 路由器接口上的 VRF;

3) 这些路由添加了 RD 之后被分配给特定的 VRF,原来的路由器变成 VPNv4 路由,进入到 MP-BGP 中;

4) BGP 将 VPNv4 路由分发给 MPLS VPN 网络中的所有 PE 路由器;

5) 接收到 MP-BGP 更新的 PE 路由根据路由上的入口 RT 并移除 RD;

6) 将 IPv4 注入到 VRF 路由表中,能否注入到 VRF 中完全依赖于 RT 是否允许输入到 VRF;

7) 这些 IPv4 路由被重分发到 PE 和 CE 间运行的 IGP 实例中,或者运行 eBGP 通告 CE 路由器,接着被传播到 CE 路由器所连接的 C 网络.

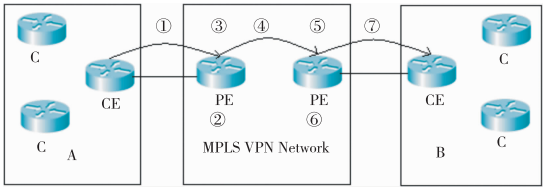

图 2 在 MPLS VPN 网络中的路由传播步骤

Fig. 2 Propagation steps in the MPLS VPN network

在上述路由中,PE 路由器之间运行的是 iBGP,PE 和 CE 路由器之间运行的是 eBGP 或 IGP,其作用是在 PE、CE 之间传递用户网络路由;而 MPLS VPN 网络中的路由协议为标记分发协议(Label Distributed Protocol,LDP)它的作用是在入口 PE 和出口 PE 之间路经多个 P 路由器建立 LSP;RSVP-TE(Resource Reservation Protocol-Traffic Engineering,根据流量工程的资源预约协议)和 CR-LDP(Constraint Resource LDP,约束资源标记分发协议)的作用是在入口 PE 和出口 PE 之间路经多个 P 路由器建立具有 QoS 能力的 ER-LSP;多协议 BGP(MP-BGP)为经过扩展后承载携带标记的 VPNv4 路由的 BGP[6].

3.3 MPLS VPN 的数据转发过程

当 CE 路由器将一个 VPN 分组转发给入口 PE 路由器后,PE 路由器查找该 VPN 对应的 VRF,从 VRF 中得到一个 VPN 标签和下一跳出口 PE 路由器的地址,VPN 标签作为内层标签打在 VPN 分组上,根据下一跳出口 PE 路由器的地址可以在全局路由表中查出到达该 PE 路由器应打上的域内路由的标签,即外层标签. 于是 VPN 分组被打上了 2 层标签,主干网的 P 路由器根据外层标签转发 VPN 分组,在最后一个 P 路由器处,外层标签弹出,VPN 分组只剩下内层标签(此过程被称作次末级弹出机制),接着 VPN 分组被发往出口 PE 路由器. 出口 PE 路由器根据内层标签查找到相应的出口后,将 VPN 分组上的内层标签删除,将不含标签的 VPN 分组转发给正确的 CE 路由器,CE 路由器根据自己的路由表将分组转发到正确的目的地[7].

4 MPLS VPN 配置实例

MPLS VPN configuration instance

如图 3 所示,有两个 VPN 场点,一个是公司 A VPN,一个是公司 B VPN. 公司 A 中,路由器 R1 与路由器 R6 中运行 RIPv2 路由协议. 公司 B 中,路由 R7 运行 OSPF 路由协议,R8 运行 EIGRP 路由协议. MPLS 骨干网中运行 IS-IS 路由协议. R1、R6、R7、R8 都是 CE 路由器,R2、R5 是 PE 路由器,R3、R4 则是 P 路由器.

对各个路由器进行配置:

1) 在 R2、R3、R4、R5 上运行 IS-IS 路由协议.

2) 为 PE 路由器 R2、R5,P 路由器 R3、R4 配置 MPLS.

3) 在 PE 路由器 R2、R5 上配置 BGP 协议(配置 BGP 协议是为了启用 MP-BGP,用于 PE 路由器之间交换 VPN 路由)并激活 R2、R5 路由器的 MP-BGP 协议.

4) 在 R2、R5 路由器上配置 VRF,即 VPN 路由

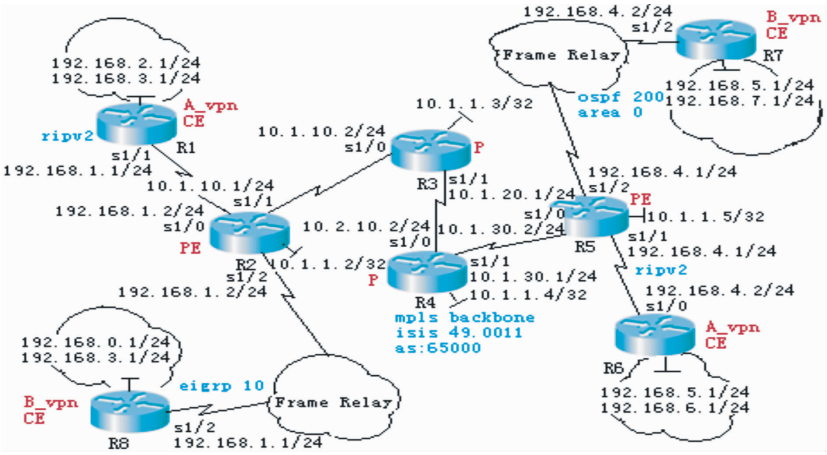

图 3　MPLS VPN 实例配置实验

Fig. 3　MPLS VPN configuration instance

转发表. 如图 4 所示. 配置完成后在 R5 上输入 show ip vrf detail 命令,查看 VRF 信息. 由图 4 可知,场点 A 的 VRF 表名称为 A_vpn,RD 为 65 000:100,RT 为 65 000:1 000.

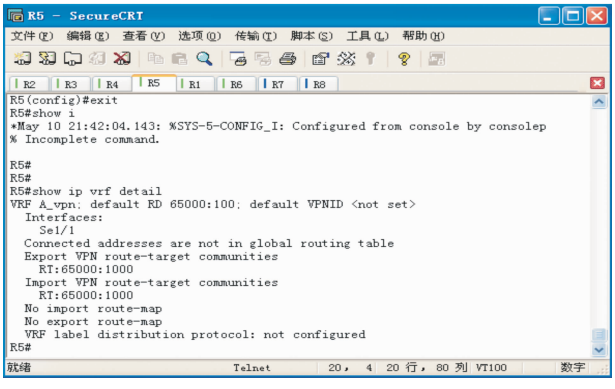

图 4　R5 路由器的 VRF 表

Fig. 4　VRF list of R5 router

5）在 R1 与 R2、R6 与 R5 路由器上配置 PE 与 CE 之间的 RIPv2 路由协议,并在 R2、R5 上进行 MP-BGP 与 RIPv2 之间的路由重发布.

6）在场点 A 中,使用 show ip route 命令在 R1 与 R6 上查看各自的路由表,以确认 MPLS VPN 配置成功,通过 ping 命令确认路由的有效性. 如图 5 所示,R1 学习到了 R6 的路由条目,并且可以 ping 通 R6 环回口地址 192.168.5.1. 如图 6 所示,R6 学习到 R1 的路由条目,并且可以 ping 通 R1 的 serial 1/1 口地址 192.168.1.1.

7）在 R2 路由器上使用 show ip bgp vpnv4 vrf A_vpn 命令,查看 MP-BGP 在 A 场点的路由信息表. 如图 7 所示,可以看到 R2 通过 MP-BGP 学习到了远

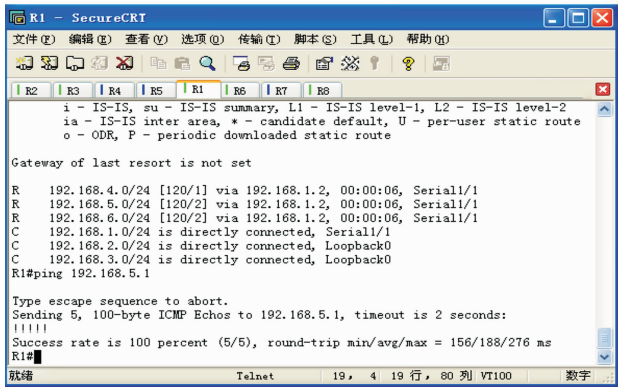

图 5　R1 的路由条目及其与 R6 的连通性

Fig. 5　R1 routing lists and R1-R6 connectivity

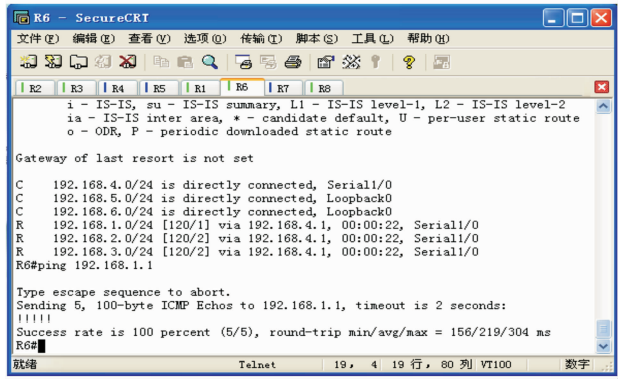

图 6　R6 的路由条目及其与 R1 的连通性

Fig. 6　R6 routing lists and R6-R1 connectivity

端 A 场点 192.168.4.0、192.168.5.0、192.168.6.0 这 3 个条目. 到此 A 场点利用 MPLS 技术建立 VPN,配置成功.

8）如前所述步骤,配置场点 B 的 MPLS VPN. 当

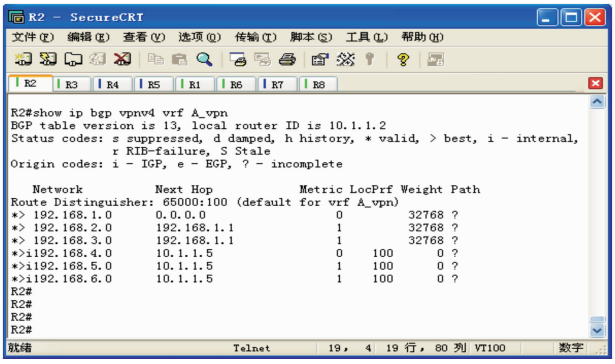

图 7　场点 A 在 R2 路由器的 VRF 表

Fig. 7　R2 router VRF list in field point A

然,要注意的是 PE 与 CE 路由器,即 R8 与 R2,R7 与 R5 中运行的是不同的路由协议,分别是 EIGRP 和 OSPF 路由协议,而不是 A 场点中所运行的 RIPv2 路由协议.

5　MPLS VPN 的安全性

MPLS VPN security

5.1　地址空间的分离

在 MPLS VPN 中,对于不同的 VPN,地址空间是完全独立的. 所有连接到一个 MPLS VPN 网络的用户都能使用整个空间的 IP 地址,而且能成功地操作企业内部网的 VPN,不会与其他 VPN 冲突,也不会在核心网络造成网络阻塞. 通过在 PE 路由器上对与之相连的用户使用不同的 VRF,可以完成地址分离[5]. 每个 VPN 都产生一个独立的 VRF,因此不会受到该 PE 路由器上其他 VPN 的影响. 在穿越 MPLS 核心到其他 PE 路由器时,这种隔离是通过为 MP-BGP 增加唯一的 VPN 标识符来实现的,即必须为所有的 VPN 路由准备一个 64 位的路由辩识符,形成一个 VPNv4 地址. MP-BGP 穿越核心网,只是把路由信息重新分发给其他 PE 路由器,并保存在其他 PE 的特定 VPN 的 VRF 中,而不会把这些 BGP 信息重分发给核心网络. 所有穿越 MPLS 网络的每个 VPN 路由是相互隔离的.

5.2　核心网络的不可见性

核心网络包括寻址和拓扑结构在内的体系结构对于一个用户 VPN 是不可见的. 对于核心网络来说,用户 VPN 的信息也不可见. MP-BGP 在 PE 路由器之间传输 VPN 信息和标签,在核心网络中只是执行转发的功能. 核心网络的地址可以通过配置命令 no mpls ip propagate-ttl forwarded 使得它们在 VPN 中不被显示,这样可以减少 C 网络对 PE 路由器进行拒绝服务攻击(DoS).

5.3　防止标签的欺骗

在 IP 网络中,包的交换是基于源 IP 地址和目的 IP 地址,这样就会出现替换包中的 IP 源地址和 IP 目的地址,达到欺骗攻击的效果. 在 MPLS 网络中交换是基于标签的,路由器不会在没有激活标签交换的接口上接受标记过的分组. 标签交换不会在通向 CE 路由器的 PE 路由器接口上出现,标记的工作应该是在 PE 路由器上完成,所有 PE 路由器不接收来自 CE 路由器的任何标记过的包,因此,任何一个从 CE 路由器到达 PE 路由器上标记过的分组将被丢弃,这样标签欺骗就不可能了[8]. 在到达 PE 路由器之前,CE 路由器中的包,有可能被替换了源 IP 地址或目的 IP 地址,但因为 MPLS VPN 具有地址分离的功能,所以这种欺骗会在客户自己的 VPN 中才有效,而不能攻击其他客户网络.

5.4　邻居的认证

为了加强 MPLS VPN 网络的安全性,可以在不同的路由器上做对应的认证,这样可以防止路由器受到来自相邻路由器的欺骗性更新操作,也可以用于验证来自标签分发端的更新操作. 邻居认证可以通过边界网关协议(BGP)、中间系统到中间系统(IS-IS)、增强内部网关路由协议(EIGRP)、开放最短路由优先(OSPF)、路由选择信息协议第 2 版(RIPv2)以及标签分配协议(LDP)来实现.

6　结论

Conclusion

与传统的 VPN 相比,MPLS VPN 吸收了它们的优点,用户可以在现有的接入业务上获得此服务,并不需要自己搭建 WAN 网络,这样可以降低企业的运营成本. 企业内部网络拓扑的变化,可在 VPN 上操作,而对于服务提供商网络则无需重新配置,并且可以把路由策略与管理工作部分交由服务提供商进行. MPLS VPN 为用户提供灵活、安全、实时的传输需求,它必将是未来构建 VPN 技术发展的方向,具有广阔的应用前景.

参考文献

References

[1] Rosen E, Rekhter Y. BGP/MPLS IP virtual private network (VPNs)[S]. RFC4364,2006:2

[2] Rosen E, Rekhter Y. BGP/MPLS VPN fundamentals [S]. RFC2547,2001:9
[3] Vitch P. Scalability and functionality challenges for MPLS VPN networks[J]. The Journal of the Communications Network,2007,6(2):38-44
[4] Welcher P J. Enterprise buyer's guide to Layer 3 MPLS VPN service[J]. Enterprise Network & Servers,2005(11):18-20
[5] 李频,唐家益,陈丹伟,等. 虚拟专用网分类和比较研究[J]. 计算机工程,2006,32(22):133-135
LI Pin,TANG Jiayi,CHEN Danwei,et al. Study on classification and comparison of virtual private network[J]. Computer Engineering,2006,32(22):133-135
[6] 侯剑峰,马明凯. MPLS VPN 中 PE-CE 互连仿真研究[J]. 计算机工程,2010,36(12):123-125
HOU Jianfeng,MA Mingkai. Research on PE-CE connection simulation in MPLS VPN[J]. Computer Engineering,2010,36(12):123-125
[7] 韩海雯,张潇元. 基于 BGP 协议的 MPLS VPN 构建机制分析[J]. 计算机工程与设计,2008,29(5):1104-1107
HAN Haiwen, ZHANG Xiaoyuan. Research on construction of BGP/MPLS VPN[J]. Computer Engineering and Design,2008,29(5):1104-1107
[8] 任金秋,马海龙,汪斌强. 跨域 BGP/MPLS VPN 在高性能路由器中的实现[J]. 计算机工程,2009,35(3):126-129
REN Jinqiu,MA Hailong,WANG Binqiang. Implementation of inter-AS BGP/MPLS VPN in high-performance router[J]. Computer Engineering,2009,35(3):126-129

MPLS VPN implementary mechanism and configuration

FU Desheng[1] XIAO Jieqin[1]
1 School of Computer and Software,Nanjing University of Information Science & Technology,Nanjing 210044

Abstract This paper discusses the implementation of MPLS VPN,detailing in its realization modes,components,features,working principle and data forwarding process,and gives the instance of MPLS VPN configuration,finally analyes its security.

Key words MPLS VPN;implementation of mechanism;configuration;BGP;VRF