宽带通信网---- MPLS VPN 及相关关键技术

一、 VPN 及其特点

传统 VPN 的隧道往往是通过手动配置的静态隧道，很难根据网络的实际情况 进行优化配置，灵活性差，且运行一段时间后容易出现效率下降的问题。同时传 统 VPN 中 IP 地址空间不能共享，网络用户数受 IP 地址总数及地址分配规则的限 制很大，用户数量受到了制约。即使可用的地址数仍然很可观，但也对一些特殊 的应用产生了障碍[1]。

MPLS_VPN 的出现解决了以上两个问题，MPLS_VPN 是一种在传统 VPN 基 础上结合 MPLS 技术的改进型网络技术。利用 MPLS 技术的特性可以有效解决以 上两个问题。MPLS 技术中的 LSP（Lable switching path）隧道解决了隧道动态建 立、维护、撤销的问题。MPLS 网络使用标签进行报文转发的特性，使得不同的用 户可以使用相同的 IP 地址，并同时在公网上进行通信。MPLS_VPN 作为一种 2.5 层技术，很好地粘合了 IP 网络的路由功能和以太网的高效传输。极大地提高了网 络的灵活性和传输效率[2,3,4]。

MPLS 报文的结构如图 1-1 所示

二层头部	MPLS 头部	三层头部	载荷

图 1-1 MPLS 报文的结构

MPLS 头部位于二层头部和三层头部之间，其结构如图 1-2 所示

Lable	EXP	S	TTL

图 1-2 MPLS 头部结构

MPLS 头部共 32bit，其各字段的意义如下。

Label ：标签，长度 20 个比特，标签值字段是转发的依据。

Exp：3 个比特，保留，没有明确规定。

S：堆栈标识符。用于标识 MPLS 标签是否为最低层的标签(值为 1 时即表示 为最低层标签)。

TTL：8 个比特，生存周期，用于避免路由环路。与 IP 头部中的 TTL 类似。每经过一路由器，TTL 值减 1(值为 0 即表示无论该报文是否传送到目的地，网络 都将其丢弃)。

MPLS 网络的基本构成要素和主要概念有：

转发等价类（FEC，Forwarding Equivalence Class），是在转发过程中以相同的 方法处理的报文集合。所谓相同的方法，具体来说就是相同的目的或相同的

通道。

标签（Label），如前所述，标签是 32bit 长度的标识符。在 MPLS 网络中，路 由器依据标签进行下一步操作。标签与 FEC 相关联，一个 FEC 可以有不止一个标 签，而一个标签只能对应一个 FEC。

标签边缘路由器(LER， Labeled Switching Edge Router) ，部署在 MPLS 网络 的边缘，根据数据入网出网的不同，分为入口（Ingress）LER 和出口（Egress）LER。 入口 LER 负责判断报文的 FEC，并加上这些 FEC 所对应的的标签。出口 LER 负 责检查报文的标签，判断是否要从本节点送出网络，如果是，出口 LER 将把报文 的标签去除，并发往相连的用户网络。

标签交换路由器(LSR，Label Switching Router) ，位于 MPLS 网络的核心区域， 它提供加标签和标签交换功能。

标签交换通道(LSP，Label Switched Path) ，一个 FEC 的数据流，在不同的节 点（LSR 或 LER）被加上标签，数据转发按照标签的指示进行。报文在网内所走 的路径就是 LSP。

加标签（PUSH），入口 LER 在报文的二层头部和三层头部间加上初始标签，或是 LSR 在旧标签前加新标签。

交换标签（SWAP），在转发过程中 LSR 依据标签的信息对栈顶标签进行替换。

弹出标签（POP），出口 LER 或 LSR 去掉报文的标签。以准备将报文发往用户 子网或减少标签的深度。

一个 MPLS 网络的结构如图 1-3 所示：

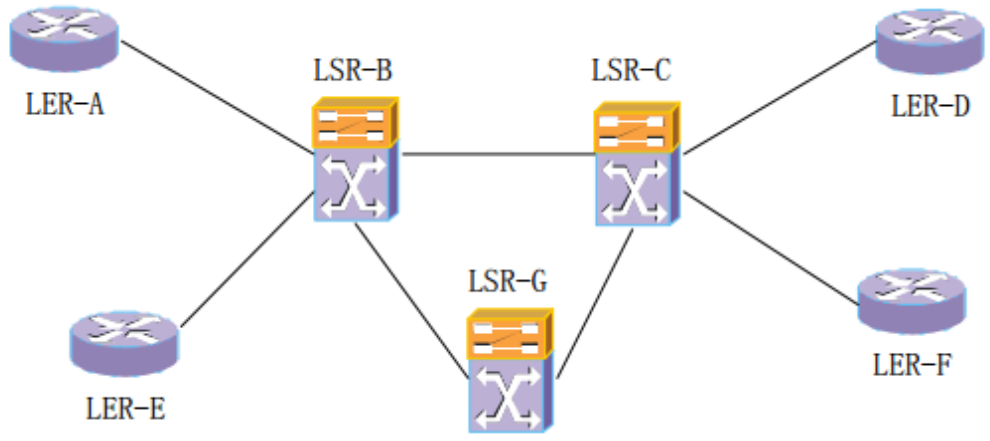

图 1-3 MPLS 网络结构示意图

假设现在一个 IP 包从 LER-A 入网，并假设其 LSP 按 A-B-C-D 的路径转发。 LER-A 即为入口 LER，它将分析 IP 包头部，从而确定该报文所属的 FEC 类型， 在 IP 包头前进行根据该 FEC 的路由信息加标签操作，然后根据标签转发表将 IP 包发往 LSP 指定的出口，LSR-B 收到带有标签的报文后，对标签进行分析，进行 交换标签或加标签的操作，并根据 LSP 将 IP 包发到相应的出口。LSR-C 是倒数第 二跳的 LSR，它不仅会分析栈顶标签本身并进行弹出或交换操作，还会检查标签 的堆栈数，如果标签数大于 1，它将把栈顶以外所有的标签全部弹出，确保出口 LER 收到的包只有一层标签。LER-D 是出口 LER，它分析标签，并对照转发表， 发现自身是最后一个节点。LER-D 将最后一个标签弹出，将 IP 包发到目的用户网 络。

MPLS_VPN 是 MPLS 网络与 VPN 技术的结合，即在 MPLS 网络上承载 VPN 业务，网络结构如图 1-4 所示：

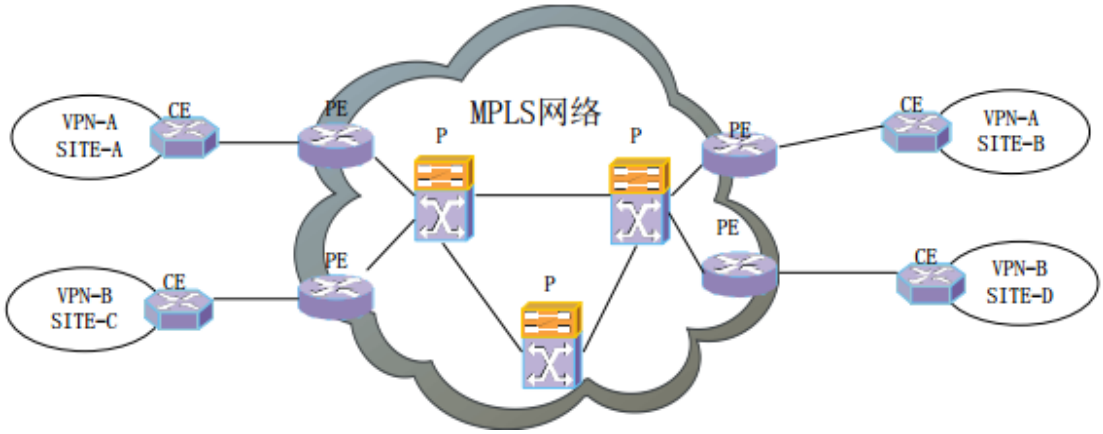

图 1- 4 MPLS VPN 网络结构示意图

用户边缘设备（CE，Costom Edge）是一个 VPN 概念，位于用户网络的出口，直接与服务供应商网络的 PE 设备相连。CE 相当于 MPLS 网络的用户网络的边缘 设备。本文所要重点探讨的正是这样一种设备的设计。

提供商边缘路由器（PE，Provider Edge Router）是一个 VPN 概念，位于骨干 网的边缘，负责用户数据的接入。PE 相当于前面提到的 LER 设备。在 MPLS VPN 中 PE 设备即负责根据标记分发协议和转发标签信息库（FLIB，Fowarding Label Information Bank）中的转发信息进行入网和出网操作。

提供商路由器（P，Provider Router）是一个 VPN 概念，位于骨干网的核心区 域，负责路由和转发工作。P 相当于相当于前面提到的 LSR 设备。在

MPLS VPN 中 P 设备按照路由协议进行报文的转发。

标记分发协议是 MPLS VPN 的信令控制协议。负责对 FEC 进行分类，标签的 分配，分类、分配结果的传输，PW 线路的建立和维护。目前主要有 MPLS LDP 和 MPLS BGP 两类协议。该类协议可以自主地分配 VPN 资源，提升了 VPN 结构 的灵活性。

FEC 的对象可以是目标 MAC 或目标 IP 地址。这一区别将 MPLS VPN 分为 MPLS L2VPN 和 MPLS L3VPN。MPLS L3VPN 是一种基于 IP 路由方式的 MPLS VPN 解决方案。该方案中的路由设备依据路由表和提前配置好的 LSP 信息以 IP 报文的目的 IP 地址为依据进行标签的分发和数据转发。MPLS_VPN 的重要特性还 有转发实例 VRF、路由标识符 RD、目标路由 RT，其中 RD 与 IP 地址的结合而成 的 VPN-IP 地址的使在 MPLS VPN 中复用地址变为可能。

MPLS L2VPN 又分为两种，一种是点到点的 VLL 技术和 VPLS 技术。

二、 VPLS 技术及接入技术

VPLS 结合了以太网技术和 MPLS VPN 技术的优势，实现了传统 LAN 的全部 功能，其主要目的是通过运营商提供的 MPLS 网络连接地域上隔离的多个由以太 网构成的 LAN，使它们像一个 LAN 那样工作[2,3,5]。服务提供商利用 VPLS 技术在 MPLS 骨干网络上为用户网络模拟了一个以太网 桥，基于 MAC 地址或者 MAC 地址加 VLAN 标识来做出标签发放和转发决策。一 个 VPLS 实例可以在所属的多个 PE 的多个站点间进行全互通，即允许 CE 设备直 接跟所有与该 VPLS 实例所辖的 PE 接口关联的其它 CE 通信。在 CE 设备看来， 服务提供商网络是一个以太网桥（以太网交换机）。 VPLS 的体系架构如图 2-1 所示。

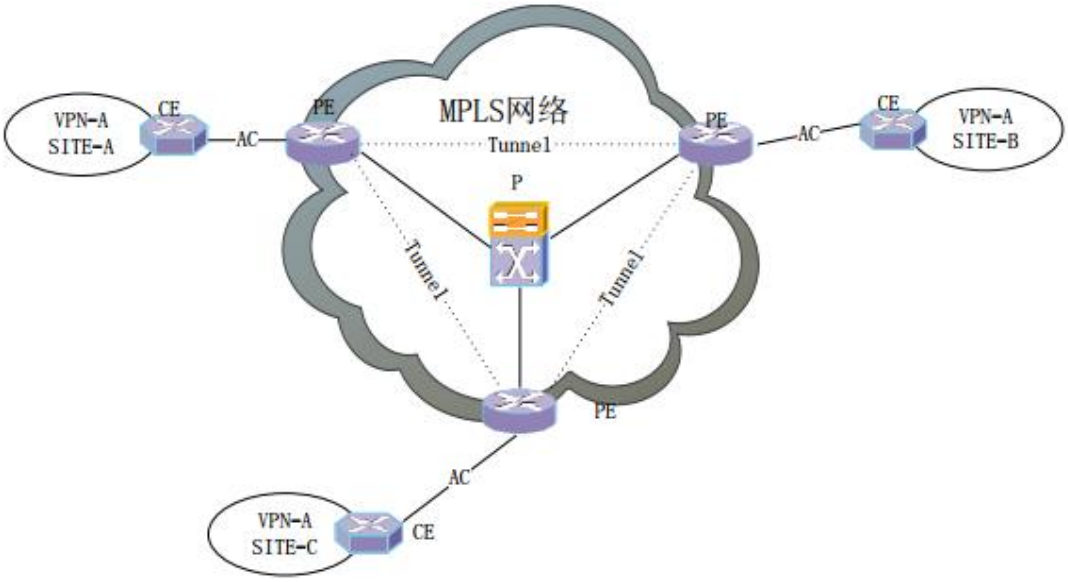

图 2-1 VPLS 网络结构示意图

可以看出 VPLS 完全继承了标准 MPLS VPN 模型的结构，但也有一些特有的 组成部分和概念[2,3,4,5]。

VSI（Virtual Switch Instance）虚拟交换实例，VPLS 实例在一台 PE 设备上体 现为一个以太网桥功能实体，每一台 PE 上都为一个 VSI 配置一个 FLIB 库用于存 放 MAC 和标签转发信息，其中最重要的信息就是 VSI 编号和该编号实例下辖的目 的 MAC 地址或 MAC 地址+VLAN TAG，再加上该地址应发出的端口，根据该表 的结合进行二层报文转发。

接入线路（AC，Attachment Circuit）是 CE 与 PE 之间的线路，一个 AC 一般 只对应一个 VSI。

隧道（tunnel），用于承载 PW，一个隧道上可以承载多条 PW。隧道是 PE 间通 过配置而形成的逻辑通道，完成 PE 之间的数据透明传输。隧道可以是通过物理线 路直连，也可以是通过 P 设备进行中继连接（示意图中的三个隧道都是经过 P 设 备中继形成的），隧道可以是 MPLS 或 GRE 隧道等，可以被视为 LSP 在 VPLS 中 的体现。

伪线（PW，Pseudo Wire）是 PE 和 PE 间的关于一个 VSI 的双向虚连接，由两 个方向相反的虚电路构成，只有两个方向的虚电路都连通才被认为 PW 是连通的。 一个 PW 只能承载一个 VSI 的报文。

PW 信令协议（PW Signaling），VPLS 的 PW 信令协议相当于 MPLS 通用模型 中 LDP 协议，负责 PW 的建立、维护、拆除以及这些信息的传输。

根据采用信令协议的不同，VPLS 又可以分为 Martini（LDP）方式和 Kompella（扩展 BGP）方式。

采用扩展 LDP（远端 LDP 会话）作为 PW 信令协议的 VPLS，称为 Martini 方 式的 VPLS。Martini 方式的优点是实现简单。但 LDP 不能提供自动发现新的 VPLS 成员。新的 PE 加入时，每个与该 PE 设备相关的 PE 上都需要进行手工配置。

采用扩展 BGP 作为 PW 信令协议的 VPLS，称为 Kompella 方式的 VPLS。 Kompella 方式可以通过配置 VPN Target 实现了 VPLS 成员的自动发现、增加或删 除。新 PE 时入网时无需手工配置，具有较好的可扩展性，不过 BGP 协议本身比 较复杂，对设备的运算能力要求较高。

由于标签的介入，VPLS 报文的封装方式在 AC 和 PW 上是明显不同的。

根据是否带有供应商的 VLAN TAG，AC 上的报文封装方式可以分为两种：VLAN 接入和 Ethernet 接入。

VLAN 接入：报文的格式如图 1-6，CE 发送给 PE 或 PE 发送给 CE 的以太网 帧头带有一个 VLAN TAG，该 TAG 是一个“服务界定符”，主要为了解决在同一 PE 端口下出现多个用户网络时如何区分的问题。服务界定符的 TAG 称为 P-TAG。

二层头部	P-TAG	载荷

二层头部	P-TAG	U-TAG	载荷

图 2-2 VLAN 接入模式的报文结构

Ethernet 接入：报文的格式如图 2-3，CE 发送给 PE 或 PE 发送给 CE 的以太网 帧头中没有服务界定符，如果此时帧头中有 VLAN TAG，也只是用户网络内部 VLAN TAG，对于 PE 设备没有意义。这种用户内部 VLAN 的 TAG 称为 U-TAG。

二层头部	载荷

二层头部	U-TAG	载荷

图 2-3 Ethernet 接入模式的报文结构

在 PW 上，VPLS 报文的格式（如图 2-3）与一般 MPLS VPN 报文的封装格式 有一点不同，那就是一个 VPLS 报文拥有至少两个标签而不是一个[2,3,4,5]。这两个 标签一个是 PW 标签，用于区分同一个隧道内不同的 PW 信息，目的

PE 设备在收 到包后可以据此判断该报文属于哪一个 VSI，并发往相应的 AC，该标签在整个传 输过程中处于不可见状态，不会发生变化。另一个标签是公网标签，公网络内的 P 设备或 PE 设备据此在网内进行转发， LSP 路径上的各个节点可能会对公网标签进行 PUSH、SWAP、POP 操作。

以太网头部	公网标签	PW 标签	数据

图 2-4 PW 线路的双标签结构

根据在传输过程中是否带有 P-TAG，PW 上的报文封装方式又分为两种：Raw 模式和 Tagged 模式。

Raw 模式下，报文格式如图 1-9 所示。PW 上传输的帧不能带 P-TAG：对于 CE 发往 PE 的上传报文，如果带有服务界定符，PE 将其去除后再压入 PW 标签和 隧道标签后转发；如果收到不带 P-TAG 的报文，则直接压入 PW 标签和隧道标签 后转发。对于 PE 发往 CE 的下行报文，根据 PE 配置选择添加或不添加 P-TAG 后 转发给 CE，但是它不能对包内 TAG 的内容作任何改变。

二层头部	公网标签	PW 标签	数据

二层头部	公网标签	PW 标签	U-TAG	数据

图 2-5 Raw 模式的报文格式

Tagged 模式下，报文格式如图 1-10 所示。PW 上传输的帧必须带 P-TAG：对 于 CE 发往 PE 的上传报文，如果收到带有 P-TAG 的报文，保留 P-TAG，压入 PW 标签和隧道标签后转发；如果收到不带 P-TAG 的报文，则添加一个对端 PE 期望 的 VLAN TAG 或空 TAG 后，再压入 PW 标签和隧道标签后转发。对于 PE 发往 CE 的下行报文，根据实际配置选择重写、去除或保留 P-TAG 后转发给 CE。

二层头部	公网标签	PW 标签	P-TAG	数据

二层头部	公网标签	PW 标签	P-TAG	U-TAG	数据

图 2-6 Tagged 模式的报文格式

VPLS 为用户网络模拟了一个以太网桥，基于 MAC 地址或者 MAC 地址加 VLAN TAG 来做出转发决策。一个 VPLS-VPN 的每个 PE 设备都为该 VPN 建立一 个 VSI，并为 VSI 维护一张 MAC-标签地址表，该表存放在 PE 设备的 FLIB 库内。 该机制具有泛洪和转发、MAC 地址学习和老化的功能，以便实现报文的转发。

参考文献

[1] Douglas E.Comer 著，林瑶，张娟，王海等译.用 TCP/IP 进行网际互联-原理、协议与结构 [M].北京：电子工业出版社，2007，21-85

[2] 李昌群.基于 VPLS 二层 VPN 技术的研究及实现[D].杭州：杭州电子科技大学，2010 年， 8-34

[3] 丁娟.基于二层 MPLS VPN 的 VPLS 的研究与实现[D]. 西安：西北工业大学，2007 年

[4] Ghein，L.D. 著.陈麒帆译.MPLS 技术架构[M].人民邮电出版社，2012 年,1-214

[5] 赵曦.MPLS-VPN 组网和的规划与实现[D]，北京:北京邮电大学，2012 年，3-21