---------------------------------------------------------------------

# 文档声明

## 合规性提示

本文档仅用于MPLS VPN技术原理及应用场景的知识科普，不涉及任何翻墙工具的推荐、使用指导或技术破解内容。根据中国法律法规，未经许可私自使用VPN访问境外网络属于违法行为，相关使用需严格遵守国家网络安全管理规定及企业合规要求。

## 版权与使用说明

本文档所有内容（包括技术原理、分类说明、应用场景等）均为作者原创整理，仅供个人学习、研究参考使用，禁止用于任何商业用途（如付费课程、商业出版物、盈利性内容分发等），禁止以任何形式（包括完整转载、节选、截图、二次编辑后转发等）在其他平台传播。任何获取、使用本文档的用户，均需完整保留作者信息及本声明内容，不得抹去或修改原创标识。

## 内容免责

本文档内容仅为技术知识梳理，不构成专业指导建议。因引用本文档内容导致的任何直接或间接后果（包括但不限于信息误差、合规风险、第三方投诉等），作者不承担法律责任。文档中提及的技术方案（如MPLS VPN协议、实现流程）仅作原理说明，具体使用需结合当地法律法规及企业内部规范。

---------------------------------------------------------------------

# MPLS VPN

## 1 简介

MPLS VPN（多协议标签交换虚拟专用网络）是一种基于MPLS技术实现的广域虚拟专用网络，能够在公共运营商网络中为不同用户提供隔离、安全、高效的私有通信服务。其核心是通过标签转发和路由隔离机制，实现不同 VPN 用户的数据在共享骨干网中独立传输。

## 2 核心组件

**用户边缘路由器（CE，Customer Edge）**：位于用户网络边缘，与用户终端或者局域网相连，负责与运营商边缘路由器进行交互。

**运营商边缘路由器（PE，Provider Edge）**：位于运营商网络边缘，负责与用户边缘路由器进行交互并与运营商网络连接交互。MPLS VPN的核心设备，负责VPN路由学习、分发、标签分配、数据标签封装与解封装。

**运营商核心路由器（P，Provider）**：位于运营商骨干网中，仅负责标签数据转发（不同于路由表，MPLS依靠标签交换路径LSP快速转发数据）。

**VPN v4地址**：由“路由分区符RD + 私网IP”组成，用于解决不同VPN中私网IP冲突的问题（使用BGP协议需要唯一标识路由）。

**路由目标（RT，Route Target）**：分为导出目标（Export Target）和导入目标（Import Target），控制VPN路由的导入和导出过程，实现VPN隔离（隔离的实现依赖与“只有匹配的路由才能被接收”）。

**标签**：MPLS中用于快速转发的标识，分为外层标签和内层标签。外层标签是骨干网LSP标签，用于P路由器的转发。内层标签是VPN标签，用于让PE快速识别VPN路由。

## 3 工作过程

MPLS VPN的工作流程可分为**路由交互**、**标签分发**、**数据转发**三个核心阶段，以下结合具体场景（两个属于同一VPN的用户站点A和站点B）详细说明。

### 3.1 路由交互 —— 建立VPN路由表

此阶段的目标是让同一VPN的不同站点（如站点A和站点B）互相学习到对方的路由，同时确保不同 VPN 的路由不混淆。【PE之间是相互流通信息的，在建立A到B的VPN通道时，也能够同时建立B到A的VPN通道】

**1.CE与PE的路由交互**：站点A的CE1通过路由协议将本地用户的私网路由发给与其相连的PE1。站点B执行同样的步骤。

**2.PE对路由进行“VPN化”处理**：PE1收到CE1的私网路由后为其添加RD，形成唯一的VPN v4地址（将私网路由加上RD前缀，确保在VPN网络中地址的唯一性，比如：RD:IPv4为100:1:192.168.1.2/24），避免与其他VPN的同网段路由产生冲突。之后，PE1为该路由添加导出目标标签，用于标识这条路由属于哪一个VPN。

**3.PE之间的VPNv4路由1传递**：PE1通过MP-BGP协议将处理后的VPN v4路由（RD:IPv4:Export-Target）发送给其他的PE。在骨干网中，PE之间通过IBGP协议建立邻居关系，专门用于传输VPN v4路由（P路由器不参与此过程，仅负责转发BGP报文）

**4.PE对路由进行筛选与导入**：PE2收到PE1的VPN v4路由后，检查Export Target是否与本地的Import Target匹配，如果匹配，则说明该数据包是本VPN路径的，PE2将移除RD，将路由表转为私网路由并通过协议发送给CE2，是站点B学习到站点A的路由；如果不匹配，将丢弃数据包，实现VPN隔离。

**5.补充说明PE之间是如何传递信息的**：

首先，运营商会对骨干网使用IGP（内部网关协议，包括OSPF和IS-IS等动态路由协议）保持骨干网中的所有设备彼此互通（大致上就是周期性的向真实的物理邻居发送自己的路由表摘要并根据邻居的路由表摘要填充路由拓扑数据库，在各个邻居都完成路由拓扑更新时使用最短路径算法计算与各个设备的联通路径并维护该路径的路由）。

然后，使用MP-BGP建立PE之间的邻居关系，PE之间的邻居关系并不是物理直连的，而是基于Loopback地址和IGP可达性的多跳相连（管理员在PE1上配置“与PE2的Loopback地址建立MP-BGP邻居关系，允许多跳。PE1通过IGP学习到路由，将BGP建邻报文通过中间路由器P转发到PE2的Loopback地址上。路由器P通过IGP学习到路由，能够顺利的将报文转发到PE2上。这样PE1和PE2就成了逻辑邻居）。

最后建立VPN v4路由只需通过MP-BGP协议构筑的邻居关系转发VPN v4路由即可建立VPN v4通道。

总的来说，骨干网中的PE是扮演者逻辑上点到点的VPN连接。而P通过OSPF等动态路由协议（隶属于：IGP，内部网关协议）和MP-BGP协议进行PE逻辑邻居构筑，并负责在真实的网络环境中传输PE之间的消息。

### 3.2 标签分发 —— 建立标签转发表

MPLS的核心是“基于标签转发”，而非传统IP的“基于最长前缀匹配”，因此需要为VPN路由分配标签并建立转发表。【传统IP的“基于最长前缀匹配”是为了应对可变长的子网掩码而设计的，具体来说，当在一个路由器中同时出现192.168.1.2/24与192.168.1.2/25的路由，会优先选择后者】

**1.内层标签（又称VPN标签）分配**：当PE1学习到CE1的私网路由后，会为这条路由分配一个内层标签，用于识别该路由属于站点A所在的VPN【因为可能出现一个PE连接的两个CE的私有网段相同的情况】。这个内层标签包含在MP-BGP的路由更新中，会随着VPN v4路由一起发送给PE2.【PE2要知道自己的数据包究竟是发给哪个CE的，否则PE1收到PE2的数据包也不知道该怎么发送】

**2.外层标签（又称骨干网标签）分配**：在运营商骨干网中，P和PE通过LDP（标签分发协议）或者PSVP-TE协议为骨干网的IP路由分配外层标签，依照外层标签建立LSP（标签交换路径）。详细的过程可参考[MPLS简介\_mpls节点如何处理数据包-CSDN博客](https://blog.csdn.net/2301_80444339/article/details/149673059?spm=1001.2014.3001.5501)【读者可能这一步有些不理解，因为阶段1已经建立了VPN通道为什么还要建立LSP呢？简单来说，LSP能够在骨干网中固定一条最优路径，实现高效转发。如果使用阶段一建立的VPN通道（实际上就是路由表中的项），那么每经过一个路由器都需要对IP头部进行解析决定下一跳去哪并还要重新封装IP数据包。换作是LSP，完全不需要解析IP数据包，只需要在数据包头部检查外层标签并替换成下一跳的标签，根据配置的标签表进行转发，效率比解析IP数据包并封装新的IP头部高很多（最理想的情况是一条VPN道独占一个外层标签，直接避免替换，直接转发）】

**3.标签转发表生成**：根据外层标签建立骨干网中的“标签——转发端口”映射，根据内层标签建立骨干网中的“标签——转发端口”映射。【这是LDP协议或者PSVP-TE协议自动完成的，无需人工设置标签与转发表】

### 3.3 数据转发 —— 基于标签的传输

**1.CE到PE的初始转发**：站点A的终端发送数据包（目的IP：192.168.2.1）到CE1，CE1根据路由表将数据包转发给PE1。

**2.PE1的标签封装**：PE1接收数据包后，检查目的IP属于站点B所在的VPN，查询标签转发表：

内层标签：对应目的路由的标签（如PE2分配的200，标识“目标 VPN”）；

外层标签：骨干网中PE1到PE2的LSP标签（如200，标识“转发路径”）。

PE1 将两层标签封装到数据包头部（先外层、后内层），发送给骨干网的 P 路由器。

**3.骨干网的标签交换**：P路由器接收数据包后，仅解析外层标签（200），查询本地标签转发表，将外层标签替换为下一跳的标签（如300），继续转发给下一个P路由器或PE2。整个过程中，P路由器无需解析IP地址或内层标签，仅通过外层标签快速交换，转发效率极高。

**4.PE2 的解封装与转发**：PE2接收数据包后，先剥去外层标签（300），露出内层标签（100）；

根据内层标签查询VPN转发表，确定该数据包属于站点B的VPN，剥去内层标签，露出原始IP数据包；

最后，PE2将数据包转发给CE2，由CE2送达站点B的终端。

### 3.4 隔离机制 —— RT的作用

MPLS VPN通过RT（路由目标）实现不同VPN的严格隔离，核心逻辑是：

1.每个VPN通道的PE在“导出”路由时，会给该路由打上Export Target（如100:100）；

2.其他PE只有配置了与该Export Target匹配的Import Target（如100:100），才会接收并导入该路由；

3.未匹配的PE会直接丢弃路由，确保不同VPN的用户无法互相访问。

## 4 保密问题

请注意，MPLS VPN本身并不具备加密功能，仅仅是依靠VPN隔离机制将运营商骨干网络的数据包进行隔离，很明显，这种情况是脆弱的。最常见的就是转发机制出现漏洞导致数据包错误转发，还可能面临着攻击者入侵运营商骨干网络或者“间谍”式数据泄露。

为了稳妥期间，通信双方在通过MPLS建立起高效、快速且稳定VPN通道后，要配合IPsec、TLS等加密协议进行通信。

**本文章归属 github 用户 WhatTheFuck-cyber**