MPLS VPN 技术原理与配置

MPLS（Multi-Protocol Label Switching）多协议标签交换
VPN　　（Virtual Private Network）虚拟专用网

==========

为什么选择 BGP 协议：
由于 BGP 的诸多优点对技术难点的解决提供了思路：
公共网络上的 VPN 路由数量庞大，BGP 是唯一支持大量路由的协议；
BGP 的报文基于 TLV 的结构，便于扩展；
BGP 可以承载附加在路由后面的任何信息，并作为可选属性传递给其他邻居。

3 个需要解决的问题：

1.本地路由冲突问题，即：在同一台 PE 上如何区分不同 VPN 的相同路由。
　　PE 设备怎么区分不同 VPN 客户的相同路由？
2.路由在网络中的传播问题，两条相同的路由，都在网络中传播，对于接收者如何分辨彼此？
　　冲突路由在公网中传播时，接收端 PE 如何正确导入 VPN 客户路由？
3.报文的转发问题，即使成功的解决了路由表的冲突，但是当 PE 接收到一个 IP 报文时，他又如何能够知道该发给那个 VPN？因为 IP 报文头中唯一可用的信息就是目的地址。而很多 VPN 中都可能存在这个地址。
　　PE 设备收到 IP 数据包后，如何正确的发送给目的 VPN

客户？

解决的方法：

1.本地路由冲突问题，可以通过在同一台路由器上创建不同的路由表解决，而不同的接口可以分属不同的路由表中，这就相当于将一台共享 PE 模拟成多台专用 PE。

可以通过在同一台 PE 设备上为不同的 VPN 建立单独的路由，这样冲突的的路由就被隔离开来；

VRF（VPN Routing and Forwarding table）VPN 路由转发表

2.在路由传递过程中，为不同的 VPN 路由添加不同的标识，以示区别。这些标识可以作为 BGP 属性进行传递；

RD　RT

增加了 RD 的 IPv4 地址称为 VPN-IPv4 地址，即 VPNv4 地址

RT（Route Target）封装在 BGP 的扩展 Community 属性中，

RD（Route Distinguisher）

将 VPN 路由发布到全局路由表之前，使用一个全局唯一的标识和路由绑定，以区分冲突的私网路由。

RT（Route Target）

使用 RT 实现本端与对端的路由正确引入 VPN

3 由于 IP 报文不可更改，可以在 IP 报文头前加一些信息。由始发路由器打上标记，接收路由器在收到带标记的的数据包时，根据标记转发给正确的 VPN。

MP-BGP 分发内层标签

==========

RD (Route Distinguisher)路由区分符

用于标识 PE 上不同 VPN 实例，全局唯一，其主要作用是实现 VPN 实例之间地址复用，与 IP 地址一起构成 12 Bytes 的 VPNv4 地址。
RD 与路由一起被携带在 BGP Update 报文中发送给对端。
RD 不具有选路能力，不影响路由的发送与接受。
RD 用来区分本地 VRF，本地有效。

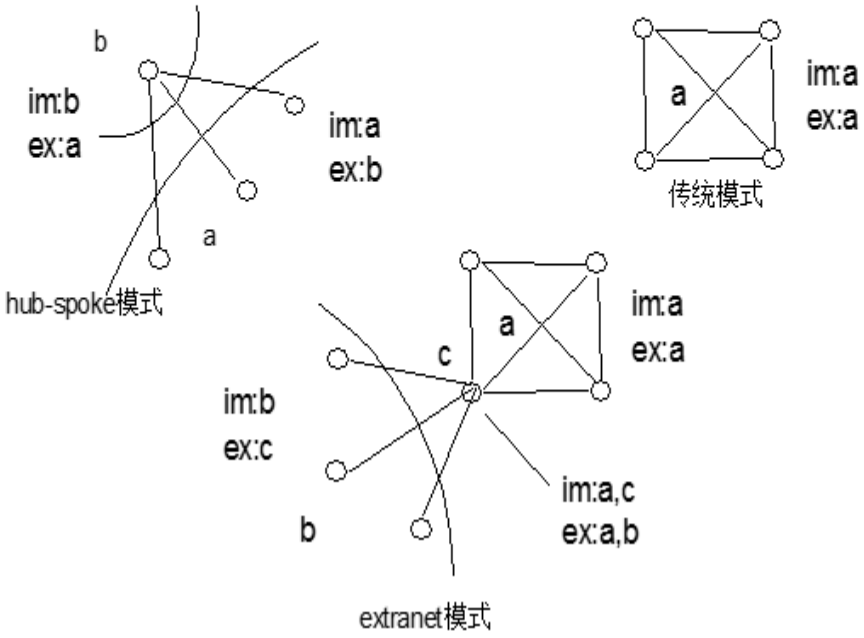
为了防止一台 PE 接收到远端 PE 发来的不同 VRF 的相同路由时不知所措，而加在路由前面的特殊信息。在 PE 发布路由时加上，在远端 PE 接收到路由后放在本地路由表中，用来与后来接收到的路由进行比较。

RT (Route Target) 路由目标

RT 是 VPNv4 路由携带的一个重要属性，它决定 VPN 路由的收发和过滤，PE 依靠 RT 属性区分不同 VPN 之间路由。
当从 VRF 表中导出 VPN 路由时，要用 Export RT 对 VPN 路由进行标记。
当往 VRF 表中导入 VPN 路由时，只有所带 RT 标记与 VRF 表中任意一个 Import RT 相符的路由才会被导入到 VRF 表中。
表明了一个 VRF 的路由喜好，通过他可以实现不同 VRF 之间的路由互通。他的本质就是 BGP 的 community 属性。

RT的灵活应用

由于每个RT Export Target与import Target都可以配置多个属性，例如：我对红色或者蓝色的路由都感兴趣。接收时是“或”操作，红色的、蓝色的以及同时具备两种颜色的路由都会被接受。所以就可以实现非常灵活的VPN访问控制。



从不同 PE 收到的相同路由靠 RD 区别
路由条目本端接受与否看 RT

举个生活的例子，RD 就是身份证，RT 就是护照。身份证只能有一张，护照可以很多张。
护照相同，就能进入相同的局域网。用在运营商的边界路由器上，RD 是一个 VRF 的身份证。RT 是这个 VRF 的护照，他可以导入很多不同的 RT。

==========

概念总结

VRF：在一台 PE 上虚拟出来的一个路由器，包括一些特定的接口，一张路由表，一个路由协议，一个 RD 和一组 RT 规则。

RD：为了防止一台 PE 接收到远端 PE 发来的不同 VRF 的相同路由时不知所措，而加在路由前面的特殊信息。在 PE 发布路由时加上，在远端 PE 接收到路由后放在本地路由表中，用来与后来接收到的路由进行比较。

RT：表明了一个 VRF 的路由喜好，通过他可以实现不同 VRF 之间的路由互通。他的本质就是 BGP 的 community 属性。

Label：为了防止一台 PE 接收到远端 PE 发给本地不同 VRF 的相同地址的主机时不知所措，而加在报文前面的特殊信息。由本地 PE 在发布路由时加上，远端 PE 接收到保存在相应的 VRF 中。

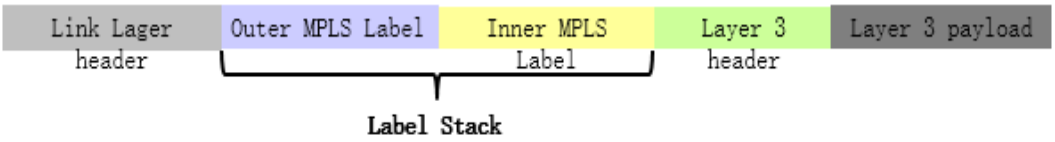
SITE：一个 VRF 加上与其相连的所有的 CE 的集合。

VPN：是一些 SITE 的集合，这些 SITE 由于共享了相同的路由信息可以互通。

==========

两层标签

内层标签由 MP-BGP 生成并在 VPNV4 的邻居中传递，用于区分不同的 VPN 流量；
外层标签由 MPLS 的 ldp 协议生成，用于解决传输的可达性问题

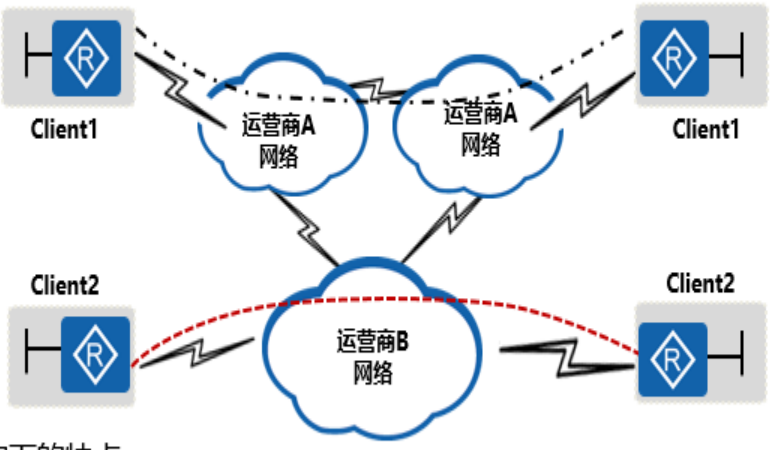


- 使用标签嵌套解决数据转发过程中冲突路由的查找问题。

前言

- 随着设备硬件性能不断提升，MPLS在提高数据转发速度上的优势逐渐弱化，但其支持多层标签嵌套和设备内转控分离的特点，使其在VPN、TE等新兴应用中得到广泛应用。
- 传统的VPN存在一些固有缺陷，导致客户组网时很多需求不能满足。MPLS VPN将传统的两种VPN模型整合到一起，推动了VPN的发展。

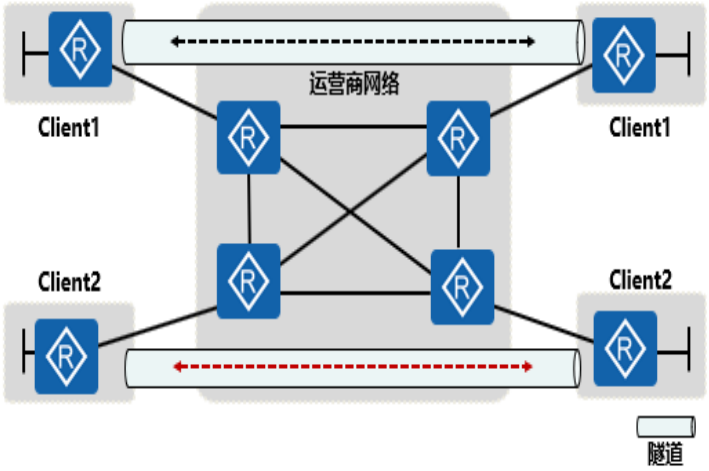
VPN技术的产生 (1)



- 专线有如下的特点:
  - 线路专有，安全性高，不同用户之间物理隔离;
  - 价格昂贵;
  - 使用不充分，带宽浪费严重。

- 最初，为了实现两个站点之间跨越公网通信，并保护私网的安全，人们通常采用专线来实现私网之间的连接。由于专线固有缺陷的存在，随着复用技术的出现，一些新的共享带宽技术逐渐替代了专线。

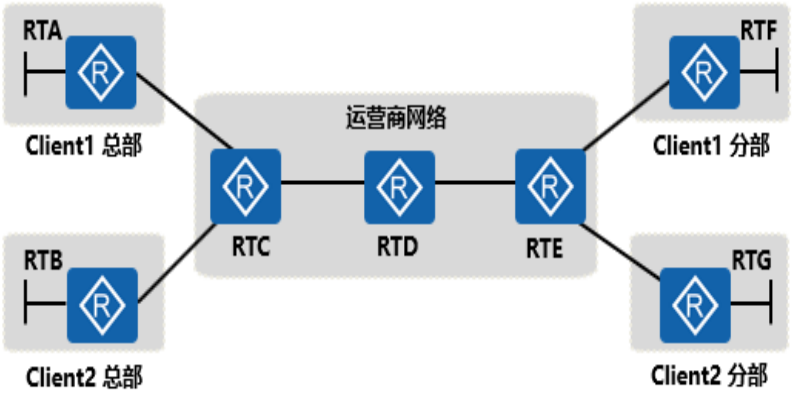
VPN技术的产生 (2)



- 新的共享带宽的技术有帧中继、X.25等，这些技术其实是一种逻辑的隔离技术，就好像在两个站点之间跨越公共网络建立了专用的隧道，站点通过隧道实现通信。

- 这些共享带宽的技术，由于能提高带宽利用率，价格相对于专线比较便宜，因此成为构成早期 VPN 网络的主要技术。
- VPN 网络的特点如下：
- 使用共享的公共网络环境实现各私网的连接；
- 不同的私有网络之间相互不可见。

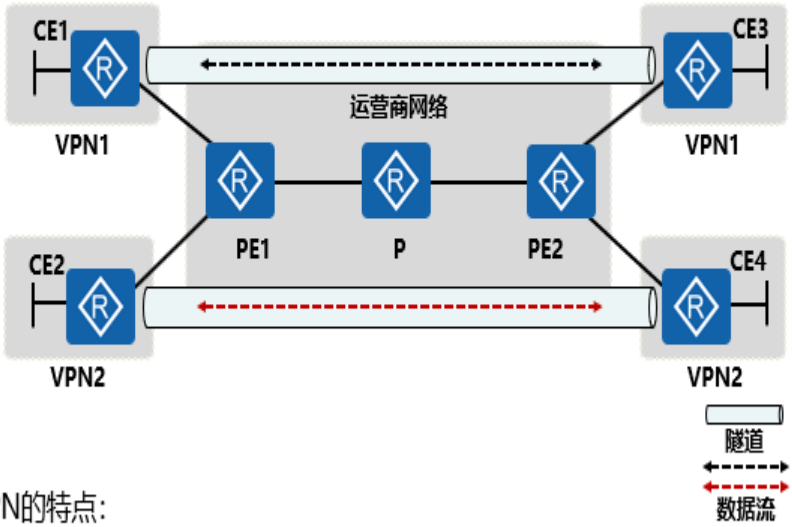
企业用户接入运营商的网络结构



- 企业用户的网络设备：
  - RTA，RTB，RTF与RTG被称为CE（Customer Edge）设备。
- 运营商的网络设备：
  - RTC与RTE，设备直接与客户设备相连，被称为PE（Provider Edge）设备；
  - RTD，是运营商网络中的骨干设备，被称为P（Provider）设备。

- 如图所示：各设备的作用：
- CE（Customer Edge）：用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是 SVN 或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。
- PE（Provider Edge）：服务提供商边缘设备，是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider）：服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。
- 用户设备所在的区域，称为一个站点（Site），站点是指相互之间具备 IP 连通性的一组 IP 系统，并且这组 IP 系统的 IP 连通性不需通过运营商网络实现。

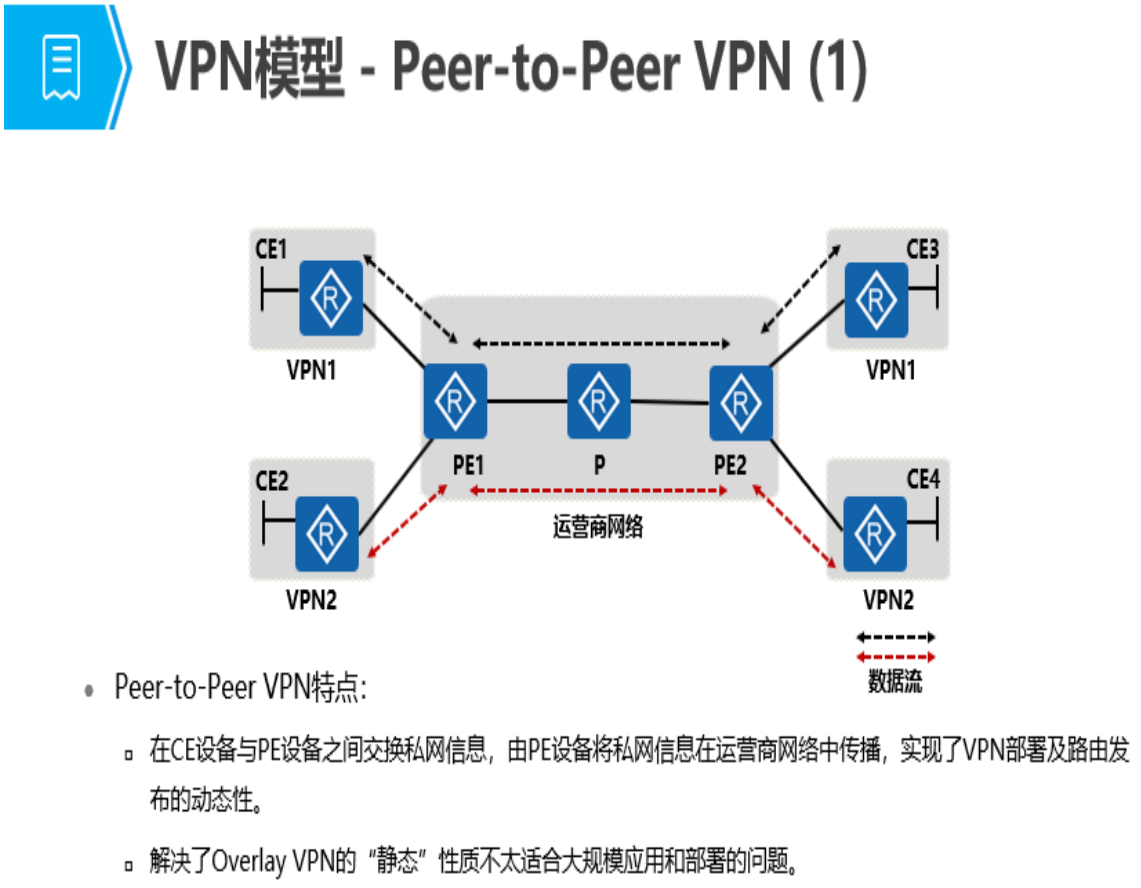
VPN模型 - Overlay VPN



- Overlay VPN的特点:
  - 客户路由协议总是在客户设备之间交换，而运营商对客户网络结构一无所知。
- 典型的协议：二层——帧中继；三层——GRE与IPSec；应用层——SSL VPN。

- Overlay VPN 可以在 CE 设备上建立隧道，也可以在 PE 设备上建立隧道：
- 在 CE 与 CE 之间建立隧道，并直接传递路由信息，路由协议数据总是在客户设备之间交换，运营商对客户网络结构一无所知。
- 优点：不同的客户地址空间可以重叠，保密性、安全性非常好；
- 缺点：本质是一种“静态”VPN，无法反应网络的实时变化。并且当有新增站点时，需要手工在所有站点上建立与新增站点的连接，配置与维护复杂，不易管理。
- 在 PE 上为每一个 VPN 用户建立相应的隧道，路由信息在 PE 与 PE 之间传递，公网中的 P 设备不知道私网的路由信息。

- 优点：客户把 VPN 的创建及维护完全交给运营商，保密性、安全性比较好；
- 缺点：不同的 VPN 用户不能共享相同的地址空间。

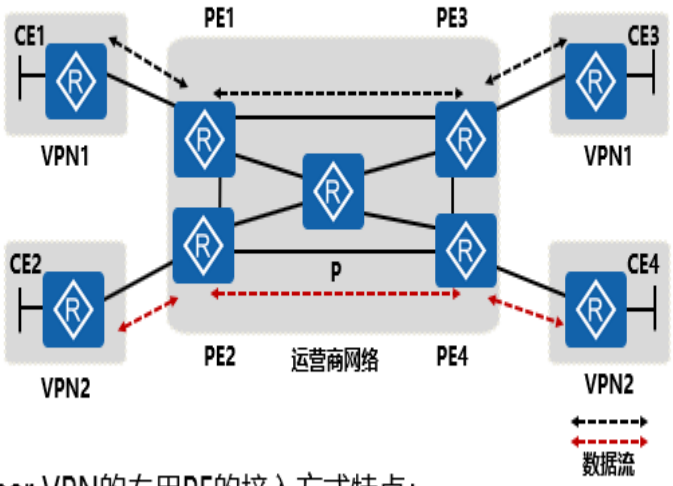


- 如图所示，所有 VPN 用户的 CE 设备都连到同一台 PE 上，PE 与不同的 CE 之间运行不同的路由协议（或者是相同路由协议的不同进程）。由始发 PE 将路由发布到公网上，在接收端的 PE 上将路由过滤后再发给相应的 CE 设备。
- Peer-to-Peer 是在 CE 与 PE 之间交换私网路由信息，然后由 PE 将私网路由在运营商网络中传播，由于 CE 与 PE 之间运行了路由协议，所以私网路由会自动地传播到 PE 上；由于 Peer-to-Peer VPN 将私网路由泄露到公网上，所以必须通过严格的路由过滤和选择机制来控制私网路由的传播。
- 缺点：
- 为了防止连接在同一台 PE 上的不同 CE 之间互通，必须

在 PE 上配置大量的 ACL，但这种操作也增加了管理 PE 设备的负担；

- VPN 客户之间如果出现地址重叠问题，PE 设备无法识别重叠的地址。
- 图中的 Peer-to-Peer VPN 使用的是共享 PE 的接入方式，为了减少配置复杂度，便于管理，可以采用 Peer-to-Peer VPN 的专用 PE 接入方式。

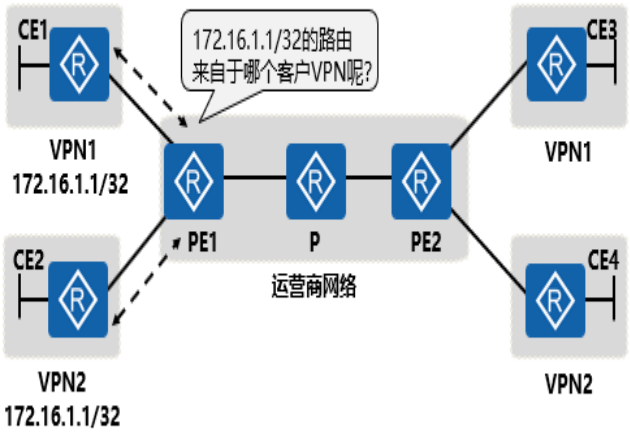
VPN模型 - Peer-to-Peer VPN (2)



- Peer-to-Peer VPN的专用PE的接入方式特点:
  - 运营商为每一个VPN单独准备一台PE设备，PE和CE之间可以运行任意的路由协议，与其他VPN无关。

- 专用 PE 接入方式的特点：
- 优点：无需配置任何的 ACL，配置复杂度、管理难度有所降低。
- 缺点：每新增一个 VPN 站点都需要新增一台专用的 PE 设备，代价过于昂贵。而且没有解决 VPN 客户之间地址空间重叠的问题。

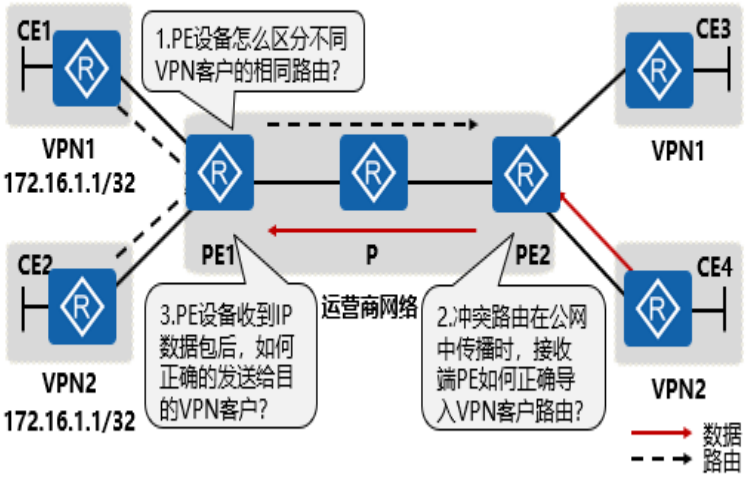
MPLS VPN产生的原因



- 两个客户的VPN存在相同的地址空间，传统VPN网络结构中的设备无法区分客户重叠的路由信息。

- 传统的 VPN 技术存在一些固有的缺陷，导致客户组网时的很多需求无法得到满足，并且实施比较复杂，MPLS VPN 的出现解决了传统 VPN 技术的固有缺陷——地址空间的重叠问题。

解决地址空间重叠问题的讨论



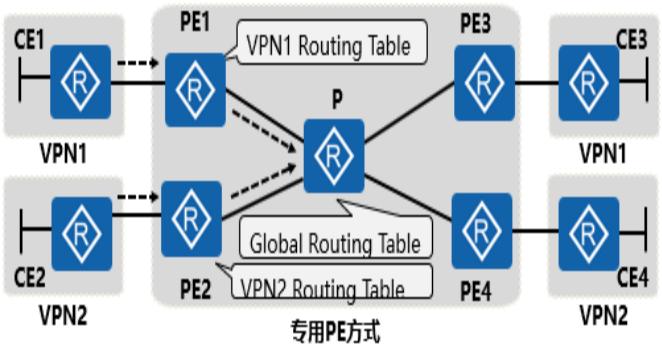
- 解决VPN客户地址空间重叠问题需要解决上述三个问题。

- 从上面的技术难点分析，主要问题都是与路由相关的特性，所以解决这些问题必须从路由协议考虑，但现在的路由协议都不具备解决这些问题的条件，因此考虑对路由协议进行改造。
- 由于 BGP 的诸多优点对技术难点的解决提供了思路：
- 公共网络上的 VPN 路由数量庞大，BGP 是唯一支持大量路由的协议；
- BGP 的报文基于 TLV 的结构，便于扩展；
- BGP 可以承载附加在路由后面的任何信息，并作为可选属性传递给其他邻居。
- 上面提到的 3 个技术难点迎刃而解：
- 本地路由冲突的问题：可以通过在同一台 PE 设备上为不同的 VPN 建立单独的路由，这样冲突的的路由就被隔离开来；
- 在路由传递过程中，为不同的 VPN 路由添加不同的标识，

以示区别。这些标识可以作为 BGP 属性进行传递；

- 由于 IP 报文不可更改，可以在 IP 报文头前加一些信息。由始发路由器打上标记，接收路由器在收到带标记的的数据包时，根据标记转发给正确的 VPN。
- 下面将针对上面的三个技术难点逐一进行解决方案的介绍。

本地路由冲突的解决方案 (1)



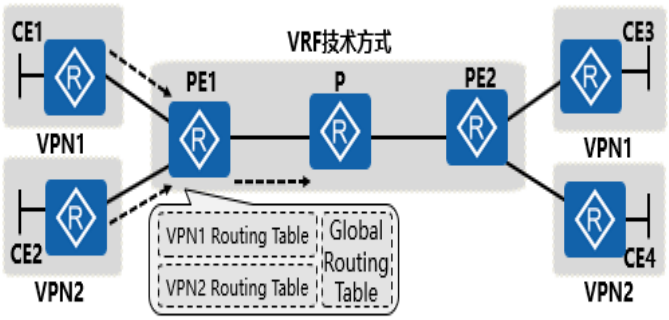
- 专用PE设备分工明确，每个PE设备只保存自己的VPN路由，P设备只保存公网路由。

  因此解决共享PE设备上地址空间重叠的思路是：

  - 将专用PE设备与P设备的功能在同一台PE设备上完成，并实现VPN路由的隔离。

- 其实传统 VPN 解决地址冲突的问题也存在一些方法：使用 ACL，NAT 等，但这些办法都没能从本质上解决问题。要想彻底解决问题，必须在理论上有所突破。可以从专用 PE 上得到启示，专用 PE 设备分工明确，每个 PE 只保存自己的 VPN 路由，P 设备只保存公网路由。而现在的思路是：将专用 PE 设备与 P 设备的功能在一台 PE 设备上完成。

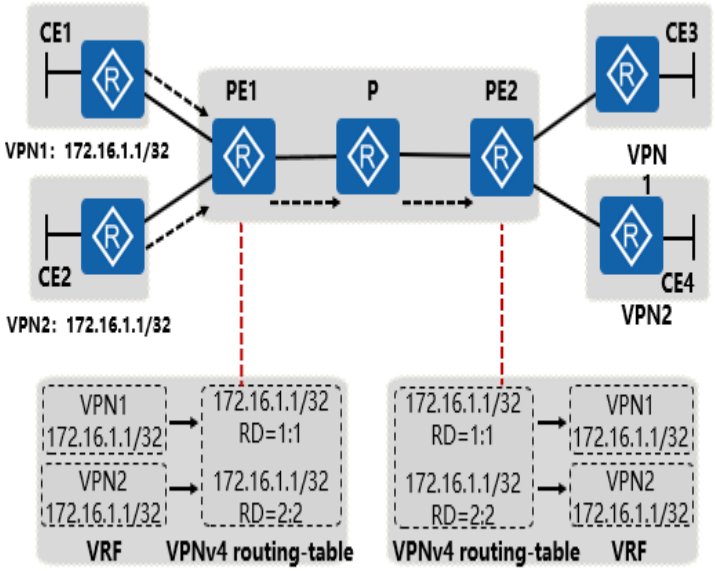
本地路由冲突的解决方案 (2)



- 在共享PE设备上使用VRF技术将重叠的路由隔离：每个VPN的路由放入自己对应的VPN Routing Table中。
- PE设备在维护多个VPN Routing Table时，同时还维护一个公网的路由表。

- 共享 PE 设备上实现重叠路由的隔离就是在 PE 设备上将来自每个 VPN 的路由放入自己对应的 VPN Routing Table 中，每个 VPN Routing Table 只记录对应 VPN 中学来的路由，就像是专用 PE 一样。这个 VPN Routing Table 称谓 VRF（VPN Routing and Forwarding table），即 VPN 路由转发表。
- 每一个 VRF 都需要对应一个 VPN instance，VPN 用户对应的接口绑定到 VPN instance 中。
- 对于每个 PE，可以维护一个或多个 VPN instance ，同时维护一个公网的路由表（也叫全局路由表），多个 VPN instance 实例相互独立且隔离。其实实现 VPN instance 并不困难，关键在于如何在 PE 上使用特定的策略规则来协调各 VPN instance 和全局路由表之间的关系。

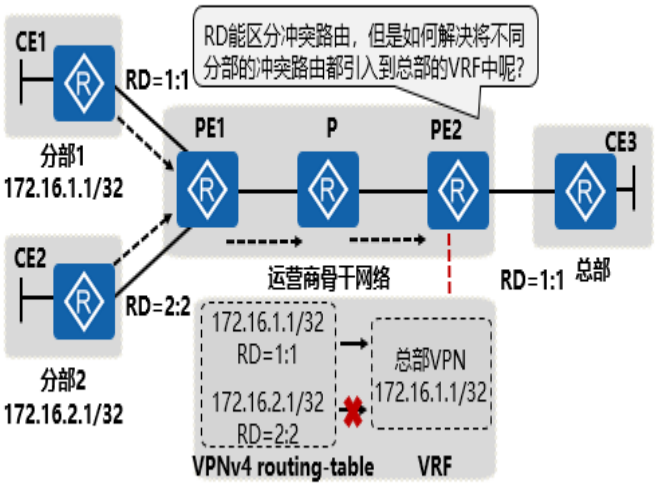
如何在网络传递过程中区分冲突路由



- 将VPN路由发布到全局路由表之前，使用一个全局唯一的标识和路由绑定，以区分冲突的私网路由。这个标识被称为RD（Route Distinguisher）。

- RD 即 VPN 路由标识符，由 8 字节组成，配置时同一 PE 设备上分配给每个 VPN 的 RD 必须唯一。
- RD 用于区分使用相同地址空间的 IPv4 前缀，增加了 RD 的 IPv4 地址称为 VPN-IPv4 地址（即 VPNv4 地址）。
- 运营商设备采用 BGP 协议作为承载 VPN 路由的协议，并将 BGP 协议进行了扩展，称为 MP-BGP（Multiprotocol Extensions for BGP-4）。PE 从 CE 接收到客户的 IPv4 私网路由后，将客户的私网路由添加各种标识信息后变为 VPNv4 路由放入 MP-BGP 的 VPNv4 路由表中，并通过 MP-BGP 协议在公网上传递。

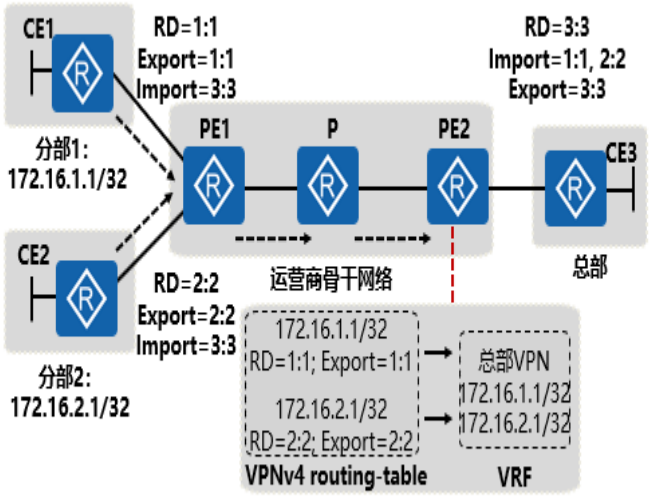
Hub-Spoke场景中VPN路由的引入问题



- RD不能解决VPN路由正确引入VPN的问题。
- 我们需要一种类似于Tag的标识。这个标识由人工分配，发送端PE发送时打上标识，接收端PE收到后，根据需要将带有相应标识的路由引入VPN。

- 如图所示，某公司分部 1 与分部 2 中存在 172.16.1.1/32 与 172.16.2.1/32 的私网地址，公司希望实现各分部只能与总部通信，分部之间不能相互通信。分配给分部 1 的 VPN RD 为 1:1，分配给分部 2 的 VPN RD 为 2:2。如果要使用 RD 解决路由引入 VPN 的问题，总部与分部 1 通信，则 RD 的值需要配置成 1:1，总部与分部 2 通信，则 RD 的值需要配置成为 2:2。但 RD 的值在本地 PE 上是唯一的，并且只能配置一个。因此，不能使用 RD 来解决路由正确引入的问题。

Hub-Spoke场景中路由引入问题的解决

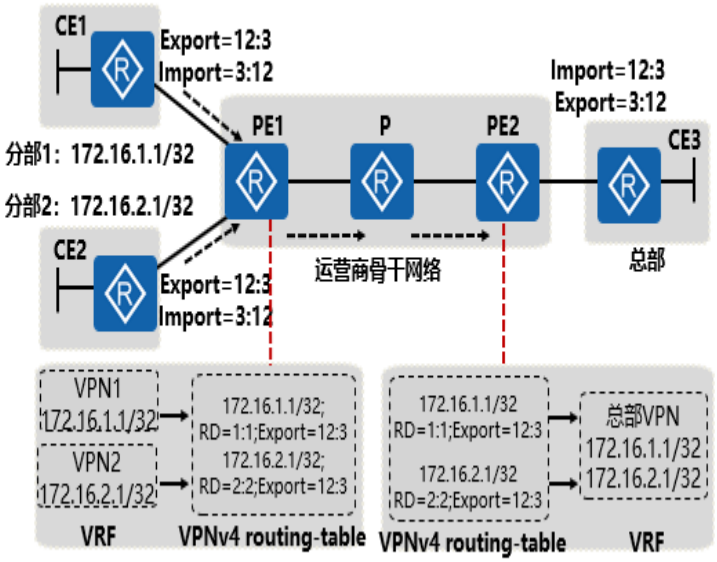


- RT属性用于将路由正确引入VPN，有两类VPN Target属性，Import Target和Export Target，分别用于VPN路由的导出与导入。

- 如图所示，希望实现分部只能与总部通信，分部之间不能通信。分配给分部 1 的 Export Target 为 1:1，Import Target 为 3:3；分配给分部 2 的 Export Target 为 2:2，Import Target 为 3:3；分配给总部的 Export Target 为 3:3，Import Target 为 1:1，2:2；PE2 上收到对端 PE1 发送的 VPNv4 的路由后，检查其 Export Target。因为总部的 Import Target 为 1:1，2:2，所以值为 1:1 或 2:2 的路由被引入总部的 VRF。PE1 的 VPNv4 的路由引入各分部 VRF 的过程类似。
- RT（Route Target）封装在 BGP 的扩展 Community 属性中，在路由传递过程中作为可选可传递属性进行传递。
- RT 的本质是每个 VRF 表达自己的路由取舍及喜好的属性，有两类 VPN Target 属性：
- Export Target：本端的路由在导出 VRF，转变为 VPNv4 的路由时，标记该属性；

- Import Target：对端收到路由时，检查其 Export Target 属性。当此属性与 PE 上某个 VPN 实例的 Import Target 匹配时，PE 就把路由加入到该 VPN 实例中。

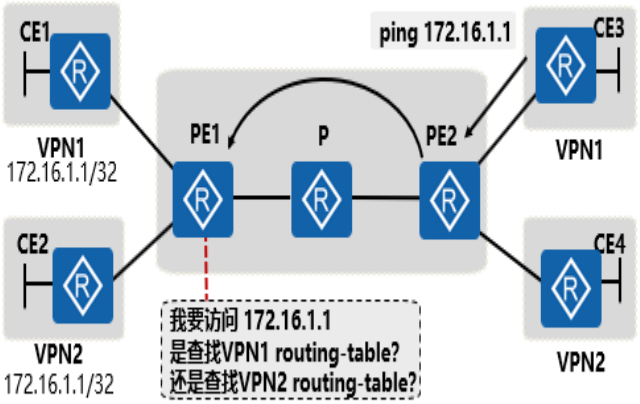
Hub-Spoke场景中路由引入问题的优化



- 使用RT实现本端与对端的路由正确引入VPN，原则如下：
  - 本端的Export Target=对端的Import Target，本端的Import Target=对端的Export Target。

- 如图，分配给所有分部的 Import Target 为 3:12，Export Target 为 12:3；而分配给总部的值正好相反，实现所有分部只与总部通信的需求。

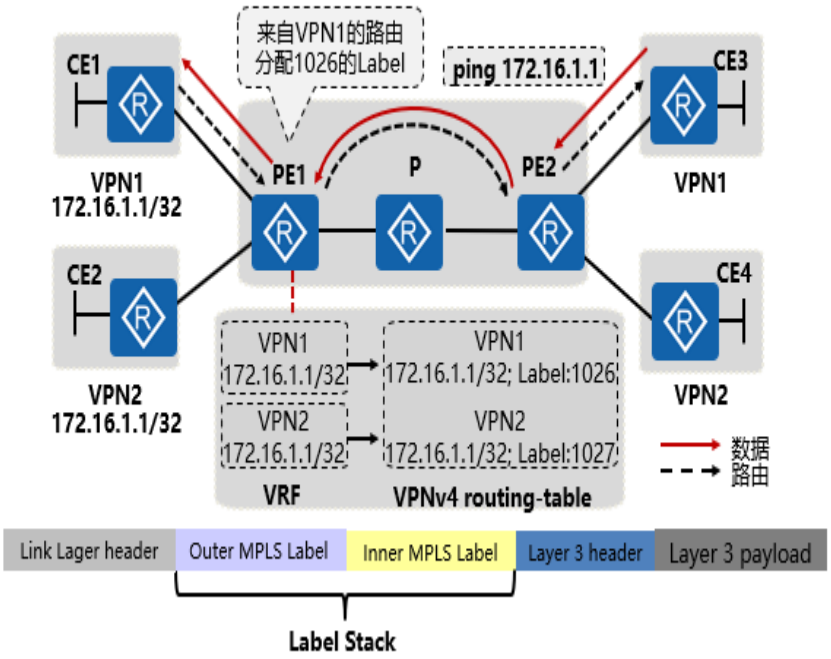
解决数据转发过程中冲突路由的查找



- 因为数据包没有携带任何标识，所以在ICMP的数据包到达PE1时，PE1并不知道该查找哪个VPN的路由表找到正确的目标地址。

- 解决该问题的方案有两种：
- 在数据包中增加标识信息，并且使用 RD 作为区分数据包所属 VPN 的标识符，数据转发时也携带 RD 信息。缺点是由于 RD 由 8 字节组成，额外增大数据包，会导致转发效率降低。
- 借助公网中已经实施的 MPLS 协议建立的标签隧道，采用标签作为数据包正确转发的标识，MPLS 标签支持嵌套，可以将区分数据包所属 VPN 的标签封装在公网标签内。

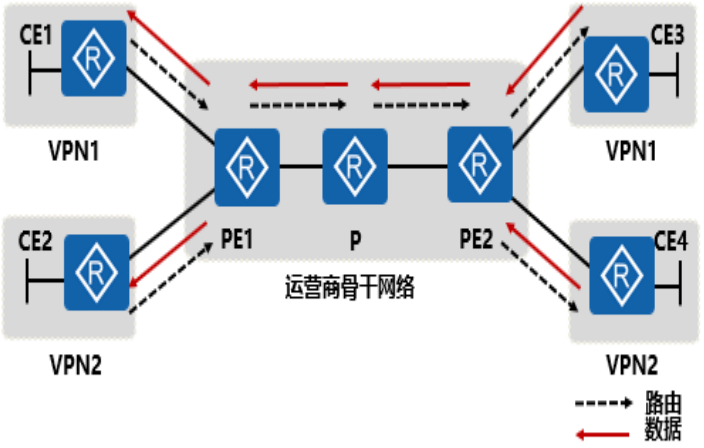
MPLS标签嵌套的应用



- 使用标签嵌套解决数据转发过程中冲突路由的查找问题。

- Outer MPLS Label 在 MPLS VPN 中被称为公网标签，用于 MPLS 网络中转发数据。一般公网标签会在到达 PE 设备时已被倒数第二跳剥掉，漏出 Inner Label。Inner MPLS Label 在 MPLS VPN 中被称为私网标签，用于将数据正确发送到相应的 VPN 中，PE 依靠 Inner Label 区分数据包属于哪个 VPN。

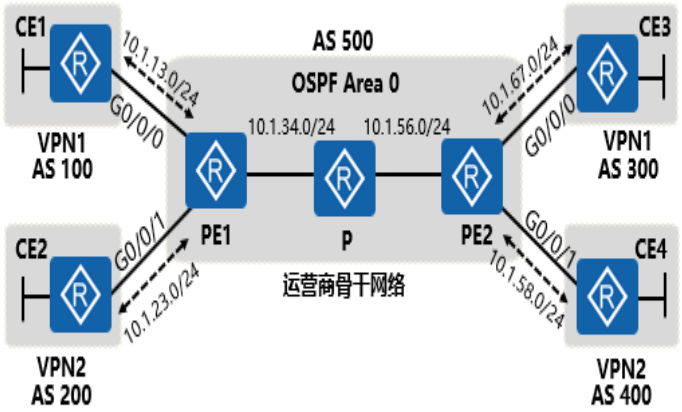
MPLS VPN的工作过程



- MPLS VPN的工作过程分为两部分:
  - MPLS VPN路由的传递过程;
  - MPLS VPN数据的转发过程。

- MPLS VPN 路由的传递过程将分为四个阶段介绍：
- CE 与 PE 之间的路由交换；
- VRF 路由注入 MP-BGP 的过程；
- 公网标签的分配过程；
- MP-BGP 路由注入 VRF 的过程。

CE与PE之间的路由交换

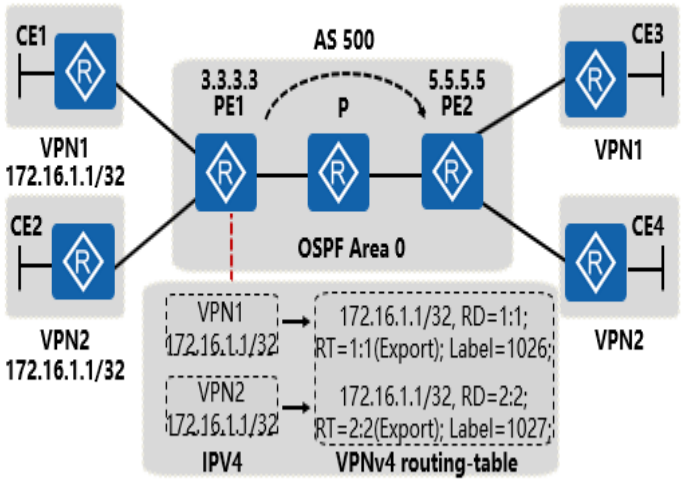


- PE与CE之间可以通过静态路由协议交换路由信息，也可以通过动态路由协议（如：RIP，OSPF，ISIS，BGP等）交换路由信息。

- 如图所示，以 CE1 与 PE1 之间采用 BGP 协议为例展示配置，其中，VPN1 被分配实例名称为 VPN1，RD 为 1:1，RT 为 1:1。配置命令如下：
- CE1 上的配置：
- bgp 100
- peer 10.1.13.3 as-number 500
- #
- ipv4-family unicast
- peer 10.1.13.3 enable
- PE1 上的配置：
- ip vpn-instance VPN1
- ipv4-family
- route-distinguisher 1:1
- vpn-target 1:1 export-extcommunity

- vpn-target 1:1 import-extcommunity
- #

VPN路由注入MP-BGP的过程

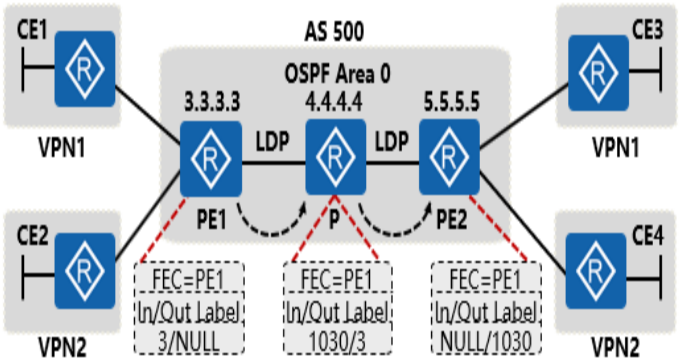


- VRF中的IPv4路由被添加上RD，RT与标签等信息成为VPN-IPv4的路由放入到MP-BGP的路由表中，并通过MP-BGP协议在PE设备之间交换路由信息。

- 两端 PE 运行 MP-BGP，通过公网将路由传递给对端，以 PE1 为例配置如下：
- bgp 500
- peer 5.5.5.5 as-number 500
- peer 5.5.5.5 connect-interface LoopBack0
- #
- ipv4-family unicast
- undo synchronization
- peer 5.5.5.5 enable
- #
- ipv4-family vpnv4
- policy vpn-target

- peer 5.5.5.5 enable

公网标签的分配过程

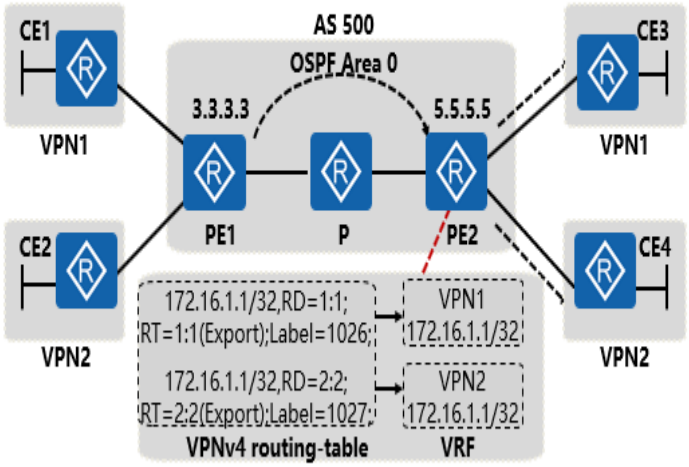


- MPLS协议在运营商网络分配公网标签，建立标签隧道，实现私网数据在公网上的转发。
- PE之间运行的MP-BGP协议为VPN路由分配私网标签，PE设备根据私网标签将数据正确转发给相应的VPN。

- 运营商的骨干网络中的 PE 设备与 P 设备，需要运行 IGP 协议使运营商网络中的路由可达。图中以 OSPF 为例，配置略。
- PE 设备与 P 设备需要运行 LDP 协议，动态分配标签，以建立标签隧道。以 P 设备上的配置为例：
- mpls lsr-id 4.4.4.4
- mpls
- mpls ldp
- interface GigabitEthernet0/0/0
- ip address 10.1.34.4 255.255.255.0
- mpls
- mpls ldp
- #

- interface GigabitEthernet0/0/1
- ip address 10.1.45.4 255.255.255.0
- mpls
- mpls ldp

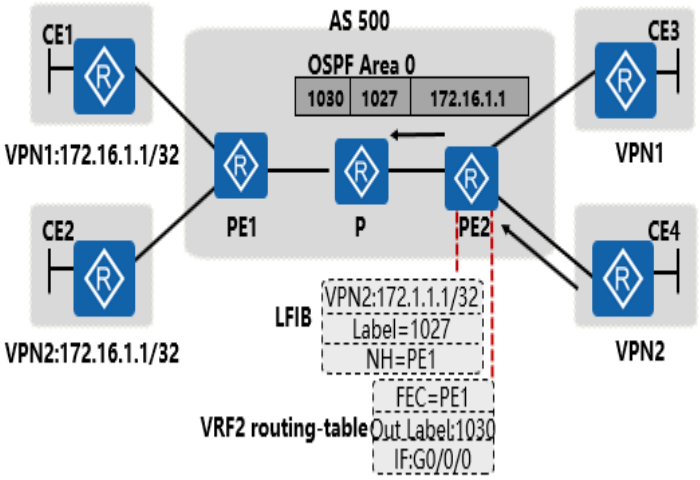
MP-BGP路由注入VPN的过程



- PE2在接收到PE1发送的VPNv4路由后将检查路由的扩展团体属性，将携带的Export Target值与本端VPN的Import Target值比较，数值相同则将路由引入VPN的路由表，实现路由的正确导入。

- 经过上述 4 个步骤，MPLS VPN 网络的路由交换过程完成。当然，我们是以单向的路由交换过程为例进行的介绍，其实路由交换的过程是双向的，但过程都是类似的。
- 下一节将介绍 MPLS VPN 的数据转发过程，并分为三个步骤进行介绍：
- CE 设备到 PE 设备的数据转发；
- 公网设备上的数据转发；
- PE 设备到 CE 设备的数据转发。

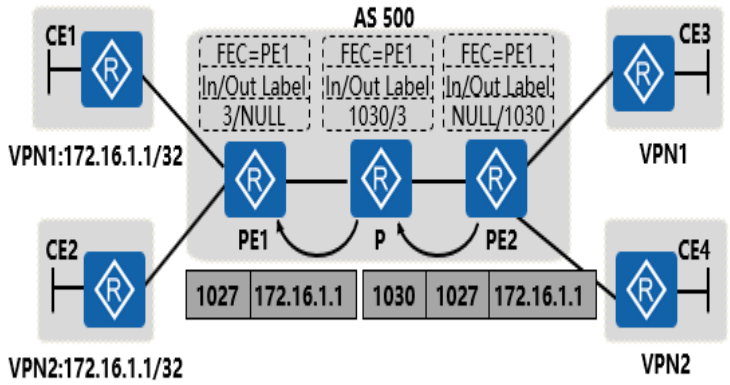
CE设备到PE设备的数据转发



- 数据从CE4转发给PE2，在PE2设备上需要查找VPN2的路由表，确定数据进行标签转发后，再查找下一跳与出接口，根据分配的标签进行MPLS的封装。

- 数据从 CE 设备到 PE 设备的转发：
- 如图所示，CE4 所连接的 VPN2 的用户要与对端 VPN2 中的 172.16.1.1/32 用户通信，PE2 收到数据包后，查找本地 VPN2 的路由表，发现数据包需要进行标签转发，分配的私网标签为 1027，到达目标地址的下一跳为 PE1。
- PE2 通过查找 LFIB 表，发现到达 PE1 被分配的公网标签为 1030，出接口为 G0/0/0，PE2 将数据包进行 MPLS 封装，内层为 1027，外层为 1030，从接口 G0/0/0 转发出去。

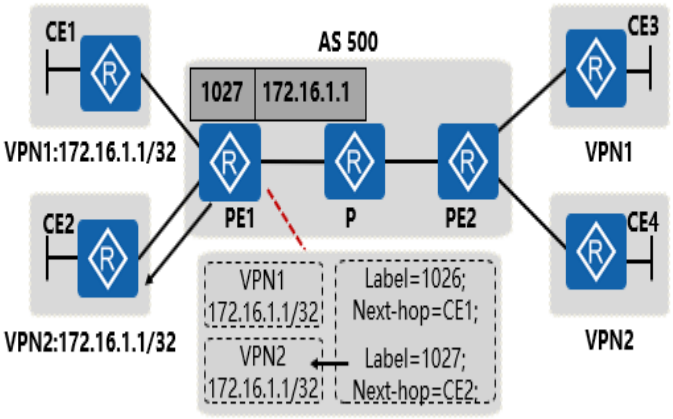
公网设备上的数据转发



- 数据包在公网上转发时，通过MPLS协议已建立好的标签隧道将数据报文转发到PE1。转发过程中，只改变公网标签。

- 数据包在公网上的传递过程：
- 如图所示，PE2 收到 VPN 用户的数据包后，封装上 MPLS 的标签，将私网数据通过 MPLS 建立的标签隧道进行转发，PE2 上数据包封装的公网标签为 1030，转发给 P 设备后，查找 LFIB 表，进标签为 1030 的数据包，对应的出标签为 3，即将公网标签标签剥离后，将数据包发送给 PE1，PE1 收到的是只有内层私网标签的数据包。

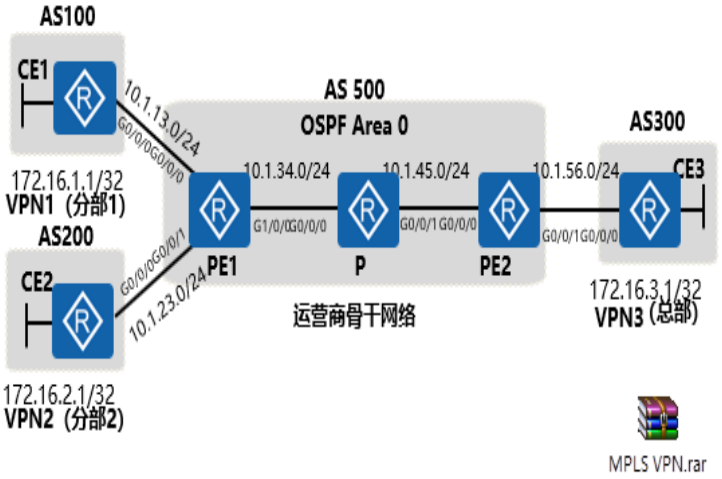
PE设备到CE设备的数据转发



- PE1收到剥离公网标签的数据包后，根据私网标签查找转发数据包的下一跳，将数据包正确发送给相应VPN客户。

- 数据包转发给相应 VPN 的过程：
- 如图所示，PE1 收到只有一层标签的数据包，查找标签表，发现标签为 1027 的数据包对应的下一跳为 CE2，于是 PE2 将数据包剥离私网标签，进行 IP 封装，查找出接口，将数据包发送给 CE2 处理。
- 至此，数据包到达正确的目标用户，我们是以单向的数据转发过程为例进行的介绍，其实数据转发的过程是双向的，但过程都是类似的。

MPLS VPN配置实例

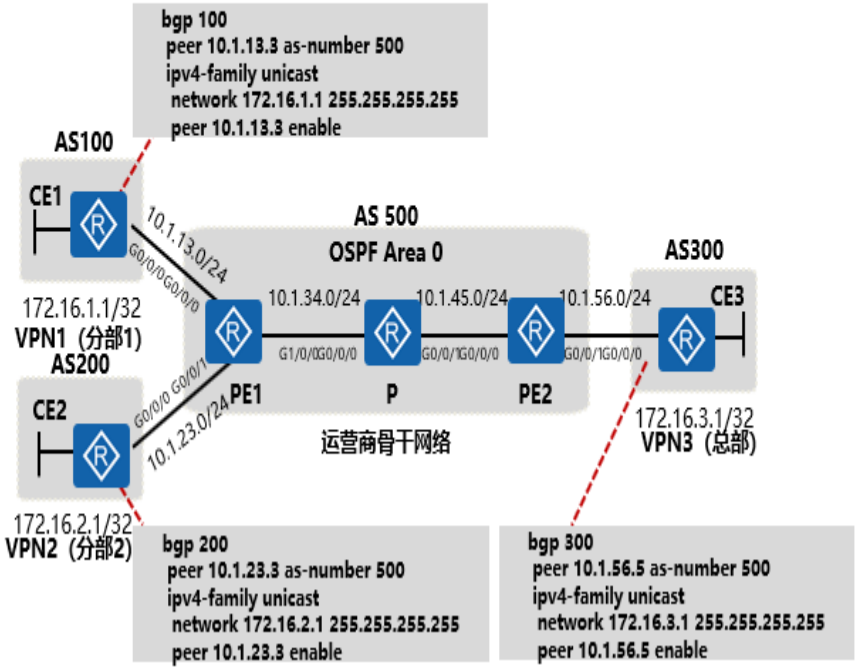


- 分部1与分部2只能与总部通信，分部之间不能通信。根据图上信息进行正确配置，使总部的用户能正确访问各分部的用户。

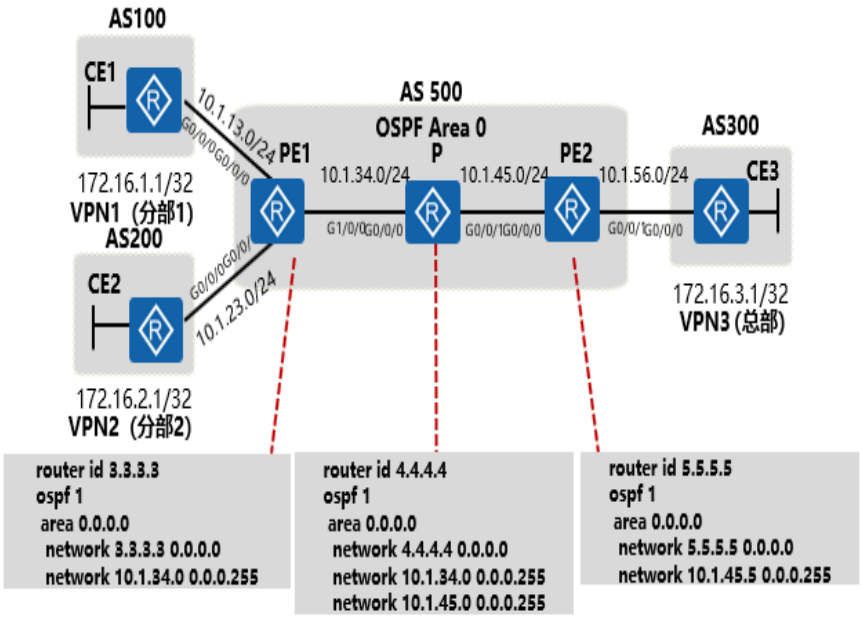
- 配置需求：
- 分部与总部之间采用 MPLS VPN 进行通信，用户与运营商之间使用 BGP 协议传递路由。分部 1 被划分到 VPN1 中，使用的 RD 为 1:1，Export Target=12:3，Import Target=3:12；分部 2 被划分到 VPN2 中，使用的 RD 为 2:2，Export Target =12:3，Import Target=3:12；总部被划分到 VPN3 中，使用的 RD 为 3:3，Export Target=3:12，Import Target=12:3。
- 如图所示，配置 MPLS VPN 需要从以下两个方面考虑：
- 用户侧设备的配置：
- 主要考虑 CE 与 PE 之间使用何种协议将私网路由传递到运营商网络；
- 运营商骨干网络的配置，运营商骨干网络的配置需要从以下三个方面考虑：
- 运营商骨干网络 IGP 协议的配置，保证运营商网络路由

可达；

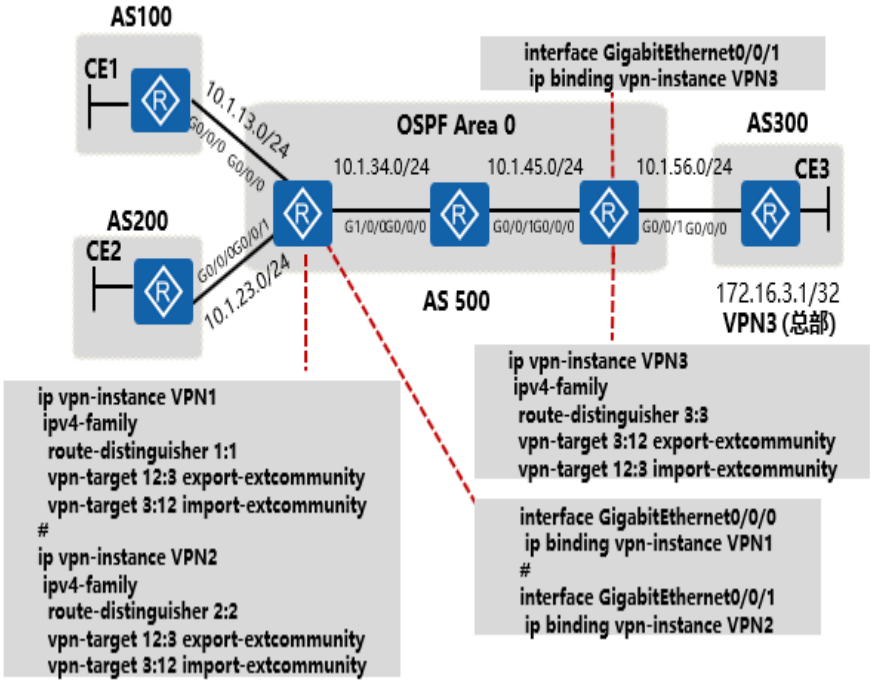
- VPN 的配置，将私网路由通过运营商设备封装并传递；
- MP-BGP 与 MPLS 协议的配置，实现私网路由的传递与标签隧道的建立。



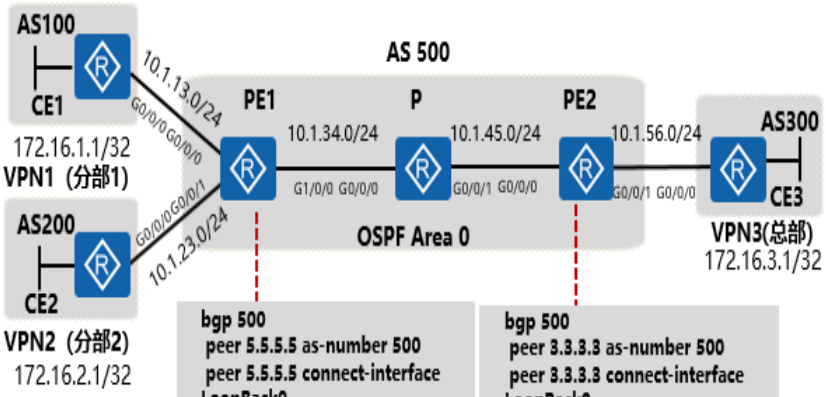
MPLS VPN配置实例 - 骨干网IGP配置



MPLS VPN配置实例 - VPN实例配置



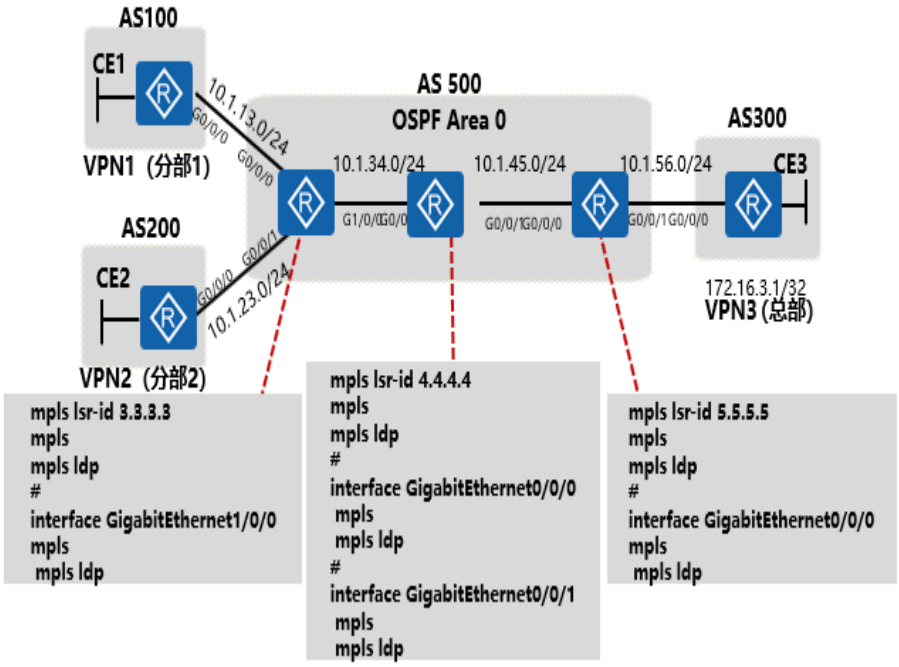
MPLS VPN配置实例 - MP-BGP配置




```
bgp 500
 peer 5.5.5.5 as-number 500
 peer 5.5.5.5 connect-interface
LoopBack0
#
 ipv4-family vpnv4
  peer 5.5.5.5 enable
#
 ipv4-family vpn-instance VPN1
  peer 10.1.13.1 as-number 100
#
 ipv4-family vpn-instance VPN2
  peer 10.1.23.2 as-number 200
```

```
bgp 500
 peer 3.3.3.3 as-number 500
 peer 3.3.3.3 connect-interface
LoopBack0
#
 ipv4-family vpnv4
  policy vpn-target
  peer 3.3.3.3 enable
#
 ipv4-family vpn-instance VPN3
  peer 10.1.56.6 as-number 300
```

MPLS VPN配置实例 - MPLS配置



思考题

1. 下列选项中，属于Overlay VPN模型的技术有哪些？（ ）

   A. IPSec VPN

   B. SSL VPN

   C. Peer-to-Peer VPN

   D. GRE

2. 下列哪个选项能够解决MPLS VPN的路由正确引入相应VRF的问题？（ ）

   A. RT

   B. RD

   C. VRF

   D. MP-BGP

答案：ABD。
答案：A。