



# (12) 发明专利申请

(10) 申请公布号 CN 102377630 A

(43) 申请公布日 2012. 03. 14

(21) 申请号 201110310193. 7

(22) 申请日 2011. 10. 13

(71) 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为  
基地总部办公楼

(72) 发明人 李振斌 余璟明 屈丹

(51) Int. Cl.

H04L 12/46 (2006. 01)

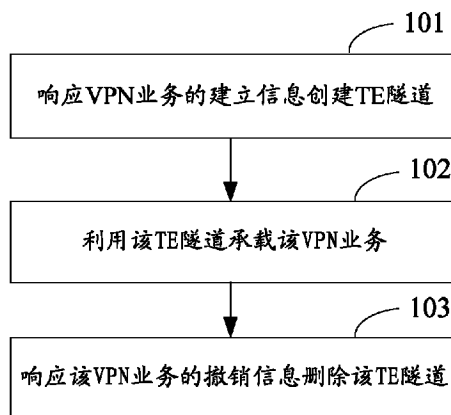
权利要求书 3 页 说明书 8 页 附图 5 页

## (54) 发明名称

基于流量工程隧道的虚拟专用网络实现方法及系统

## (57) 摘要

本发明实施例提供了一种基于流量工程隧道的虚拟专用网络实现方法及系统。该基于流量工程隧道的虚拟专用网络实现方法包括：响应虚拟专用网络业务的建立信息创建流量工程隧道；利用该流量工程隧道承载该虚拟专用网络业务；响应该虚拟专用网络业务的撤销信息删除该流量工程隧道。通过上述方式，根据虚拟专用网络业务的需要动态创建或删除流量工程隧道，提供了一种流量工程隧道按需创建的机制，并及时删除不被虚拟专用网络业务使用的隧道，有效地节省了网络资源。



1. 一种基于流量工程隧道的虚拟专用网络实现方法,其特征在于,所述虚拟专用网络实现方法包括:

响应虚拟专用网络业务的建立信息创建流量工程隧道;  
利用所述流量工程隧道承载所述虚拟专用网络业务;以及  
响应所述虚拟专用网络业务的撤销信息删除所述流量工程隧道。

2. 根据权利要求1所述的虚拟专用网络实现方法,其特征在于,所述响应虚拟专用网络业务的建立信息创建流量工程隧道的步骤包括:

利用隧道策略设定与所述虚拟专用网络业务关联的隧道模板,以利用所述隧道模板控制所述流量工程隧道的公共属性。

3. 根据权利要求2所述的虚拟专用网络实现方法,其特征在于,所述利用隧道策略设定与所述虚拟专用网络业务关联的隧道模板的步骤包括:

根据所述虚拟专用网络业务的业务要求为所述虚拟专用网络业务设定所述隧道模板,以利用所述隧道模板将所述流量工程隧道限定在对应的转发平面上。

4. 根据权利要求1-3任意一项所述的虚拟专用网络实现方法,其特征在于,所述虚拟专用网络业务是多协议标签交换三层虚拟专用网络业务,所述响应虚拟专用网络业务的建立信息创建流量工程隧道的步骤包括:

在学习到通过边界网关协议传递的虚拟专用网络路由信息后触发所述流量工程隧道的自动创建。

5. 根据权利要求1-3任意一项所述的虚拟专用网络实现方法,其特征在于,所述响应虚拟专用网络业务的建立信息创建流量工程隧道的步骤包括:

在相互连接的至少两个自治系统中的各自治系统的服务商边缘设备与自治系统边界路由器之间分段建立所述流量工程隧道。

6. 根据权利要求5所述的虚拟专用网络实现方法,其特征在于,所述在相互连接的至少两个自治系统中的各自治系统的服务商边缘设备与自治系统边界路由器之间分段建立所述流量工程隧道的步骤包括:

在所述服务商边缘设备和所述自治系统边界路由器上配置虚拟路由转发实例,且在所述服务商边缘设备和所述自治系统边界路由器上为虚拟专用网络路由信息设定相应的隧道模板,并利用所述隧道模板在各自治系统的所述服务商边缘设备与所述自治系统边界路由器之间分段建立所述流量工程隧道。

7. 根据权利要求5所述的虚拟专用网络实现方法,其特征在于,所述在相互连接的至少两个自治系统中的各自治系统的服务商边缘设备与自治系统边界路由器之间分段建立所述流量工程隧道的步骤包括:

在所述服务商边缘设备上配置虚拟路由转发实例,且在所述自治系统边界路由器上利用边界网关协议路由策略为边界网关协议对端设定隧道模板,并利用所述隧道模板在各自治系统的所述服务商边缘设备与所述自治系统边界路由器之间分段建立所述流量工程隧道。

8. 根据权利要求5所述的虚拟专用网络实现方法,其特征在于,所述在相互连接的至少两个自治系统中的各自治系统的服务商边缘设备与自治系统边界路由器之间分段建立所述流量工程隧道的步骤包括:

在所述服务商边缘设备和所述自治系统边界路由器上利用边界网关协议路由策略为边界网关协议对端设定隧道模板,并学习到带公网标签的边界网关协议路由信息后,利用所述隧道模板在各自治系统的所述服务商边缘设备与所述自治系统边界路由器之间分段建立所述流量工程隧道。

9. 根据权利要求 1-3 任意一项所述的虚拟专用网络实现方法,其特征在于,所述虚拟专用网络业务是多协议标签交换二层虚拟专用网络业务,所述响应虚拟专用网络业务的建立信息创建流量工程隧道的步骤包括:

通过静态或动态的二层虚拟专用网络虚电路信息来触发所述流量工程隧道的自动创建。

10. 根据权利要求 9 所述的虚拟专用网络实现方法,其特征在于,所述通过静态或动态的二层虚拟专用网络虚电路信息来触发所述流量工程隧道的自动创建的步骤包括:

在配置所述二层虚拟专用网络虚电路信息时设定隧道模板,并在配置所述二层虚拟专用网络虚电路信息的同时或者学习到通过标签分发协议或边界网关协议传递的所述二层虚拟专用网络虚电路信息时触发基于所述隧道模板的所述流量工程隧道的自动创建。

11. 根据权利要求 9 所述的虚拟专用网络实现方法,其特征在于,所述通过静态或动态的二层虚拟专用网络虚电路信息来触发所述流量工程隧道的自动创建的步骤包括:

在配置虚拟交换接口对等体或虚拟交换接口实例时设定隧道模板,并在学习到通过标签分发协议或边界网关协议传递的所述二层虚拟专用网络虚电路信息时触发基于所述隧道模板的所述流量工程隧道的自动创建。

12. 根据权利要求 9 所述的虚拟专用网络实现方法,其特征在于,所述通过静态或动态的二层虚拟专用网络虚电路信息来触发所述流量工程隧道的自动创建的步骤包括:

在配置交换伪线时设定隧道模板,并在学习到通过标签分发协议传递的所述二层虚拟专用网络虚电路信息时触发基于所述隧道模板的所述流量工程隧道的自动创建。

13. 一种基于流量工程隧道的虚拟专用网络实现系统,其特征在于,所述虚拟专用网络实现系统包括:

隧道建立模块,响应虚拟专用网络业务的建立信息创建流量工程隧道;

隧道维护模块,利用所述流量工程隧道承载所述虚拟专用网络业务;以及

隧道删除模块,响应所述虚拟专用网络业务的撤销信息删除所述流量工程隧道。

14. 根据权利要求 13 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块利用隧道策略设定与所述虚拟专用网络业务关联的隧道模板,以利用所述隧道模板控制所述流量工程隧道的公共属性。

15. 根据权利要求 14 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块根据所述虚拟专用网络业务的业务要求为所述虚拟专用网络业务设定所述隧道模板,以利用所述隧道模板将所述流量工程隧道限定在对应的转发平面上。

16. 根据权利要求 13-15 任意一项所述的虚拟专用网络实现系统,其特征在于,所述虚拟专用网络业务是多协议标签交换三层虚拟专用网络业务,所述隧道建立模块在学习到通过边界网关协议传递的虚拟专用网络路由信息后触发所述流量工程隧道的自动创建。

17. 根据权利要求 13-15 任意一项所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在相互连接的至少两个自治系统中的各自治系统的服务商边缘设备与自治系

统边界路由器之间分段建立所述流量工程隧道。

18. 根据权利要求 17 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在所述服务商边缘设备和所述自治系统边界路由器上配置虚拟路由转发实例,且在所述服务商边缘设备和所述自治系统边界路由器上为虚拟专用网络路由信息设定相应的隧道模板,并利用所述隧道模板在各自治系统的所述服务商边缘设备与所述自治系统边界路由器之间分段建立所述流量工程隧道。

19. 根据权利要求 17 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在所述服务商边缘设备上配置虚拟路由转发实例,且在所述自治系统边界路由器上利用边界网关协议路由策略为边界网关协议对端设定隧道模板,并利用所述隧道模板在各自治系统的所述服务商边缘设备与所述自治系统边界路由器之间分段建立所述流量工程隧道。

20. 根据权利要求 17 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在所述服务商边缘设备和所述自治系统边界路由器上利用边界网关协议路由策略为边界网关协议对端设定隧道模板,并学习到带公网标签的边界网关协议路由信息后,利用所述隧道模板在各自治系统的所述服务商边缘设备与所述自治系统边界路由器之间分段建立所述流量工程隧道。

21. 根据权利要求 13-15 任意一项所述的虚拟专用网络实现系统,其特征在于,所述虚拟专用网络业务是多协议标签交换二层虚拟专用网络业务,所述隧道建立模块通过静态或动态的二层虚拟专用网络虚电路信息来触发所述流量工程隧道的自动创建。

22. 根据权利要求 21 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在配置所述二层虚拟专用网络虚电路信息时设定隧道模板,并在配置所述二层虚拟专用网络虚电路信息的同时或者学习到通过标签分发协议或边界网关协议传递的所述二层虚拟专用网络虚电路信息时触发基于所述隧道模板的所述流量工程隧道的自动创建。

23. 根据权利要求 21 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在配置虚拟交换接口对等体或虚拟交换接口实例时设定隧道模板,并在学习到通过标签分发协议或边界网关协议传递的所述二层虚拟专用网络虚电路信息时触发基于所述隧道模板的所述流量工程隧道的自动创建。

24. 根据权利要求 21 所述的虚拟专用网络实现系统,其特征在于,所述隧道建立模块在配置交换伪线时设定隧道模板,并在学习到通过标签分发协议传递的所述二层虚拟专用网络虚电路信息时触发基于所述隧道模板的所述流量工程隧道的自动创建。

## 基于流量工程隧道的虚拟专用网络实现方法及系统

### 技术领域

[0001] 本发明涉及虚拟专用网络技术领域,特别是涉及一种基于流量工程隧道的虚拟专用网络实现方法及系统。

### 背景技术

[0002] 随着网络的日益普及,公司各分支机构之间为了共享商业数据,需要将各分支机构联网,以在保证数据存储和传输安全的前提下共享数据。为了达到此目的,各分支机构之间除了租用专线来实现互联外,还可以直接通过公共网络建立虚拟专用网络(Virtual Private Network, VPN)。VPN利用公共网络,通过隧道技术等手段将公共网络虚拟成专用网络,从而实现类似于私用专网的安全数据传输。

[0003] VPN业务可使用流量工程(Traffic Engineering, TE)隧道承载,其优势是可以保证带宽和服务品质(Quality of Service, QoS)服务,同时提供丰富多彩的高可靠性保护特性。

[0004] 目前,在现有的VPN实现方案中,TE隧道往往通过配置预先建立,并通过隧道策略(Tunnel Policy)为VPN业务选择满足要求的一条或多条TE隧道,从而完成VPN业务到TE隧道的映射。在这种方案中,TE隧道的建立与VPN业务是分离的,存在建立的TE隧道没有被VPN业务使用的情况,因此造成网络资源的浪费。

[0005] 综上,需要提供一种基于TE隧道的VPN实现方法及系统,以解决现有VPN实现方案中的TE隧道的建立与VPN业务相互分离所导致的网络资源浪费问题。

### 发明内容

[0006] 本发明主要解决的技术问题是提供一种基于TE隧道的VPN实现方法及系统,以有效地节省网络资源。

[0007] 为解决上述技术问题,本发明一方面采用的一个技术方案是:提供一种基于TE隧道的VPN实现方法,包括:响应VPN业务的建立信息创建TE隧道;利用该TE隧道承载该VPN业务;响应该VPN业务的撤销信息删除该TE隧道。

[0008] 为解决上述技术问题,本发明一方面采用的另一个技术方案是:提供一种基于TE隧道的VPN实现系统,包括:隧道建立模块,响应VPN业务的建立信息创建TE隧道;隧道维护模块,利用该TE隧道承载该VPN业务;隧道删除模块,响应该VPN业务的撤销信息删除该TE隧道。

[0009] 本发明一方面的有益效果是:区别于现有技术的情况,本发明实施例的基于TE隧道的VPN实现方法及系统根据VPN业务的需要动态创建或删除TE隧道,提供了一种TE隧道按需创建的机制,并及时删除不被VPN业务使用的隧道,有效地节省了网络资源。

### 附图说明

[0010] 图1是根据本发明实施例的基于TE隧道的VPN实现方法的流程图;

[0011] 图 2 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第一应用场景的网络结构示意图；

[0012] 图 3 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第二应用场景的网络结构示意图；

[0013] 图 4 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第三应用场景的网络结构示意图；

[0014] 图 5 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第四应用场景的网络结构示意图；

[0015] 图 6 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第五应用场景的网络结构示意图；

[0016] 图 7 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第六应用场景的网络结构示意图；

[0017] 图 8 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第七应用场景的网络结构示意图；

[0018] 图 9 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第八应用场景的网络结构示意图；

[0019] 图 10 是根据本发明实施例的基于 TE 隧道的 VPN 实现系统的示意框图。

## 具体实施方式

[0020] 请参见图 1, 图 1 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的流程图。如图 1 所示, 本实施例的基于 TE 隧道的 VPN 实现方法主要包括以下步骤：

[0021] 步骤 101 : 响应 VPN 业务的建立信息创建 TE 隧道；

[0022] 步骤 102 : 利用该 TE 隧道承载该 VPN 业务；以及

[0023] 步骤 103 : 响应该 VPN 业务的撤销信息删除该 TE 隧道。

[0024] 通过上述方式, 本实施例的基于 TE 隧道的 VPN 实现方法根据 VPN 业务的需要动态创建或删除 TE 隧道, 提供了一种 TE 隧道按需创建的机制, 并及时删除不被 VPN 业务使用的隧道, 有效地节省了网络资源。

[0025] 请参见图 2, 图 2 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第一应用场景的网络结构示意图。如图 2 所示, 在本实施例中, 本发明实施例的基于 TE 隧道的 VPN 实现方法应用于单个自治系统 (Autonomous System, AS) 内部的多协议标签交换 (Multi-Protocol Label Switching, MPLS) 三层虚拟专用网络 (L3VPN) 场景, 即本实施例的 VPN 业务为 MPLS L3VPN 业务。

[0026] 在图 2 所示的场景中, 主要存在三种设备 : 用户边缘 (Customer Edge, CE) 设备、服务商边缘 (Provider Edge, PE) 设备以及服务商骨干 (Provider, P) 设备。其中, CE 设备是用户驻地网络的一个组成部分, 例如路由器、交换机或主机, 其感知不到 VPN 的存在, 也不需要维护 VPN 的整个路由信息。PE 设备是服务商网络的边缘设备, 其与 CE 设备直接连接, 且在 MPLS 网络中, 完成对 VPN 的所有处理。P 设备处于服务商网络中, 其不与 CE 设备直接相连, 且仅需要具有 MPLS 的基本信令功能和转发能力。在各 PE 设备上配置有多个虚拟路由转发 (Virtual Routing and Forwarding, VRF) 实例。这些 VRF 实例与 PE 设备上的一个

或多个子接口相对应,用于存放这些子接口所属 VPN 的路由信息。通常情况下,每一 VRF 实例中只包含一个 VPN 的路由信息,但当子接口属于多个 VPN 时,其所对应的 VRF 实例中则包含该子接口所属的所有 VPN 的路由信息。

[0027] 对于每一 VRF 实例都具有路由区分符 (Route Distinguisher, RD) 和路由目标 (Route Target, RT) 两大属性。其中, RD 用于避免不同 VPN 之间的地址重叠现象,具有全局唯一性。通常情况下,对于不同的 PE 设备上属于同一个 VPN 的子接口为其所对应的 VRF 实例分配相同的 RD,换句话说,就是为每一个 VPN 分配一个唯一的 RD。对于地址重叠的 VPN,由于 PE 设备上的某个子接口属于多个 VPN,此时该子接口所对应的 VRF 实例只能被分配一个 RD,从而多个 VPN 共享一个 RD。RT 用于路由信息的分发,分成入口 RT (Import RT) 和出口 RT (Export RT),分别用于路由信息的导入和导出策略。RT 同样具有全局唯一性,并且只能被一个 VPN 使用。

[0028] 在 VPN 业务建立后, PE 设备之间通过边界网关协议 (Border Gateway Protocol, BGP) 来传递 VPN 路由信息。具体来说,当一 PE 设备从某个子接口学习到来自 CE 设备的路由信息后,除了将该路由信息导入对应的 VRF 实例外, PE 设备还为该路由信息分配一 VPN 标签,该 VPN 标签用于识别接收该路由信息的子接口。然后,通过路由重新发布将 VRF 实例中的路由信息重新发布到 BGP 中,此时通过附加 VRF 实例的 RD 和 RT 参数,将原始路由信息转换成 VPN 路由信息。

[0029] 当一 PE 设备学习到对端的 PE 设备通过 BGP 传递的 VPN 路由信息后,先根据 RD 确定该 VPN 路由信息所属的 VRF 实例,然后去掉 VPN 路由信息所携带的 RD,使之还原成原始路由信息。随后,根据所属 VRF 实例配置的导入策略决定是否在本地 VRF 实例中导入该路由信息。

[0030] 在本实施例中,当一 PE 设备学习到对端的 PE 设备通过 BGP 传递的 VPN 路由信息后,触发创建一条到对端 PE 设备的 TE 隧道。在优选实施例中, TE 隧道的创建是基于隧道模板自动进行的。具体来说,在 PE 设备中设置有多个隧道模板。对于某 VPN 业务,利用隧道策略 (Tunnel Policy) 从多个隧道模板中选择并设定与该 VPN 业务关联的隧道模板。隧道策略包括按优先级顺序选择方式和 VPN 绑定方式。每一隧道模板作为一组配置命令的组合,用来控制 TE 隧道的公共属性,包括但不限于带宽、优先级、亲和属性、快速重路由 (Fast ReRoute, FRR)、隧道备份 (Backup) 以及自动带宽调整等。在其他实施例中,隧道策略也可省略,此时根据默认的隧道模板来控制 TE 隧道的公共属性。TE 隧道的创建以及各种属性的具体配置为本领域公知技术,在此不再赘述。

[0031] 在 TE 隧道创建后, VPN 业务通过该 TE 隧道传递 VPN 数据,即利用该 TE 隧道承载该 VPN 业务。具体来说,当入口 PE 设备通过某子接口从 CE 设备接收到一 VPN 分组数据后,入口 PE 设备从 VRF 实例中得到 VPN 标签和初始外层标签,并为该 VPN 分组数据打上外标签 (又称隧道标签) 和内标签 (又称 VPN 标签) 两层标签。随后,将打上标签的 VPN 分组数据发送到相应的 P 设备。P 设备之间根据外层标签逐跳转发该 VPN 分组数据,并在最后一个 P 设备弹出外层标签,将只包含 VPN 标签的 VPN 分组数据转发给出口 PE 设备。出口 PE 设备根据 VPN 标签确定对应的子接口,并将弹出 VPN 标签后的 VPN 分组数据通过该子接口发送到正确的 CE 设备。

[0032] 当 VPN 业务撤销后,响应 VPN 业务的撤销信息删除 TE 隧道。TE 隧道的具体删除过

程为本领域公知技术,在此不再赘述。

[0033] 请参见图 3,图 3 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第二应用场景的网络结构示意图。如图 3 所示,在本实施例中,本发明实施例的基于 TE 隧道的 VPN 实现方法应用于跨域的 MPLS L3VPN 场景。

[0034] 在图 3 所示的场景中,存在相互连接的至少两个 AS。不同的 AS 的自治系统边界路由器 (Autonomous System Border Router,ASBR) 相互作为 PE 设备和 CE 设备,进而也被称作背靠背跨域。其中,同一 AS 中的 PE 设备与 ASBR 之间可通过正常的多协议内部边界网关协议 (Multiprotocol-Internal Border Gateway Protocol,MP-IBGP) 传递 VPN 路由信息,而 ASBR 之间可通过外部边界网关协议 (External Border Gateway Protocol,EBGP) 传送 VPN 路由信息。

[0035] 在本场景中,为了在不同的 AS 的 PE 设备之间创建 TE 隧道,需要各 PE 设备和 ASBR 上均配置 VRF 实例,且在各 PE 设备和 ASBR 上为 VPN 路由信息设定相应的隧道模板,进而利用隧道模板在各 AS 的 PE 设备与 ASBR 之间分段建立 TE 隧道。同时,在 ASBR 之间则依靠网络互连协议 (Internet Protocol,IP) 连接。

[0036] 请参见图 4,图 4 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第三应用场景的网络结构示意图。如图 4 所示,在本实施例中,本发明实施例的基于 TE 隧道的 VPN 实现方法同样应用于跨域的 MPLSL3VPN 场景。

[0037] 在图 4 所示的场景中,同一 AS 中的 PE 设备与 ASBR 之间可通过正常的 MP-IBGP 传递 VPN 路由信息,而在 AS 之间可通过单跳的多协议外部边界网关协议 (Multiprotocol-External Border Gateway Protocol MP-EBGP) 传递 VPN 路由信息,进而被称为单跳 MP-EBGP 跨域。

[0038] 在本场景中,为了在不同的 AS 的 PE 设备之间创建 TE 隧道,需要在各 PE 设备上配置 VRF 实例,并且各 PE 设备的处理方式与第二应用场景相同。与第二应用场景的不同之处在于,ASBR 上不需配置 VRF 实例。此时,需要在 ASBR 上利用 BGP 路由策略为 BGP 对端 (BGP Peer) 设定隧道模板,进而利用该隧道模板在各 AS 的 PE 设备与 ASBR 之间分段创建 TE 隧道。

[0039] 请参见图 5,图 5 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第四应用场景的网络结构示意图。如图 5 所示,在本实施例中,本发明实施例的基于 TE 隧道的 VPN 实现方法同样应用于跨域的 MPLS L3VPN 场景。

[0040] 在图 5 所示的场景中,不同的 AS 的 PE 设备之间通过多跳的 MP-EBGP 传递 VPN 路由信息,进而被称为多跳 MP-EBGP 跨域。

[0041] 在本场景中,由于 PE 设备和 ASBR 之间传递的是带公网标签的 BGP 路由信息,因此不再需要利用 VPN 路由信息直接触发 TE 隧道的自动创建,而是在 PE 设备和 ASBR 上全部利用 BGP 路由策略为 BGP 对端设定隧道模板,并在 PE 设备学习到带公网标签的 BGP 路由信息后利用该隧道模板在各 AS 的 PE 设备与 ASBR 之间分段创建 TE 隧道。

[0042] 除了上述实施例所描述的 MPLS L3VPN 场景外,本发明实施例的基于 TE 隧道的 VPN 实现方法同样适用于多协议标签交换 (Multi-Protocol Label Switching, MPLS) 二层虚拟专用网络 (L2VPN) 应用场景,即 VPN 业务为 MPLS L2VPN 业务。目前,MPLS L2VPN 主要有虚拟租用线路 (Virtual leased Line, VLL) 和虚拟专用 LAN 服务 (Virtual Private LAN



Service, VPLS) 两种典型技术。其中, VLL 适用于点到点的 VPN 组网, VPLS 适用于点到多点或者多点到多点的 VPN 组网。此外, 按照传递 L2VPN 信息的方式, 又分为 SVC 方式、Martini 方式和 Kompella 方式。

[0043] 在 MPLS L2VPN 中, CE 设备与 PE 设备之间通过接入电路 (Attachment Circuit, AC) 连接, AC 是一条独立的链路或电路, AC 接口可以是物理接口或逻辑接口。PE 设备之间通过虚电路 (Virtual Circuit, VC) 进行逻辑连接。其中, SVC 方式采用静态配置方式设置二层虚拟专用网络虚电路信息 (L2VPN VC 信息), Martini 方式采用标签分发协议 (Label Distribution Protocol, LDP) 传递 L2VPN VC 信息, 而 Kompella 方式则采用 BGP 传递 L2VPN VC 信息。

[0044] 下面将结合具体实施例描述本发明实施例的基于 TE 隧道的 VPN 实现方法在各种 MPLS L2VPN 场景中的应用。

[0045] 请参见图 6, 图 6 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第五应用场景的网络结构示意图。如图 6 所示, 在本实施例中, 本发明实施例的基于 TE 隧道的 VPN 实现方法应用于由 VLL 方式实现的 MPLS L2VPN 场景。

[0046] 在图 6 所示的场景中, 通过静态或动态 L2VPN VC 信息来触发 TE 隧道的自动创建。具体来说, 在 PE 设备上配置 L2VPN VC 信息时设定隧道模板, 并根据 L2VPN VC 信息触发基于隧道模板的 TE 隧道的自动创建。其中, SVC 方式在配置 L2VPN VC 信息时直接触发基于隧道模板的 TE 隧道的自动创建, Martini 方式在学习到通过 LDP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建, 而 Kompella 方式则在学习到通过 BGP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建。

[0047] 请参见图 7, 图 7 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第六应用场景的网络结构示意图。如图 7 所示, 在本实施例中, 本发明实施例的基于 TE 隧道的 VPN 实现方法应用于由 VPLS 技术实现的 MPLS L2VPN 场景。

[0048] 在图 7 所示的场景中, 通过动态 L2VPN VC 信息来触发 TE 隧道的自动创建。具体来说, Martini 方式在配置虚拟交换接口 (Virtual Switch Interface, VSI) 对等体时设定隧道模板, 并在学习到通过 LDP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建, 而 Kompella 方式则在配置 VSI 实例时设定隧道模板, 在学习到通过 BGP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建。

[0049] 此外, MPLS L2VPN 还有一种边缘到边缘的伪线仿真 (Pseudo-Wire Emulation Edge to Edge, PWE3) 技术。PWE3 技术按照传递 L2VPN VC 信息的方式分为静态伪线 (Pseudo-Wire, PW) 和动态 PW, 而按照实现方案分为单跳 PW 和多跳 PW。

[0050] 本发明实施例的基于 TE 隧道的 VPN 实现方法在静态 PW 下的实现方式与上文描述的 SVC 实现方式类似, 主要是通过静态 L2VPN VC 信息触发基于隧道模板的 TE 隧道的自动创建。本发明实施例的基于 TE 隧道的 VPN 实现方法在动态 PW 下的实现方式与上文描述的 Martini 方式的 VLL 技术类似, 主要是通过 LDP 协议传递的动态 L2VPN VC 信息触发基于隧道模板的 TE 隧道的自动创建。在 PWE3 技术中, 需要特别提到的是如图 8 所示的多跳 PW 场景。

[0051] 在图 8 所示的场景中, 将 PE 设备划分为端点服务商边缘 (Ultimate PE, U-PE) 和交换服务商边缘 (Switching PE, S-PE) 两层, 共同完成一个 PE 设备的功能。因此, 需要在

S-PE 上配置交换伪线时设定隧道模板,并在学习到通过 LDP 传递的 L2VPN VC 信息后触发基于隧道模板的 TE 隧道的自动创建。

[0052] 通过上述方式,本实施例的基于 TE 隧道的 VPN 实现方法能够在 MPLS L3VPN 和 MPLS L2VPN 场景中根据 VPN 业务的需要动态创建或删除 TE 隧道,提供了一种 TE 隧道按需创建的机制,并及时删除不被 VPN 业务使用的隧道,有效地节省了网络资源。

[0053] 请参见图 9,图 9 是根据本发明实施例的基于 TE 隧道的 VPN 实现方法的第八应用场景的网络结构示意图。如图 9 所示,在本实施例中,本发明实施例的基于 TE 隧道的 VPN 实现方法用于实现 VPN 业务的分级服务。

[0054] 在图 9 所示的场景中,虚线所示的转发平面的转发能力相对较强,而实线所示的转发平面的转发能力相对较弱。因此,可设置两个不同的第一隧道模板和第二隧道模板。在 PE 设备上为业务要求较高的 VPN 业务设定第一隧道模板来触发创建 TE 隧道,使得承载该 VPN 业务的 TE 隧道限定在虚线所示的转发平面。同时,在 PE 设备上为业务要求较低的 VPN 业务设定第二隧道模板来触发创建 TE 隧道,使得承载该 VPN 业务的 TE 隧道限定在实线所示的转发平面。

[0055] 通过上述方式,对于不同业务要求的 VPN 业务设定不同的隧道模板,以创建满足各自业务需要的 TE 隧道,实现整个网络按照业务类型提供差分服务,不同 VPN 业务之间互不影响。

[0056] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成,上述程序可以存储于一计算机可读取存储介质中,上述存储介质可以是 ROM/RAM、磁碟、光盘等。该程序在执行时,包括如下步骤:

[0057] 响应 VPN 业务的建立信息创建 TE 隧道;

[0058] 利用该 TE 隧道承载该 VPN 业务;以及

[0059] 响应该 VPN 业务的撤销信息删除该 TE 隧道。

[0060] 请参见图 10,图 10 是根据本发明实施例的基于 TE 隧道的 VPN 实现系统的示意框图。如图 10 所示,本实施例的基于 TE 隧道的 VPN 实现系统主要包括隧道建立模块 1001、隧道维护模块 1002 以及隧道删除模块 1003。

[0061] 其中,隧道建立模块 1001 响应 VPN 业务的建立信息创建 TE 隧道,隧道维护模块 1002 利用该 TE 隧道承载 VPN 业务,隧道删除模块 1003 则响应该 VPN 业务的撤销信息删除该 TE 隧道。

[0062] 通过上述方式,本发明实施例的基于 TE 隧道的 VPN 实现系统根据 VPN 业务的需要动态创建或删除 TE 隧道,提供了一种 TE 隧道按需创建的机制,并及时删除不被 VPN 业务使用的隧道,有效地节省了网络资源。

[0063] 下面将结合图 2-9 所示的应用场景详细描述各模块的功能,上述各模块一般设置于 PE 设备上,例如 PE 路由器。

[0064] 在图 2 所示的应用场景中,当学习到对端的 PE 设备通过 BGP 传递的 VPN 路由信息后,隧道建立模块 1001 触发创建一条到对端 PE 设备的 TE 隧道。在优选实施例中,TE 隧道的创建是基于隧道模板自动进行的。具体来说,在 PE 设备中设置有多个隧道模板。针对某 VPN 业务,利用隧道策略(Tunnel Policy)从多个模板中选择并设定与该 VPN 业务关联的隧道模板。隧道策略包括按优先级顺序选择方式和 VPN 绑定方式。每一隧道模板作为一组配

置命令的组合,用来控制 TE 隧道的公共属性,包括但不限于带宽、优先级、亲和属性、快速重路由 (Fast ReRoute, FRR)、隧道备份 (Backup) 以及自动带宽调整等。在其他实施例中,隧道策略也可省略,此时根据默认的隧道模板来控制 TE 隧道的公共属性。TE 隧道的创建以及各种属性的配置为本领域公知技术,在此不再赘述。

[0065] 在图 3 所示的场景中,为了在不同的 AS 的 PE 设备之间创建 TE 隧道,隧道建立模块 1001 需要在各 PE 设备和 ASBR 上均配置 VRF 实例,且在各 PE 设备和 ASBR 上为 VPN 路由信息设定相应的隧道模板,进而使得隧道建立模块 1001 利用隧道模板在各 AS 的 PE 设备与 ASBR 之间分段建立 TE 隧道。

[0066] 在图 4 所示的场景中,为了在不同的 AS 的 PE 设备之间创建 TE 隧道,隧道建立模块 1001 需要在各 PE 设备上配置 VRF 实例,并且各 PE 设备的处理方式与第二应用场景相同。与第二应用场景的不同之处在于,ASBR 上不需配置 VRF 实例。此时,需要在 ASBR 上利用 BGP 路由策略为 BGP 对端 (BGP Peer) 设定隧道模板,进而使得隧道建立模块 1001 能够利用该隧道模板在各 AS 内的 PE 设备与 ASBR 之间分段创建 TE 隧道。

[0067] 在图 5 所示的场景中,由于 PE 设备和 ASBR 之间传递的是带公网标签的 BGP 路由信息,因此隧道建立模块 1001 不再需要利用 VPN 路由信息直接触发 TE 隧道的自动创建,而是在 PE 设备和 ASBR 上全部利用 BGP 路由策略为 BGP peer 设定隧道模板,并学习到带公网标签的 BGP 路由信息后利用该隧道模板在各 AS 内的 PE 设备与 ASBR 之间分段创建 TE 隧道。

[0068] 在图 6 所示的场景中,隧道建立模块 1001 通过静态或动态 L2VPN VC 信息来触发 TE 隧道的自动创建。具体来说,隧道建立模块 1001 配置 L2VPN VC 信息时设定隧道模板,并根据 L2VPN VC 信息触发基于隧道模板的 TE 隧道的自动创建。其中, SVC 方式在配置 L2VPN VC 信息时直接触发基于隧道模板的 TE 隧道的自动创建, Martini 方式在学习到通过 LDP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建,而 Kompella 方式则在学习到通过 BGP 传递的对端 L2VPNVC 信息时触发基于隧道模板的 TE 隧道的自动创建。

[0069] 在图 7 所示的场景中,隧道建立模块 1001 通过动态 L2VPN VC 信息来触发 TE 隧道的自动创建。具体来说, Martini 方式在配置 VSI 对等体时设定隧道模板,并在学习到通过 LDP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建,而 Kompella 方式则在配置 VSI 实例时设定隧道模板,在学习到通过 BGP 传递的对端 L2VPN VC 信息时触发基于隧道模板的 TE 隧道的自动创建。

[0070] 在图 8 所示的场景中,隧道建立模块 1001 需要在 S-PE 上配置交换 PW 时设置隧道模板,并在学习到通过 LDP 传递的 L2VPN VC 信息后触发基于隧道模板的 TE 隧道的自动创建。

[0071] 通过上述方式,本发明实施例的基于 TE 隧道的 VPN 实现系统能够在 MPLS L3VPN 和 MPLS L2VPN 场景中根据 VPN 业务的需要动态创建或删除 TE 隧道,提供了一种 TE 隧道按需创建的机制,并及时删除不被 VPN 业务使用的隧道,有效地节省了网络资源。

[0072] 在图 9 所示的场景中,虚线所示的转发平面的转发能力相对较强,而实线所示的转发平面的转发能力相对较弱。因此,隧道建立模块 1001 可设置两个不同的第一隧道模板和第二隧道模板。进一步,隧道建立模块 1001 为业务要求较高的 VPN 业务设定第一隧道模板来触发创建 TE 隧道,使得承载该 VPN 业务的 TE 隧道限定在虚线所示的转发平面。同时,隧道建立模块 1001 为业务要求较低的 VPN 业务设定第二隧道模板来触发创建 TE 隧道,使

得承载该 VPN 业务的 TE 隧道限定在实线所示的转发平面。

[0073] 通过上述方式,对于不同业务要求的 VPN 业务设定不同的隧道模板,以创建满足各自业务需要的 TE 隧道,实现整个网络按照业务类型提供差分服务,不同 VPN 业务之间互不影响。

[0074] 以上所述仅为本发明的实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

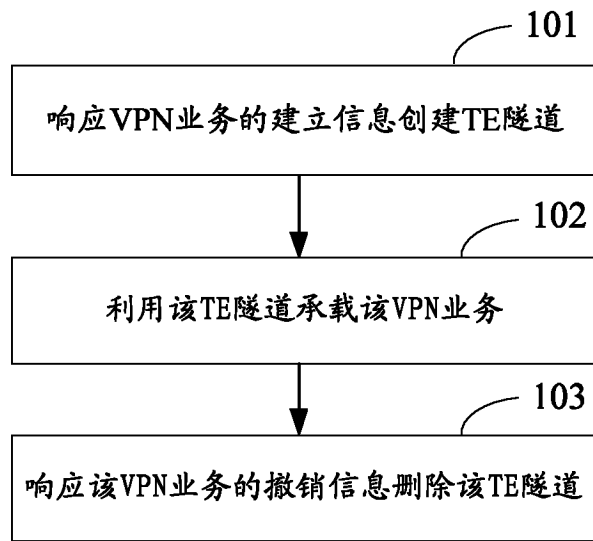


图 1

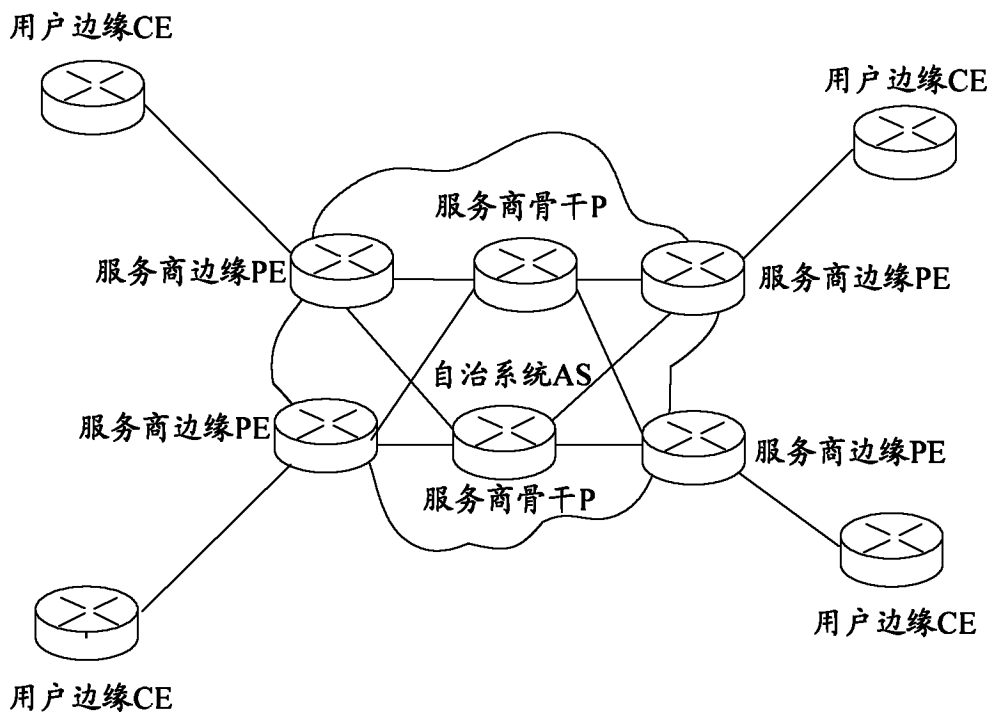


图 2

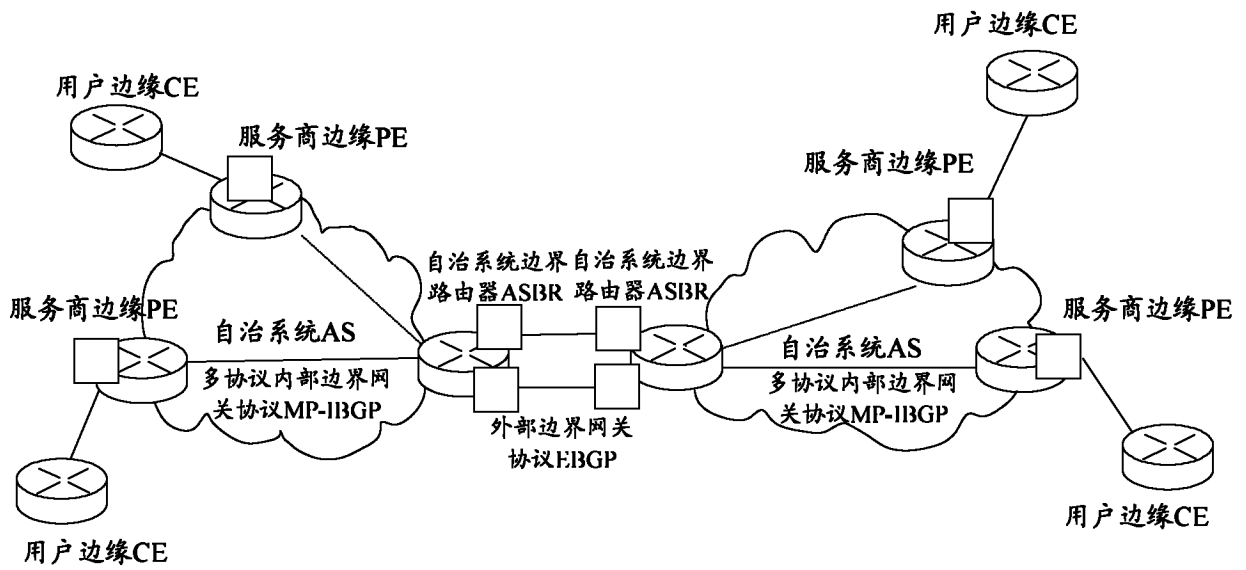


图 3

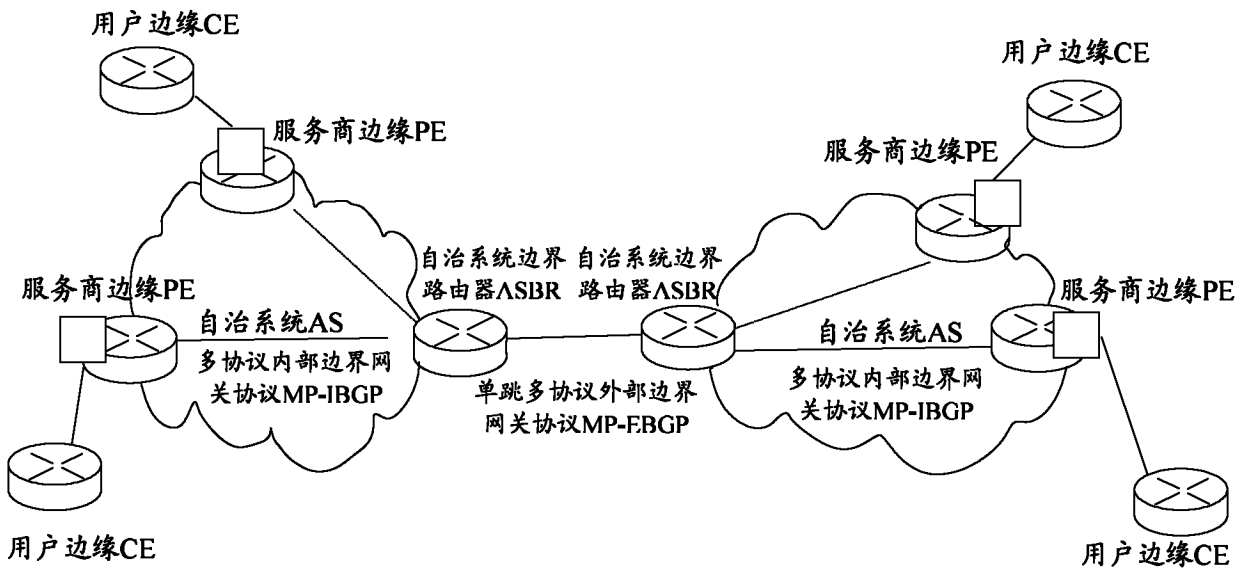


图 4

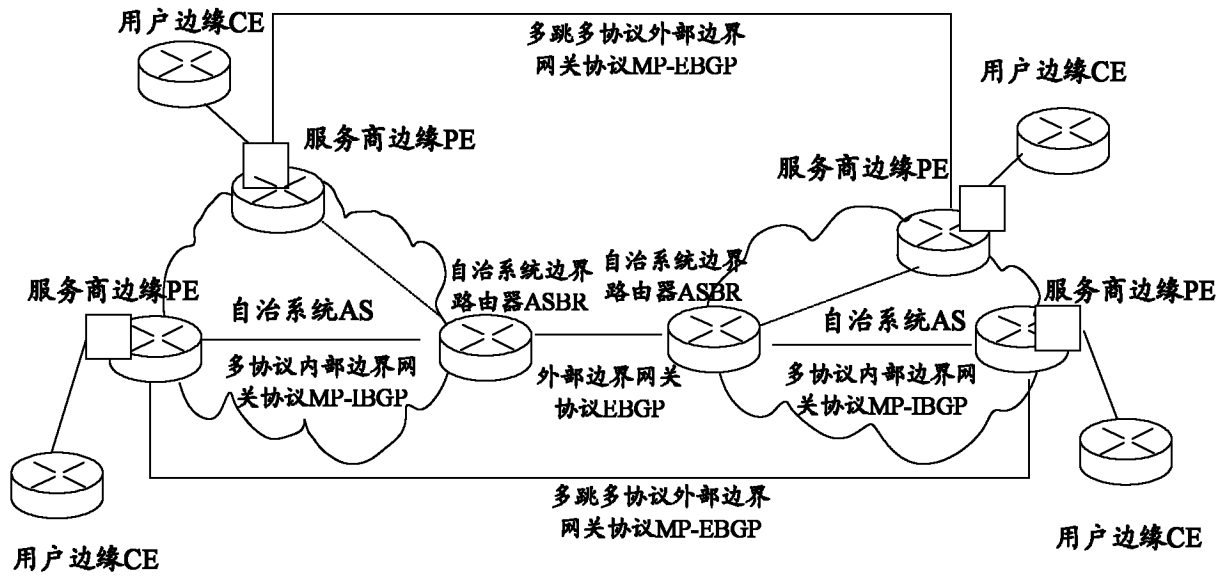


图 5

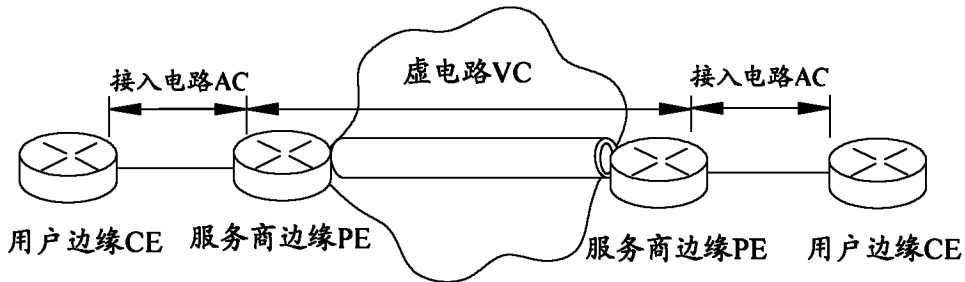


图 6

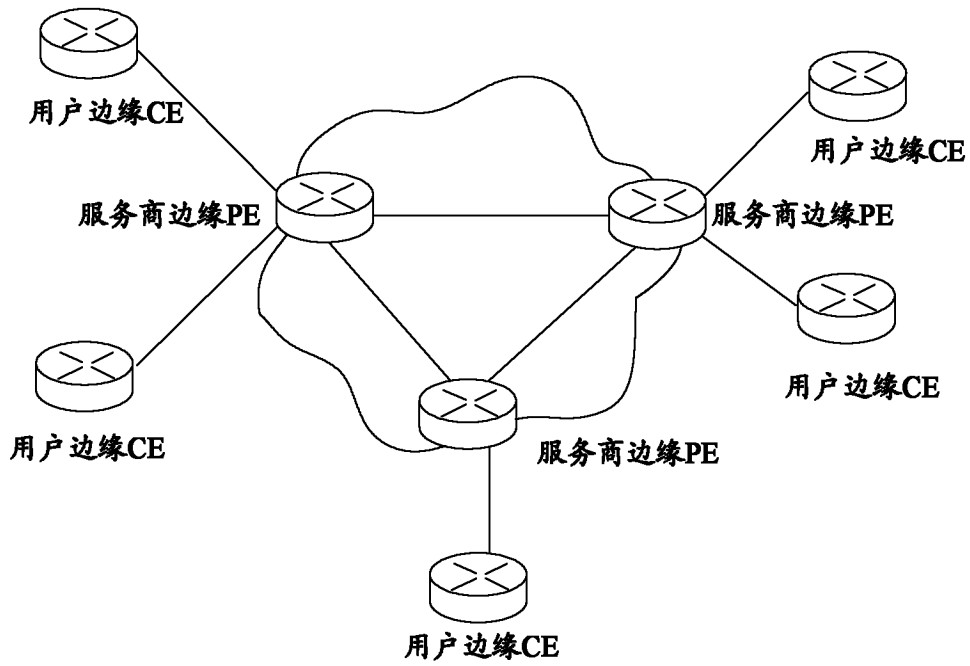


图 7

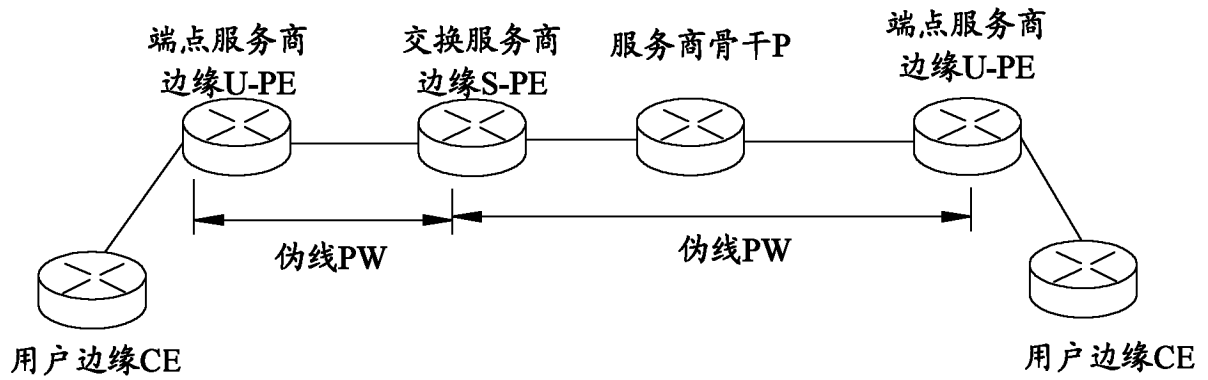


图 8



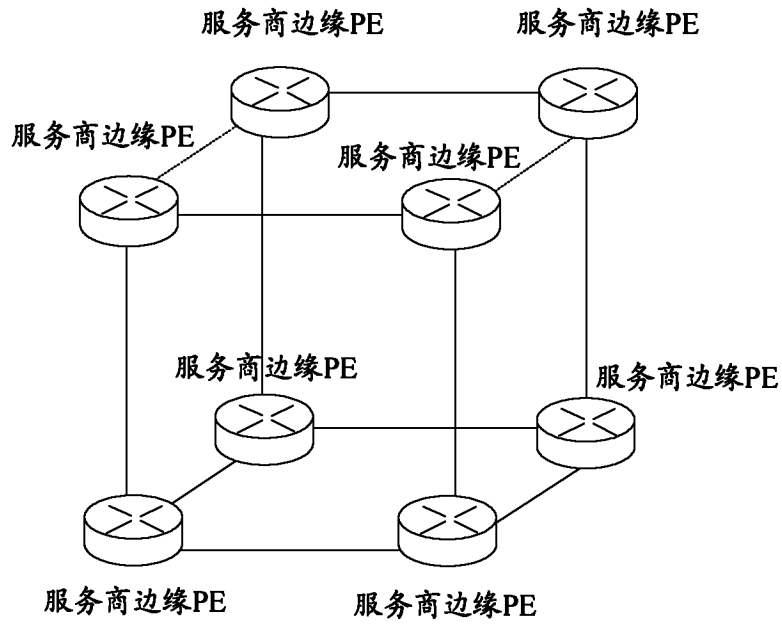


图 9

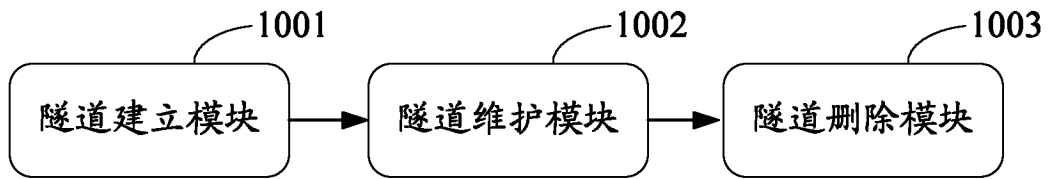


图 10