

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/56 (2006.01)

H04L 12/28 (2006.01)



## [12] 发明专利申请公布说明书

[21] 申请号 200680004180.4

[43] 公开日 2008年5月14日

[11] 公开号 CN 101180839A

[22] 申请日 2006.2.22

[21] 申请号 200680004180.4

[30] 优先权

[32] 2005.3.28 [33] US [31] 11/091,058

[86] 国际申请 PCT/US2006/006232 2006.2.22

[87] 国际公布 WO2006/104604 英 2006.10.5

[85] 进入国家阶段日期 2007.8.6

[71] 申请人 思科技术公司

地址 美国加利福尼亚州

[72] 发明人 托马斯·D·纳德奥

迈克尔·T·派库彻 旺松·利姆

罗伯特·汉兹

[74] 专利代理机构 北京东方亿思知识产权代理有限  
责任公司

代理人 王 怡

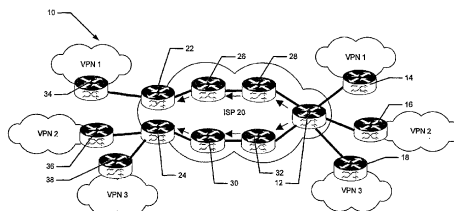
权利要求书4页 说明书12页 附图5页

### [54] 发明名称

基于网络的虚拟专用网的服务级别诊断测试  
点的自调整库

### [57] 摘要

提供了一种产生并维护用于基于网络的虚拟专用网的服务级别测试点库的方法及装置。确定在用于一个或多个虚拟专用网的网络中是否存在不止一个自治系统(AS)。当不存在不止一个自治系统时,找到用于虚拟专用网的下一跳。接下来,找到与虚拟专用网相关联的虚拟专用网前缀,并产生用于虚拟专用网的使用中的一组标签交换路径(LSP)。当确定存在不止一个的自治系统时,找到在与虚拟专用网相关联的当前自治系统中的路由器。虚拟专用网标签栈被用于找到与虚拟专用网相关联的所有供应商边缘(PE)路由器。从路由器及虚拟专用网标签栈中产生用于虚拟专用网的使用中的一组标签交换路径。



1. 一种用于基于网络的虚拟专用网的服务级别测试点库的产生和维护方法，包括：

选择对用于至少一个感兴趣的虚拟专用网的网络中的单个自治系统配置还是多个自治系统配置执行所述方法；

当所述选择结果是选择了单个自治系统配置，则：

找到用于所述至少一个感兴趣的虚拟专用网的下一跳；

找到与所述至少一个感兴趣的虚拟专用网相关联的虚拟专用网前缀；以及

从所述下一跳和所述虚拟专用网前缀中确定用于所述至少一个感兴趣的虚拟专用网的使用中的一组标签交换路径；

当所述选择结果是选择了多个自治系统配置，则：

找到在与所述至少一个感兴趣的虚拟专用网相关联的当前自治系统中的路由器；以及

找到与所述至少一个感兴趣的虚拟专用网相关联的所有提供商边缘路由器以及自治系统边界路由器；

从所述路由器中确定用于所述至少一个感兴趣的虚拟专用网的使用中的一组标签交换路径；以及

使得所述一组标签交换路径可用于其他处理。

2. 如权利要求 1 所述的方法，其中所述确定一组标签交换路径还包括过滤所述一组标签交换路径，以去除不期望的路径。

3. 如权利要求 1 所述的方法，其中所述确定一组标签交换路径还包括删减所述一组标签交换路径，以去除不活动的路径。

4. 如权利要求 3 所述的方法，其中所述删减包括从所述一组标签交换路径中去除重复的路径。

5. 如权利要求 1 所述的方法，其中所述确定一组标签交换路径还包括通过处理路由更新信息，来保持所述一组标签交换路径组最新。

6. 如权利要求 5 所述的方法，其中所述保持包括在预定时间执行路由

更新。

7. 如权利要求 1 所述的方法，其中所述找到用于所述至少一个感兴趣的虚拟专用网的下一跳包括发现与所述感兴趣的虚拟专用网相关联的标签栈的外部 IGP 标签可到达的下一跳。

8. 如权利要求 7 所述的方法，其中所述找到与所述至少一个感兴趣的虚拟专用网相关联的虚拟专用网前缀包括发现用于所述标签栈的前缀。

9. 如权利要求 1 所述的方法，其中所述找到与所述至少一个感兴趣的虚拟专用网相关联的所有提供商边缘路由器包括找到与所述提供商边缘路由器相关联的虚拟路由和转发表正在使用的所有标签交换路径。

10. 一种标签交换路径发现系统，包括：

与至少一个客户端通信的标签交换路径发现数据库；

与所述标签交换路径发现数据库以及至少一个路由处理通信的缺省路由表；

与所述标签交换路径发现数据库以及所述至少一个路由处理通信的至少一个虚拟专用网路由表；以及

用于将路由信息分发到所述路由表中的路由处理，其中，所述系统能够在所述标签交换路径发现数据库中产生并维护用于基于网络的虚拟专用网的服务级别测试点的库。

11. 如权利要求 10 所述的标签交换路径发现系统，其中所述标签交换路径发现数据库与所述路由表交互，以收集使用中的下一跳。

12. 如权利要求 10 所述的标签交换路径发现系统，其中来自所述标签交换路径发现数据库的信息可用于至少一个客户端。

13. 如权利要求 12 所述的标签交换路径发现系统，其中所述客户端被通知了数据库的变化。

14. 如权利要求 10 所述的标签交换路径发现系统，其中通过执行对所述路由表的扫描和通过路由更新，所述数据库被维护。

15. 如权利要求 10 所述的标签交换路径发现系统，其中所述路由表将用于每一虚拟专用网的路由与下一跳信息一起存储。

16. 如权利要求 10 所述的标签交换路径发现系统，其中所述系统能够

执行以下操作：

选择对用于至少一个感兴趣的虚拟专用网的网络中的单个自治系统配置还是多个自治系统配置执行所述方法；

当所述选择结果是选择了单个自治系统配置，则：

找到用于所述至少一个感兴趣的虚拟专用网的下一跳；

找到与所述至少一个感兴趣的虚拟专用网相关联的虚拟专用网前缀；以及

从所述下一跳和所述虚拟专用网前缀中确定用于所述至少一个感兴趣的虚拟专用网的使用中的一组标签交换路径；

当所述选择结果是选择了多个自治系统配置，则：

找到在与所述至少一个感兴趣的虚拟专用网相关联的当前自治系统中的路由器；以及

找到与所述至少一个感兴趣的虚拟专用网相关联的所有提供商边缘路由器以及自治系统边界路由器；

从所述路由器中确定用于所述至少一个感兴趣的虚拟专用网的使用中的一组标签交换路径；以及

使得所述一组标签交换路径可用于其他处理。

17. 一种用于产生并维护用于基于网络的虚拟专用网的服务级别测试点库的系统，包括：

用以选择对用于至少一个感兴趣的虚拟专用网的网络中的单个自治系统配置还是多个自治系统配置执行所述方法的装置；

当所述选择结果是选择了单个自治系统配置，则：

用以找到用于所述至少一个感兴趣的虚拟专用网的下一跳的装置；

用以找到与所述至少一个感兴趣的虚拟专用网相关联的虚拟专用网前缀的装置；以及

用以从所述下一跳和所述虚拟专用网前缀中确定用于所述至少一个感兴趣的虚拟专用网的使用中的一组标签交换路径的装置；

当所述选择结果是选择了多个自治系统配置，则：

用以找到在与所述至少一个感兴趣的虚拟专用网相关联的当前自治系统中的路由器的装置；以及

用以找到与所述至少一个感兴趣的虚拟专用网相关联的所有提供商边缘路由器以及自治系统边界路由器的装置；

用以从所述路由器中确定用于所述至少一个感兴趣的虚拟专用网的使用中的一组标签交换路径的装置；以及

用以使得所述一组标签交换路径可用于其他处理的装置。

## 基于网络的虚拟专用网的服务级别诊断测试点的自调整库

### 背景技术

计算机网络通常在不同计算机之间提供实体互连，从而使得能够便利地交换程序及数据。多个诸如开关和路由器之类的连接设备将每个连接到网络的用户计算机互连。连接设备维护计算机的路由信息，并执行关于计算机之间经由连接设备传递的消息流量的路由决定。每个连接设备或路由器与表示其已经直接或间接访问的其他计算机的网络路由前缀（prefix）相对应。因此，从一个计算机发送到另一计算机的数据沿着由两个计算机之间的路由器定义的路径穿过网络。

路由器定义网络中的节点，且数据在网络上一系列所谓“跳（hop）”的节点之间传送。由于每个路由器通常被连接到多个其他的路由器，所以在给定计算机之间可能存在多个可能路径。通常，在每个路由器中的路由表中使用路由信息，路由信息被用于确定到目的地计算机或网络的路径。路由器利用路由表做出路由决定，以识别下一“跳”，或下一路由器，从而将数据依次发送使其最终到达目的地计算机。然而，可能出现网络问题致使路由器以及路由器之间的传输路径不可操作。

存在两类路径特性及其验证/诊断，当考虑基于网络的互联网协议（IP）虚拟专用网（VPN）时，这是尤其被感兴趣的。第一类路径特性与根据基础连接的路径验证相关。基于网络的 VPN 的用户所感兴趣的第二类特性落入实时统计的范围。这些实时统计可被定义为用户边缘（CE）路由器获得与如下具体路径相关的实时统计的能力：CE 用该具体路径来将其流量承载穿过基于网络的 VPN 提供商的核心。这样的属性性质包含（但并不局限于）延迟（单向或往返程）、抖动（jitter）以及错误率（即，包丢失/错误）。目前一些服务提供商提供这些类型的统计，然而这些统计很大程度上是基于平均值的，将其用于用户计算实时路径特性是不

够的。

希望得到诸如延迟及抖动之类的各种路径特性的上至分钟的值，以便实时地使具体路径合格，从而当一些诸如延迟之类的路径特性被检测为异常高时，易于故障查找，立即修补破坏的路径，或者为了选择替代路径（即：改变路由行为，从而使网络缺陷对用户而言不明显），或者只是为了获得如下的信息：所请求的路径属性是否被核心网络在任意给定点及时地传送。

某些应用，例如可从加州圣何塞的思科系统公司得到的服务保证代理（Service Assurance Agent, SAA），可被用户在其用户边缘路由器之间使用以验证使用 IP 协议包的端到端路径。这些应用提供了关于整体端到端路径的重要信息，但是并未提供任何关于在其位置之间实际传输 IP 流量的提供商 PE 路由器之间的关键核心网络路径的直接信息。因此，用户不能够肯定具体问题位于网络中的哪个区段，或者哪些具体的路径特性在任意具体点被及时地传送。基于网络的 IP 用户可利用这些信息来触发在其 PE 到 CE 链路上适当的 QoS 参数设置调整，触发局部链路更新等等，如果服务级别协议（Service Level Agreement, SLA）降级原因位于这些链路上。服务提供商必需利用 MPLS 特定工具及算法收集这些信息，以确保当将其用于纠正由他们检测到的任何缺陷时，其准确性和高效性。

在具体示例中，客户端能够识别一组“重要的”目的地，针对这些“重要的”目的地，要求实时地收集路径属性（因为必需测量特定路径的性能）。注意，术语“实时”并非指代路径属性被获取的频度，而是用于标识在经授权的 CE 明确请求时，这些信息被收集的事实。客户端能够识别要收集路径属性的一组重要目的地。

许多标签交换路径（label switched path）可被用于为许多不同的应用传输流量，所述应用例如在 MPLS 网络的端点之间的流量工程（Traffic Engineering）或 MPLS L3 VPN。在某些情况下，这些路径可包含许多被称作负载分享路径（load-share path, LSP）的并行等开销分支。当这些路径穿过网络时可能相当发散，但是最终在相同的端点处停止。这些路径使得流量能够在等开销链路中被更好的分布，从而更好地利用网络中的可用带

宽。负载分享路径虽然有其自身的优点，但它在测试这些路径的每一个的特性方面也存在潜在的困难。此外，仅是这些 LSP 的子集在任意给定的时间点处正在被任一给定的 VPN 使用的事实更增大了此困难。路径的实际选择也是很大程度上依赖于由具体类型的转发硬件（即：路由器）做出的局部转发决定。

### 发明内容

诸如以上所说明的传统机制存在多种缺陷。这些缺陷之一是操作者必需利用手动手段来“发现”VPN 所使用的路径及其组合，所述手动手段例如在沿 LSP 的每一设备上的抓取大量命令行接口（Command Line Interface, CLI）屏幕。这是耗时且易出错的，不精确并且麻烦，而且最终可能因太慢而使得操作者不能对 VPN 网络中的变化做出反应。

本发明的实施方式有效的克服了这些缺陷并提供了如下的机制和技术，所述机制和技术可通过确定哪些 PE 路由器以及到这些路由器的路径将被使用，自动地确定哪些 LSP 路径可能正在被给定的 L3 VPN 使用。这使得系统能够确切地知道哪些 LSP 对于具体的 VPN 是重要的，并且使得这些 LSP 能够被验证或以其他方式被测量。

通过所描述的方法及设备，VPN（或用以测试路径的工具）所使用的路径以及对这些路径的任何更新被动态地发现，从而允许 LSP 发现处理能够运行而无需操作者干涉。例如，如果不再使用一个路径，则将其从待测试路径列表中动态地删除。在过去，操作者必需手动地发现此路径并将其删除，从而导致浪费网络带宽及处理，并且导致因这些路径对测试没有响应（因为他们不再存在）而出现无效警报的可能性。此外，如果在待验证的 PE 列表中某些 PE 是不期望的，则所述方法及设备可对条目过滤。例如，如果操作者采用大量的 PE，则可能仅希望测试这些 PE 的一个子集（可能基于某些统计置信度或局部试探（local heuristic））。另一重要使用是过滤位于具体 ASBR 之外的条目，因为其数目可能是巨大的。

本方法及设备提供了一次且仅一次测试任意两个 PE 设备之间的路径的能力。在 L3 VPN 的情况下，PE（PE1）可能容留不止一个虚拟路由转



发实例（例如：VPN），并且那些 VPN 可能具有到相同远程 PE（PE2）的连接。在这种情况下，显然的应用可能是测试从 PE1 到 PE2 的 VRF A 和 VRF B 之间的路径，因此测试了两遍相同的 LSP（经常的情况是相同的 LSP 穿过核心网络在 PE 之间行进）。本方法及设备能够滤除重复，进一步优化并增强其效用。

当基于路由更新（实际上被用于转发数据，因此存储在本发明所管理的数据库中的数据可即时地保持最新）描述具体实施方式时，还可以利用计时器来实施本发明，当计时器到时的时候，将引起本发明检查当前路由数据库并相应地更新该数据库。

一种用于基于 VPN 的网络的服务级别测试点的库的产生和维护方法的具体实施方式包括：选择对用于至少一个感兴趣的 VPN 中的单个自治系统（AS）配置还是多个 AS 配置执行所述方法。当选择是对单个 AS 配置执行所述方法时，用于至少一个感兴趣的 VPN 的下一跳被找到。接下来，与所述至少一个感兴趣的 VPN 相关联的 VPN 前缀被找到，并且从下一跳和 VPN 前缀中产生用于所述至少一个感兴趣的 VPN 的使用中的一组 LSP。这组 LSP 可用于其他处理。

当所述选择是存在不止一个 AS 时，在与所述至少一个感兴趣的 VPN 相关联的当前 AS 中的路由器被找到。与所述至少一个感兴趣的 VPN 相关的所有提供商边缘（PE）路由器及/或自治系统边界路由器（ASBR）被找到。用于所述至少一个感兴趣的 VPN 的使用中的一组 LSP 被产生。这组 LSP 可用于其他处理。

其他实施方式包含其上具有计算机可读代码的计算机可读介质，所述计算机可读介质用于提供产生并维护用于基于网络的 VPN 的服务级别测试点库的处理。介质包含用以选择对用于至少一个感兴趣的 VPN 的单个 AS 配置还是多个 AS 配置执行所述方法的指令。介质还包含用以当不存在多于一个 AS 时找到用于所述至少一个感兴趣的 VPN 的下一跳的指令。介质还包括用以找到与所述至少一个感兴趣的 VPN 相关联的 VPN 前缀并且从下一跳和 VPN 前缀中产生用于所述至少一个感兴趣的 VPN 的使用中的一组 LSP 的指令。介质还包含用以使得这组 LSP 可用于其他处理的指令。

介质还可包含用以当所述选择是存在不止一个 AS 时找到与所述至少一个感兴趣的 VPN 相关的路由器，以找到与所述至少一个感兴趣的 VPN 相关的所有提供商边缘 (PE) 路由器的指令。介质包含用以产生用于所述至少一个感兴趣的 VPN 的使用中的一组 LSP 的指令。介质还包含用以使得这组 LSP 可用于其他处理的指令。

其他实施方式还包含计算机化设备，该计算机化设备被配置为处理在此作为本发明的实施方式公开的所有方法操作。在这样的实施方式中，计算机化设备包含存储器系统、处理器，以及以一种连接机制将这些部件连接的通信接口。根据如下的处理编码所述存储器系统：提供了在此说明的产生并维护用于基于网络的 VPN 的服务级别测试点的库的处理，当所述处理在处理器上被执行时（例如，当执行所述处理时），在计算机化设备中如在此所说明的进行操作以执行在此作为本发明的实施方式说明的所有的方法实施方式及操作。因此，任何执行或被编程以执行这里说明的以上处理的计算机化设备都是本发明的实施方式。

在此公开的本发明的实施方式的其他配置包含以上所总结的并将在以下详细公开的用于执行所述方法实施方式的步骤及操作的软件程序。更具体而言，计算机程序产品是一种具有其上包含已编码的计算机程序逻辑的计算机可读介质的实施方式，当在计算机化设备上执行所述计算机程序逻辑时则提供相关操作，即提供如在此所说明的产生并维护用于基于网络的 VPN 的服务级别测试点库的方法及设备。当在至少一个具有计算系统的处理器上执行所述计算机程序逻辑时，将使得处理器执行在此作为本发明的实施例指示的操作（例如，方法）。本发明的这样的配置通常被设置为计算机可读介质上配置或编码的软件、代码及/或其他数据结构，所述计算机可读介质例如光介质（例如，CD-ROM），软盘（floppy）或硬盘，或其他介质，例如一或多个 ROM、或 RAM、或 PROM 芯片中的固件或微代码，或专用集成电路（ASIC），或一个或多个模块中的可下载软件镜像，共享程序库等等。软件或固件或其他此类配置可被安装到计算机化设备上以使得所述计算机设备中的一或多个处理器执行在此作为本发明的实施方式说明的技术。在诸如数据通信设备组或其他实体之类的计算机化设备的

集合中操作的软件处理也具有本发明的系统。本发明的系统可分布在几个数据通信设备上的多个软件处理之间，或者所有处理可在较小的专用计算机组或一个单独的计算机上运行。

应理解，例如在数据通信设备中，本发明的实施方式可作为软件程序、作为软件和硬件，或作为硬件及/或单独的电路被确实地实施。

### 附图说明

通过以下对如附图中所示出的本发明优选实施方式的更具体的描述，本发明的前述及其他目的、特征及优点将变得明了，其中相同参考字符指代不同视图中的相同部分。图形未必是按比例绘制的，而是强调示出本发明的原理。

图 1 示出了基础 VPN 部署情况的框图；

图 2 示出了 Inter-AS VPN 部署情况的框图；

图 3 示出了根据本发明的一个实施方式的 LSP 发现系统的框图；

图 4A 和图 4B 包括根据本发明的实施方式的用于基于网络的 VPN 的服务级别诊断测试点的自调整库的创建和维护方法的流程图。

### 具体实施方式

在 MPLS L3 VPN 网络中，诸如 BGP 之类的信令协议建立了提供商边缘 (PE) 路由器和自治系统边界路由器 (ASBR) 之间的会话。这些路径被实现为 MPLS 标签交换路径 (Label Switched Path, LSP)。经由多个 MPLS 控制面信令协议 (即：LDP 或 RSVP-TE) 向 LSP 发送信号。当记录用于到达远程 PE 路由器的 LSP 时，诸如 BGP 之类的信令协议在 PE 和 ASBR 之间交换 VPN 路由 (VPNv4 或 VPNv6)。LSP 被指定为用于为具体的 VPN 所安装的每个 VPNv4 路由的递推的下一跳。VPN 所使用的 LSP 以具有两个标签的标签栈为起点。外部是 IGP 标签。此标签在紧接 BGP 下一跳之前出栈。内部标签是 VPN 标签，其在 LSP 的最终目的地出栈。

用于基于网络的 VPN 的服务级别诊断测试点的自调整库的创建和维

护方法及装置（也被称作 LSP 发现）周期性地扫描期望的 VRF 路由表中的所有路由，并且接收路由更新以便构造被指定给每个路由的下一跳 LSP 的数据库。过滤策略然后被用于从数据库中除去不期望的端点。此时重复也被从数据库去除，从而防止了测试工具重复测试代表不同 VPN 的相同下一跳（参见以上给出的示例）。然后数据库可被客户端路径测试工具读取，从而自动地向其提供要测试 LSP 路径特性的端点。

LSP 发现可用于单个 AS 配置和多个 AS 配置二者。在单个 AS 配置中，VRF 正在使用的用于到达每个 BGP 下一跳的 LSP 被发现。此方法使得允许验证 AS 中的所有 PE 和 ASBR。这可以不提供更复杂的 VPN 拓扑的端到端的覆盖。在一些自治系统间（Inter-AS）的情况下，在其他 AS 中的 PE 及 ASBR 将不会到达。代替发现下一跳，用于多个 AS 配置的 LSP 发现是发现 VPN 前缀。

以下是在不同的 VPN 情况下当正确配置 LSP 发现时所期望的结果：

1. 简单 VPN – LSP 发现将发现到每个使用中的目的地 PE 的 LSP。
2. Inter-AS（背对背（back-to-back）VRF）——此情况与上述情况相同，然而，所发现的 PE（ASBR）将都在相同 AS 的边缘处。
3. Inter-AS（ASBR 上的 VPNv4，ASBR 上的下一跳自身（next-hop-self））——到相同 AS 的边缘上的每个 ASBR 的 LSP 将被发现。
4. Inter-AS（ASBR 上的 VPNv4，无下一跳自身）——到穿过 AS 边界的每一 ASBR 的 LSP 将被发现。
5. Inter-AS（Ipv4+ASBR 上的标签）——到其他 AS 中的每个 PE 的 LSP 将被发现。
6. Inter-AS（非 VPN MPLS 转变提供商）——虽然需要 LSP ping 来推动两个标签从而将消息转发到远程 PE，但是此情况与第五种情况相同。
7. CsC（较低层（tier）中的 IP 或 MPLS）——在承载支持承载（carrier supporting carrier）的情况下，LSP 发现将仅应用于核心 ISP 内，因为较低层提供商不使用 VRF。此情况应与第一种情况相同。

## 8. CsC（分层 VPN）——LSP 发现将仅发现到相同层中正使用的所有 PE 的 LSP。

现参考图 1，网络拓扑 10 的具体实施方式被示出。网络拓扑 10 包含三个 VPN：VPN1、VPN2 和 VPN3。VPN1、VPN2 和 VPN3 的一个端点可与 PE12 通信。PE12 是因特网服务提供商（ISP）20 的一部分，所述 ISP 20 还包含 PE22 和 PE24。在 ISP 20 内，在 PE 12 和 PE 22 之间的是提供商（P）路由器 26 和 28。类似地，在 PE 12 和 PE 24 之间的是 P 路由器 30 和 32。因此，VPN1 从路由器 14 延伸到 PE 12、到 P 28、到 P 26、到 PE 22，到路由器 34。VPN2 从路由器 16 延伸到 PE 12、到 P 32、到 P 30、到 PE 24，到路由器 36。VPN3 从路由器 18 延伸到 PE 12、到 P 32、到 P 30、到 PE 24，到路由器 38。

从 PE 12 的角度，经由 BGP 下一跳 PE 22 和 PE 24 可远程到达这些 VPN。当在 PE 12 上运行 LSP 发现时，基于局部 VRF 路由表，可产生数据库。在此示例中，数据库包含两个下一跳条目：一个用于 PE 22，一个用于 PE 24。PE 22 被 VPN1 使用并且 PE 24 被 VPN2 和 VPN3 使用。

针对每下一跳，路由表 ID 被维护，以区分哪些下一跳被包含在哪些 VRF 中。注意，多个 VPN 可能可以使用相同的下一跳。对于每个下一跳条目，设置了全局路由表中 BGP 下一跳的 IPv4 前缀，从而利用 LSP ping 的 IPv4 前缀 FEC 可对其进行 ping。这对 IPv6、流量工程以及 BGP 对等端之间的任何其他连接也是适用的。

图 2 示出了 Inter-AS VPN 部署情况的框图。现参考图 2，拓扑 50 的具体实施方式被示出，其中用于单个 AS 配置的 LSP 发现可以不找到在不同 AS 中的 PE。在拓扑 50 中，第一 VPN 54 与 PE 52 通信。PE 52 是第一 ISP 70 的一部分。第一 ISP 70 包含 PE 60 和 PE 62。第二 IPS 网络 72 与第一 ISP 70 通信。第二 ISP 72 包含 ASBR 58，所述 ASBR 58 与第一 ISP 70 的 ASBR 56 通信。ASBR 58 还与 PE 64、PE 66 及 PE 68 通信。PE 66 也与作为第一 VPN 的一部分的路由器 74 通信。在此 Inter-AS VPN 的情况下，发现了作为用于 PE 52 的 BGP 下一跳的路由器 ASBR 56。PE 52 无法确定越过 ASBR 56 的拓扑。在此示例中，存在隐藏在 ASBR 58 之后的其他 AS 中

的其他 PE 路由器（PE 64、PE 66 及 PE 68）。在此环境中，在 PE 52 上运行的 LSP 发现处理将发现 PE 60、ASBR 56 及 PE 62。

对于 Inter-AS 配置，发现 VRF 正在使用的每个 LSP 的进一步处理被执行。此方法是端到端的方案，并且发现了所有的 PE 和 ASBR，即使是在更复杂的 VPN 拓扑中。缺点是存在过多的需要被验证的 LSP。事实上，必需发现 VRF 路由表中的每一个前缀，从而保证所有的 PE 被验证。

现参考图 3，LSP 发现系统 100 的具体实施方式被示出。系统 100 包含 LSP 发现数据库 102，所述数据库 102 与 VRF 路由表（也称作路由信息表（RIB））104、106 及 108 交互，以收集全部的使用中的唯一 BGP 下一跳。LSP 发现的客户端 112、114 和 116 可经由 API 调用数据库 102 来获取这些信息。

LSP 发现数据库 102 存储已经从路由信息表 104、106 及 108 内的路由前缀发现的所有下一跳。来自多个路由信息表的路由前缀可能共享数据库中相同的下一跳条目。通过对路由表的扫描以及通过来自处理 110 的路由更新，来保持数据库最新。客户端 112、114 和 116 通过 API 在该表中执行查找。经由登记（registry）调用来通知客户端 112、114 和 116 关于数据库的变化。

路由表 104、106 和 108 将用于每个 VPN 的路由与下一跳信息一起存储。扫描这些表以找到要被放入数据库的下一跳。边界网关协议（Border Gateway Protocol, BGP）是将来自网络的路由信息分发到路由信息表 104、106 及 108 的路由处理的示例。

LSP 发现系统对所发生的不同类型的事件执行某些操作。初始时，LSP 发现数据库被起。VFR 和全局路由表被扫描以填充（populate）LSP 发现数据库。路由表刷新请求被使用于保持数据库最新。当路由表刷新请求被提供时，路由表被扫描。数据库中的条目被添加或被标记为已刷新。任何没有被刷新的条目被去除。将添加或去除通知给客户端。利用下一跳的 VPN 前缀的数目被计数，并且如果计数变到零则下一跳被去除。

初始化之后，客户端可在任何时间执行对数据库的查阅。当设法发现使用中的所有 LSP 时，负载分享可能被考虑。任一具体的 LSP 可在被分割

到不同方向。所获得的信息可被提供给其他用于找到负载分享路径的工具。

图 4A 和图 4B 中描述了当前所公开的方法的流程图。矩形元素在此表示“处理框”，并表示计算机软件指令或指令组。菱形元素在此表示“判断框”，并表示影响由处理框所表示的计算机软件指令的执行的计算机软件指令或指令组。

或者，处理框及判断框表示由诸如数字信号处理器电路或专用集成电路（ASIC）之类的功能上等价的电路所执行的步骤。流程图并不描述任何具体编程语言的语法。更确切的，流程图示出本领域普通技术人员用以制造电路或生成计算机软件从而执行本发明所需的处理而需要功能信息。应注意，许多诸如循环和变量的初始化以及临时变量的使用之类的例行程序元素没有被示出。本领域的普通技术人员应理解除非在此另外指出，所描述的步骤的具体顺序仅是说明性的，且可将其改变，只要不背离本发明的精神。因此，除非另外陈述，以下描述的步骤是无序的，即，当可能的时候可以任何便利或期望的顺序来执行所述步骤。

参考图 4A 和图 4B，示出了一种基于网络的 VPN 200 的服务级别测试点的库的产生和维护方法的具体实施方式。方法从判断框 202 开始，其中确定在用于至少一个感兴趣的 VPN 的网络中，是否存在不止一个自治系统（Autonomous System, AS）。当不存在多于一个 AS 时，根据处理框 204 进行处理。当存在不止一个 AS 时，根据处理框 224 继续处理。

在处理框 204 中，当判断框中的判断为不存在多于一个用于感兴趣的 VPN 的 AS 时，用于至少一个感兴趣的 VPN 的下一跳被找到。

在处理框 206 中，与至少一个感兴趣的 VPN 相关的 VPN 前缀被找到。如处理框 208 所示，与感兴趣的 VPN 相关联的标签栈的外部 IGP 标签可到达的下一跳被找到。在处理框 210 中，标签栈的前缀被发现。

在处理框 212 处，处理继续，其中从下一跳及 VPN 前缀中，确定用于至少一个感兴趣的 VPN 的使用中的标签交换路径（LSP）组。如处理框 214 中所示，可过滤 LSP 组以去除不期望的路径。这样做可减少被发现的 PE 路由器和相关 LSP 的数目。在处理框 216 中，LSP 组可被删减以去除

不活动 (inactive) 的路径。已经被拿掉或相反的账户不再被使用。在处理框 218 中, 删减还包含从 LSP 组中去除重复的路径。处理框 220 公开了通过处理路由更新信息, 来保持 LSP 组最新。可将更新作为路由处理的一部分动态地发生。或者, 如处理框 222 所示, 可在预定的时间执行路由更新。

在处理框 224 中, 当判断框中的判断是存在不止一个用于感兴趣的 VPN 的 AS 时, 在与至少一个感兴趣的 VPN 相关的当前 AS 中的路由器被找到。

在处理框 226 中, 与至少一个感兴趣的 VPN 相关的所有提供商边缘 (PE) 路由器和/或自洽系统边界路由器 (ASBR) 被找到。如处理框 228 所示, 与 PE 路由器相关的虚拟路由和转发 (VRF) 表正在使用的所有 LSP 被找到。

如处理框 230 所示, 从路由器以及 VPN 标签栈中确定用于至少一个感兴趣的 VPN 的使用中的 LSP 组。如处理框 232 所示, 可过滤 LSP 组以去除不期望的路径。这样做可减少被发现的 PE 路由器和相关 LSP 的数目。在处理框 234 中, LSP 组可被删减从而去除不活动的路径。已经被拿掉或相反的账户不再被使用。在处理框 236 中, 删减还包含从 LSP 组中去除重复的路径。处理框 220 公开了通过处理路由更新信息, 来保持 LSP 组最新。可将更新作为路由处理的一部分动态地发生。或者, 如处理框 240 所示, 可在预定的时间执行路由更新。

在处理框 242 中, 在完成处理框 222 或处理框 240 之后, 所得到的 LSP 组可被使得能用于其他处理。以这样的方式, 执行发现处理, 以识别可用于其他处理的用于 VPN 的 LSP 组。

已经描述了本发明的优选实施方式, 现在本领域普通技术人员将了解并入这些概念的其他实施方式也可被采用。此外, 作为本发明的一部分而被包含的软件可在包含计算机可用介质的计算机程序产品中被实施。例如, 这样的计算机可用介质可包含其上存储了计算机可读程序代码区段的可读存储器设备, 例如硬盘驱动设备、CD-ROM、DVD-ROM, 或计算机磁盘。计算机可读介质还可包含其上具有作为数字或模拟信号的程式代码



---

区段的光通信链接、有线通信链接或无线通信链接。因此，主张本发明不应局限于所描述的实施方式，而仅应该由随附权利要求的精神和范围来限定本发明。

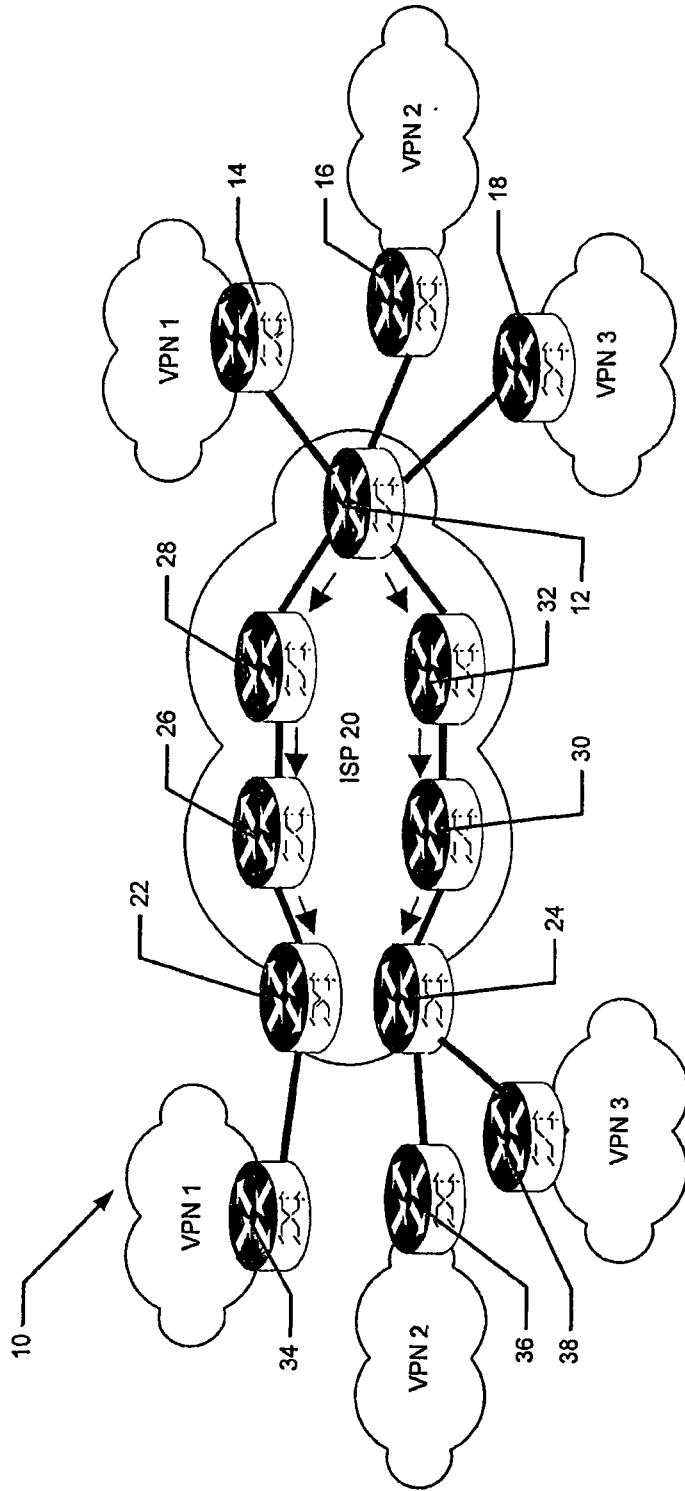


图1

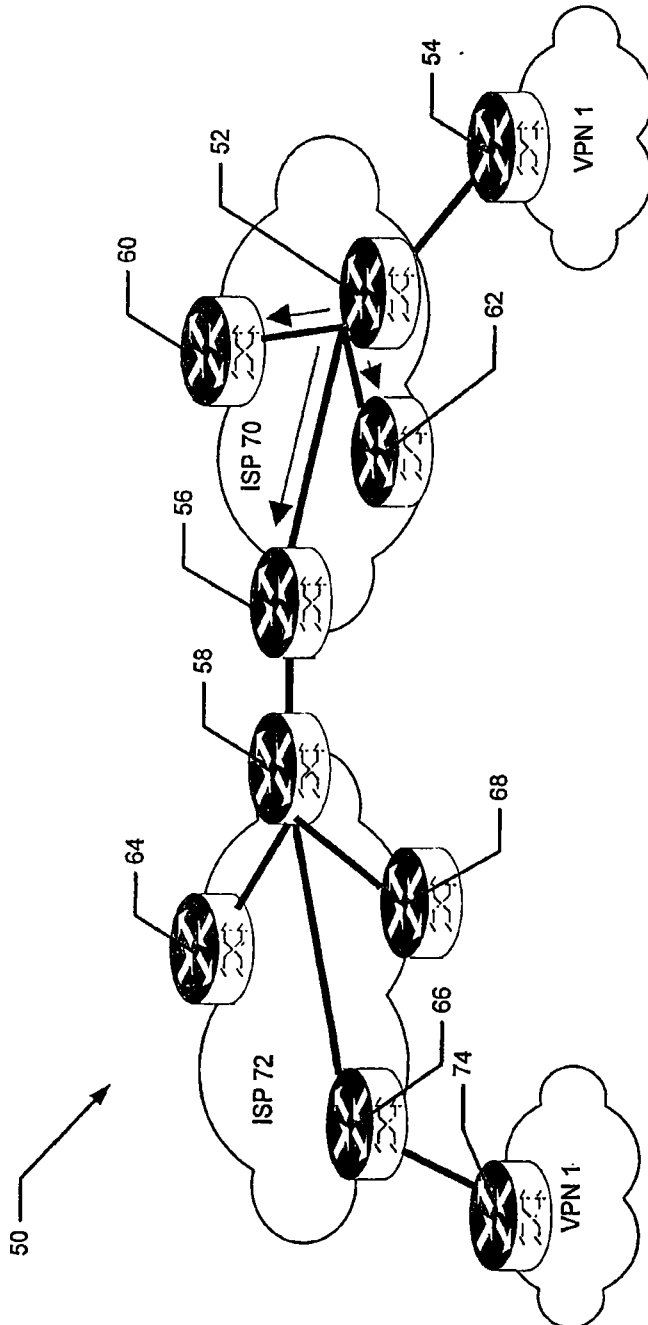


图2

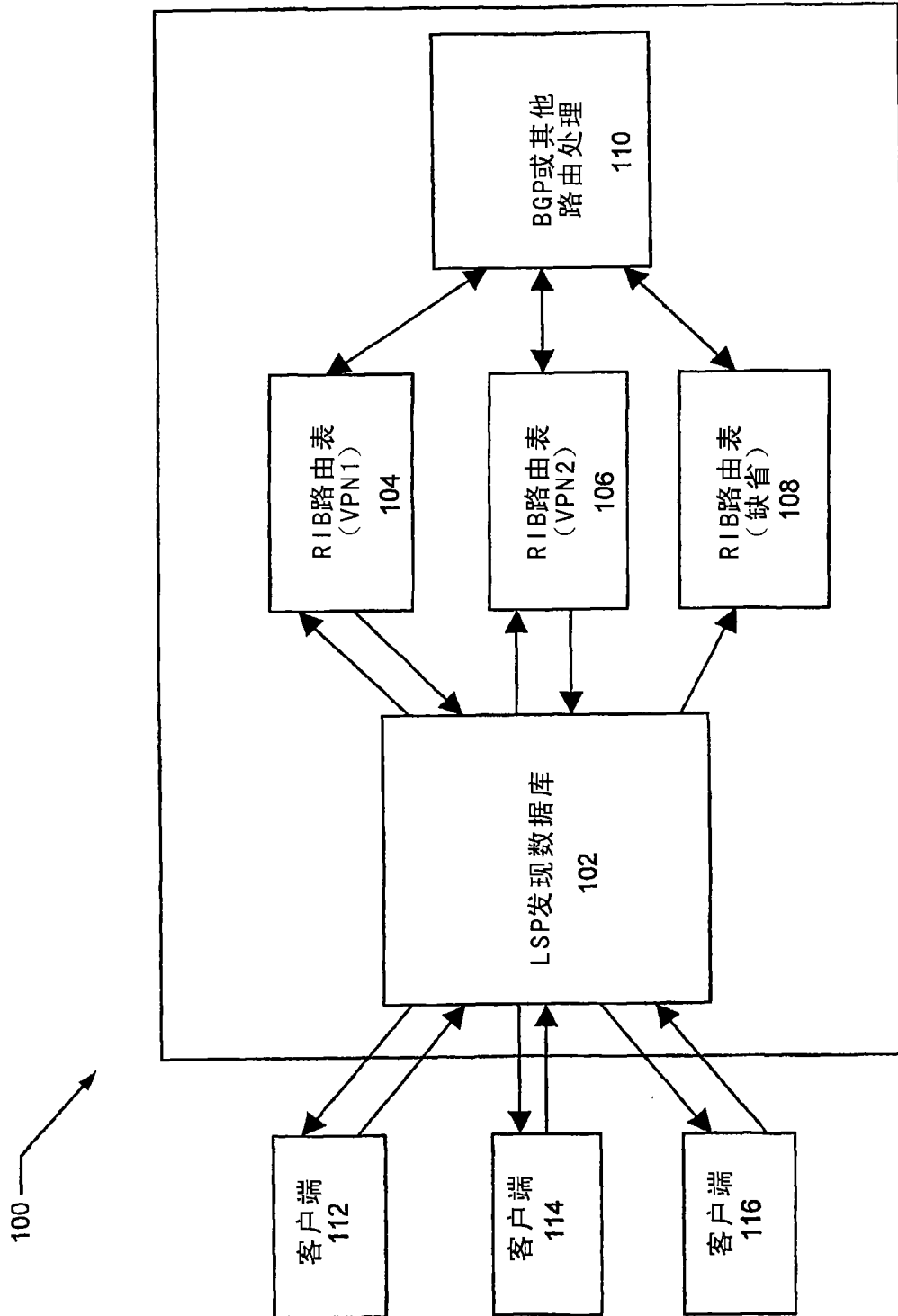


图3

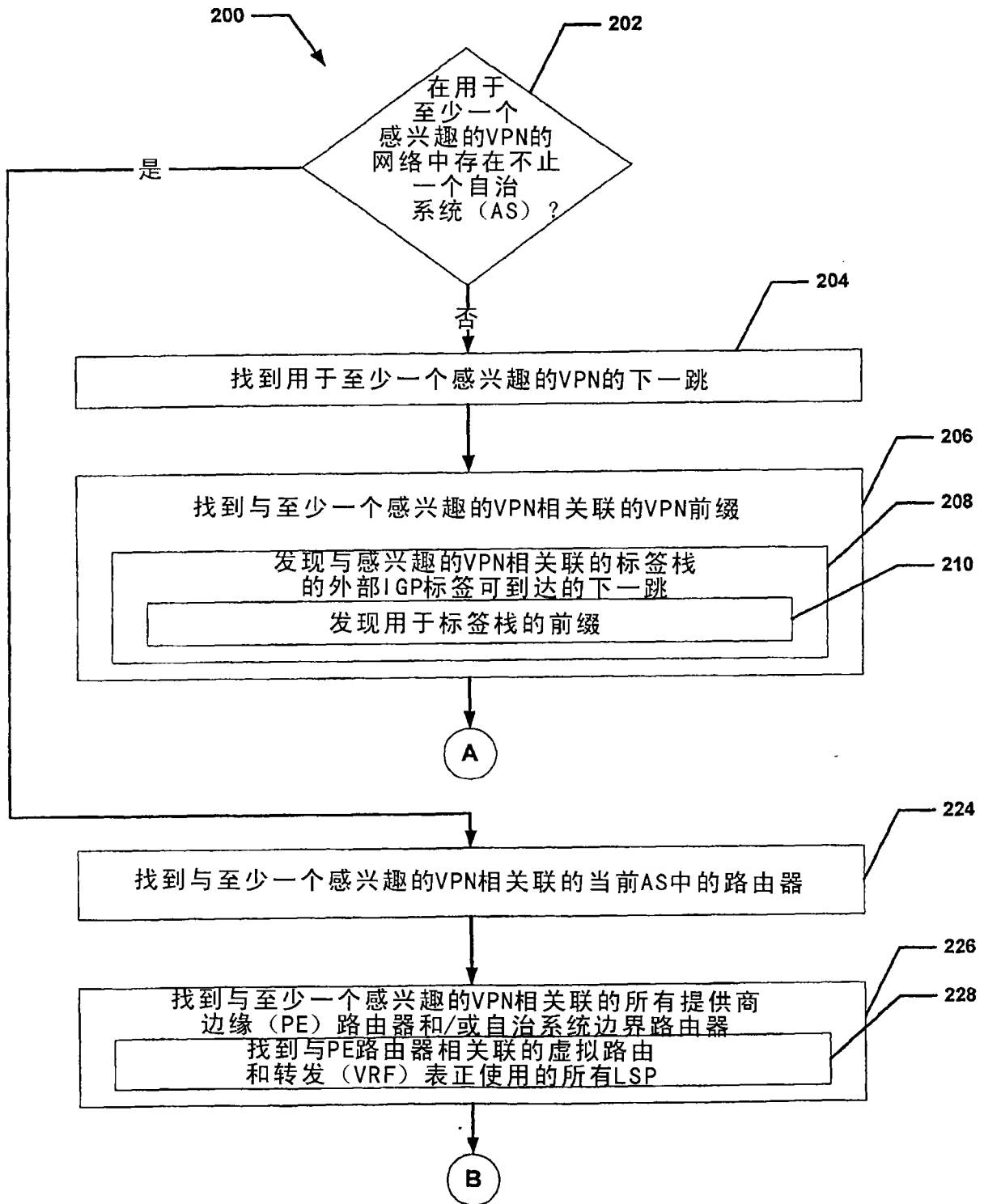


图4A

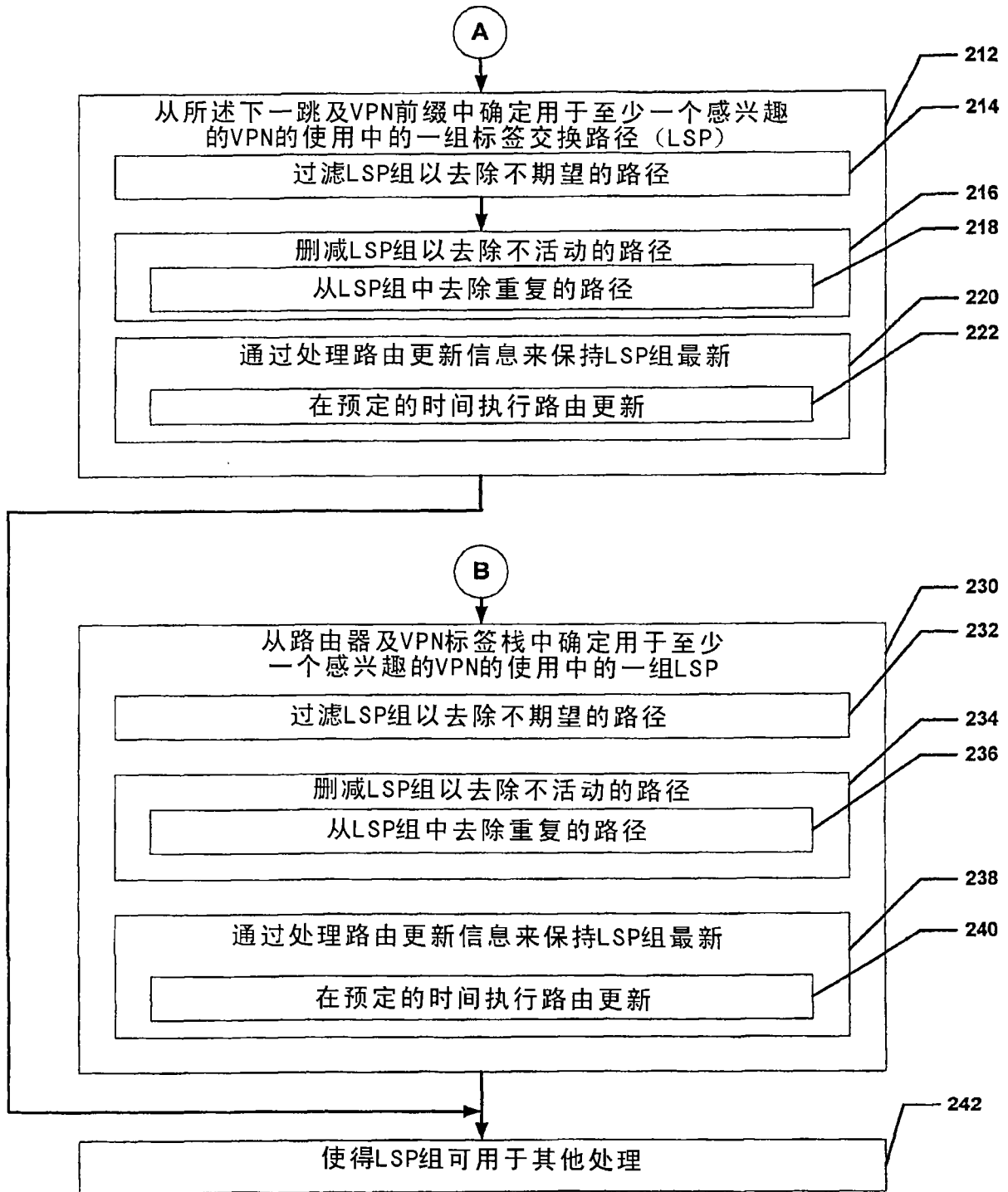


图4B