

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017年9月28日 (28.09.2017)



(10) 国际公布号
WO 2017/162095 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2017/076960
- (22) 国际申请日: 2017年3月16日 (16.03.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610160664.3 2016年3月21日 (21.03.2016) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 李振斌 (LI, Zhenbin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 庄顺万 (ZHUANG, Shunwan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陈霞 (CHEN, Xia); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 吴楠 (WU, Nan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 梁

乾灯 (LIANG, Qiandeng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(54) Title: COMMUNICATION METHOD, DEVICE AND SYSTEM BASED ON FLOW SPECIFICATION PROTOCOL

(54) 发明名称: 基于流规则协议的通信方法、设备和系统

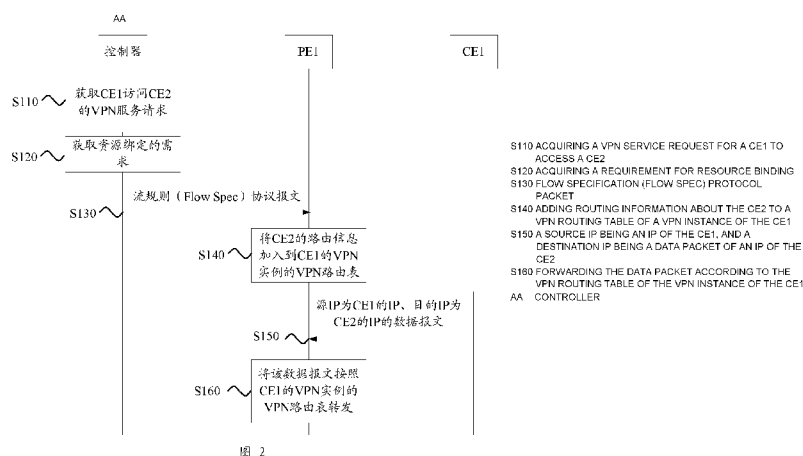


图 2

(57) Abstract: Provided are a communication method, device and system based on a flow specification protocol. The method comprises: a controller acquiring a requirement that a first resource on a forwarding device needs to be associated with a second resource on the forwarding device; and the controller sending a border gateway protocol flow specification (BGP Flow Spec) protocol packet to the forwarding device according to the requirement, the BGP Flow Spec protocol packet comprising a network layer accessibility information field and an expansion group attribute field, the network layer accessibility information field carrying feature information about the first resource, the expansion group attribute field carrying a global identifier (GID) for indicating the second resource, and the BGP Flow Spec protocol packet being used for indicating the association of the first resource and the second resource. The embodiments of the present invention can effectively avoid the unlimited expansion of a BGP Flow Spec protocol.

(57) 摘要:

[见续页]



WO 2017/162095 A1



本发明实施例提供一种基于流规则的通信方法、设备和系统，该方法包括：控制器获取转发设备上的第一资源需要关联该转发设备上的第二资源的需求；该控制器根据该需求，向该转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，该网络层可达性信息字段携带第一资源的特征信息，该扩展团体属性字段携带用于指示该第二资源的全局标识 GID，该 BGP Flow Spec 协议报文用于指示关联该第一资源与该第二资源。本发明实施例能够有效避免无限限制地扩展 BGP Flow Spec 协议。

基于流规则协议的通信方法、设备和系统

本申请要求于 2016 年 3 月 21 日提交中国专利局、申请号为 CN 201610160664.3、发明名称为“基于流规则协议的通信方法、设备和系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明实施例涉及通信领域，并且更具体地，涉及一种基于流规则 Flow Spec 协议的通信方法、设备和系统。

10 背景技术

边界网关协议 (Border Gateway Protocol, BGP), 是一种用于自治系统 (Autonomous System, AS) 之间的动态路由协议, 早期发布的三个版本分别是 BGP-1 (RFC1105)、BGP-2 (RFC1163) 和 BGP-3 (RFC1267), 主要用于交换 AS 之间的可达性路由信息, 构建 AS 域间的传播路径, 防止路由环路的生产, 并在 AS 级别应用一些路由策略。当前使用的版本是 BGP-4 (RFC4271)。BGP 作为事实上的互联网 (Internet) 外部路由协议标准, 被广泛应用于互联网服务提供商 (Internet Service Provider, ISP) 之间。

BGP 流规则 (Flow Specification, Flow Spec) (RFC 5575), 表示通过传递 BGP Flow Specification 路由将流量策略传递给 BGP Flow Specification 对等体 (传递 BGP Flow Specification 路由的对端设备互为对方的对等体), BGP Flow Specification 对等体收到 BGP Flow Specification 路由后, 将该 BGP Flow Specification 路由对应的优选的路由转换为转发平面的流量控制策略, 进而进行流量控制。其中, BGP Flow Specification 路由为 RFC5575 中定义的一种 BGP 路由, 这种 BGP Flow Specification 路由包含 BGP 网络层可达信息类型 (BGP Flow Spec NLRI) 和扩展团体属性。通过网络层可达信息和扩展团体属性, BGP Flow Specification 路由可以携带流量的匹配条件和流量匹配后执行的动作。RFC 5575 定义了 12 种常用的流量匹配规则: 目的地址、源地址、IP 协议号、端口号、目的端口号、源端口号、ICMP 类型、ICMP 编码、TCP 的标志位、DSCP、分片类型等, 这 12 种流量匹配规则封装在 BGP Flow Specification 路由中, 作为网络层可达信息传递。RFC 5575 定义了 4 种常用的流量处理行为: 丢弃流量、流量限速、修改报文的 DSCP 值、重定向动作 (redirect Actions), 这 4 种流量处理行为封装在 BGP Flow Spec 路由中, 作为扩展团体属性携带, 其中, redirect Actions 指的是引导特定数据流进入相应的转发通道。

目前, BGP Flow Spec 协议支持的重定向动作 (redirect Actions) 已经有下面六种: 重定向到 2 字节 AS 号形式的路由目标标识的虚拟专用网 VPN 路由转发表 (Virtual Routing Forwarding, VRF) (redirect AS-2byte); 重定向到 IPv4 地址形式的路由目标标识的 VRF (redirect IPv4 format); 重定向到 4 字节 AS 号形式的路由目标标识的 VRF (redirect AS-4byte); 重定向到 IPv6 地址形式的路由目标标识的 VRF (redirect IPv6 specific AS); 重定向到 IPv4 下一跳 (redirect IPv4 address); 重定向到 IPv6 下一跳 (redirect IPv6 address)。

利用传统方式扩展相关应用, 例如, 重定向到 VRF/IP/隧道 (Tunnel), 每增加一个新

业务需求,就要给 BGP Flow Spec 协议打个补丁,使 BGP FlowSpec 协议始终处于变化状态。例如,目前研究的 BGP Flow Spec Redirect Actions 方案为,定义一种通用的 Path-ID,用于引导数据流进入该 Path-ID 所对应的传输层隧道,就要在 BGP Flow Spec 协议的扩展团体属性中携带该 Path-ID,必要时还要携带隧道的具体信息。

5 因此,沿用传统方式扩展相关应用,会导致无限制地扩展 BGP FlowSpec 协议。

发明内容

10 本发明实施例提供一种基于流规则 Flow Spec 协议的通信方法和设备,能够有效避免 Flow Spec 协议的无限制扩展。

第一方面提供了一种基于流规则 Flow Spec 协议的通信方法,包括:

控制器获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求;

15 所述控制器根据所述需求,向所述转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文,所述 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段,所述网络层可达性信息字段携带第一资源的特征信息,所述扩展团体属性字段携带用于指示所述第二资源的全局标识 GID,所述 BGP Flow Spec 协议报文用于指示关联所述第一资源与第二资源。

应理解,第一资源的特征信息能够指示所述第一资源。

20 在本申请中,所述转发设备的第一资源与第二资源均指存储在所述转发设备上的用于转发数据报文(数据流)的信息。通过关联所述第一资源与第二资源,能够引导数据报文进入相应的转发通道。例如所述第一资源指示所述转发设备上存储的第一节点的路由信息,第二资源指示所述转发设备上存储的第二节点的路由表,则关联所述第一资源与第二资源指的是,将所述第一节点的路由信息加入到所述第二节点的路由表中,这样,就能够引导来源于所述第二节点的数据报文进入所述第一节点的转发通道。再例如,所述
25 第一资源指示源 IP 地址为第一节点的 IP 地址,目的 IP 地址为第二节点的 IP 地址,其中,所述第一节点的 IP 地址以及所述第二节点的 IP 地址均存储在所述转发设备上,所述第二资源指示所述转发设备上存储的所述第二节点的路由表(转发表),则关联所述第一资源与第二资源指的是,将源 IP 地址与目的 IP 地址与所述第一资源相一致的数据报文,按照所述第二节点的路由表进行转发,这样,也能够引导来源于所述第一节点的数据报文
30 进入所述第二节点的转发通道。

因此,本申请中,通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息,扩展团体属性字段中携带用于指示第二资源的全局标识 GID,能够指示转发设备关联所述第一资源与第二资源,以引导数据流进入相应的转发通道。如上一段所述,BGP Flow Spec 协议报文中携带的所述第一资源与第二资源可以是不同的资源组合,从而通过本申请的 BGP Flow Spec 协议报文,可以实现多种业务需求。传统技术
35 中每扩展一个新的业务需求就需要给 BGP FlowSpec 协议打个补丁,即需要扩展 BGP FlowSpec 协议中的扩展团体属性,导致 BGP FlowSpec 协议始终处于变化状态。相对于传统技术,本申请中的 BGP FlowSpec 协议通过统一的报文格式,可以满足多种业务需求,从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。

在本申请中，所述扩展团体属性中携带的所述 GID 用于在所述转发设备中唯一指示所述第二资源。例如，所述控制器与所述转发设备上存储有映射表，该映射表包括所述第二资源与所述 GID 之间的映射关系，因此，通过所述 GID，所述控制器与所述转发设备都能够定位到所述第二资源。因此，在本申请中，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所述第二资源，这样能够节省信令开销。

结合第一方面，在第一方面的第一种可能的实现方式中，所述通信方法还包括：

所述控制器获取所述转发设备上存储的资源，所述资源包括所述第二资源；

所述控制器为所述转发设备上存储的资源分配映射标识；

所述控制器向所述转发设备发送映射表，所述映射表包括所述转发设备上存储的资源与所分配的映射标识之间的映射关系，

其中，所述 GID 为所述控制器为所述第二资源分配的映射标识。

在本申请中，控制器通过搜集转发设备上存储的资源，并为其分配映射标识，然后将资源与映射标识之间的映射关系告知给所述转发设备，使得控制器与转发设备通过在通信信令中仅携带映射标识，就能定位到对应的资源，从而能够提供通信效率，同时也能够节省信令开销。

结合第一方面，在第一方面的第二种可能的实现方式中，所述扩展团体属性字段包括 GID 字段与标志 Flags 字段，所述 GID 字段携带所述 GID，所述 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联所述第一资源与所述第二资源的信息。

传统技术中，扩展的应用通常仅局限在转发平面引导数据流进入相应的转发通道。在本申请中，不仅可以在转发平面引导数据流进入相应的转发通道，也可以在控制平面引导数据流进入相应的转发通道，从而本申请能够实现灵活地业务编排。

结合第一方面的第二种可能的实现方式，在第一方面的第三种可能的实现方式中，所述 Flags 字段包括转发平面比特位与控制平面比特位，当所述转发平面比特位赋值为 0、且所述控制平面比特位赋值为 1 时，用于指示在所述控制平面上关联所述第一资源与所述第二资源，当所述转发平面比特位赋值为 1、且所述控制平面比特位赋值为 0 时，用于指示在所述转发平面上关联所述第一资源与所述第二资源。

应理解，在上述第一方面的第三种可能的实现方式中，所述 Flags 字段中的转发平面比特位与控制平面比特位，也可以用第一比特位替换，当该第一比特位赋值为 1 时，表示在所述控制平面上关联所述第一资源与所述第二资源，当该第一比特位赋值为 0 时，表示在所述转发平面上关联所述第一资源与所述第二资源。

结合第一方面的第三种可能的实现方式，在第一方面的第四种可能的实现方式中，所述 Flags 字段还包括增量比特位，当所述增量比特位赋值为 1 时，表示在所述转发设备上增加一个资源关联关系，当所述增量比特位赋值为 0 时，表示利用所述第一资源与所述第二资源之间的关联关系覆盖所述第一资源原有的与其他资源之间的关联关系。

结合第一方面的第二种至第四种可能的实现方式中的任一种可能的实现方式，在第一方面的第五种可能的实现方式中，所述转发设备为服务商边缘 PE 设备，所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例，所述转发设备上包括第二 CE 设备的路由信息，且所述第二 CE 设备的路由信息不在所述第一 CE 设备的 VPN 实例的 VPN 路由表中，所述通信方法还包括：

所述控制器获取 VPN 服务请求, 所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备;

所述控制器获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求, 包括:

5 所述控制器根据所述 VPN 请求, 获取所述第一资源需要关联所述第二资源的需求, 所述第一资源为所述第二 CE 设备的路由信息, 所述第二资源为所述第一 CE 设备的 VPN 实例;

所述控制器根据所述需求, 向所述转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文, 包括:

10 所述控制器根据所述需求, 向所述转发设备发送所述 BGP Flow Spec 协议报文, 所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在控制平面上关联所述第一资源与所述第二资源, 所述 BGP Flow Spec 协议报文用于指示将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中。

在本申请中, 通过控制器向 PE 设备 (即转发设备) 下发 BGP Flow Spec 协议报文, 指示 PE 设备将 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由信息加入所述第一
15 CE 设备的路由表中, 从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道, 即实现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此, 相对于现有技术中的手工配置方式, 本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。此外, 相对于传统技术中局限于在转发平面引导数据流进入相应的转发通道, 本申请能够在控制平面引导数据流进入相应的转发通道, 从而能够实现灵活的业务
20 编排。

结合第一方面的第五种可能的实现方式, 在第一方面的第六种可能的实现方式中, 所述通信方法还包括:

所述控制器从所述转发设备上获取所述第一 CE 设备的 VPN 实例的属性信息, 所述属性信息包括: VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例
25 索引值和 VPN 实例接口信息;

所述控制器为所述第一 CE 设备的 VPN 实例的属性信息分配映射标识, 所述映射标识在所述转发设备中唯一指示所述第一 CE 设备的 VPN 实例的属性信息;

所述控制器向所述转发设备发送映射表, 所述映射表包括所述第一 CE 设备的 VPN 实例的属性信息与所述映射标识之间的映射关系,

30 所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

在本申请中, 控制器通过搜集 PE 设备上建立的 VPN 实例的属性信息, 并为其分配映射标识, 然后将 VPN 实例的属性信息与映射标识之间的映射关系告知给所述 PE 设备, 使得控制器与 PE 设备通过在 BGP Flow Spec 协议报文中仅携带映射标识, 就能定位到对应的 VPN 实例, 从而能够提供通信效率, 同时也能够节省信令开销。

35 结合第一方面的第六种可能的实现方式, 在第一方面的第七种可能的实现方式中, 所述通信方法还包括:

所述控制器获取用于请求为所述转发设备上新建立的第三 CE 设备的 VPN 实例配置属性信息的 VPN 服务请求;

所述控制器为所述第三 CE 设备的 VPN 实例配置如下属性信息: VPN 实例名称、VPN 实例 RD、VPN 实例 RT 和 VPN 实例接口信息, 其中, 所述第三 CE 设备的 VPN 实例的下列属性
40

信息与所述第一 CE 设备的 VPN 实例对应的属性信息互不冲突: VPN 实例名称、VPN 实例 RD、VPN 实例接口信息。

在本申请中, 控制器通过获取 PE 设备上已有的 VPN 实例的属性信息, 从而在为所述 PE 设备上增加的 VPN 实例配置属性信息时, 能够避免不同 VPN 实例的属性信息之间的冲突。

5 相比于现有技术中靠规划避免冲突, 本申请能够有效地避免冲突, 而且操作效率较高。

结合第一方面的第五种至第七种可能的实现方式中的任一种可能的实现方式, 在第一方面的第八种可能的实现方式中, 所述转发设备上建立有所述第二 CE 设备的 VPN 实例, 所述第二 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息;

10 所述第一资源的特征信息为所述第二 CE 设备的 VPN 实例的下列属性信息中的至少一种信息: VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID。

结合第一方面的第五种至第七种可能的实现方式中的任一种可能的实现方式, 在第一方面的第九种可能的实现方式中, 所述转发设备上没有建立所述第二 CE 设备的 VPN 实例, 所述转发设备的 VPN 公网路由表中包括所述第二 CE 设备的路由信息;

15 所述第一资源的特征信息为下列信息中的至少一种: 所述第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息。

结合第一方面的第二种至第四种可能的实现方式中的任一种可能的实现方式, 在第一方面的第十种可能的实现方式中, 所述转发设备为服务商边缘 PE 设备, 所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例, 所述转发设备上还包括第二 CE 设备的路由信息, 且所述第一 CE 设备的 VPN 实例的 VPN 路由表中不包括所述第二 CE 设备的路由信息, 所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息, 所述通信方法还包括:

所述控制器获取 VPN 服务请求, 所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备;

25 所述控制器获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求, 包括:

所述控制器根据所述 VPN 请求, 获取所述第一资源需要关联所述第二资源的需求, 所述第一资源为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址, 所述第二资源为所述第三 CE 设备的 VPN 实例;

所述控制器根据所述需求, 向所述转发设备发送 BGP Flow Spec 协议报文, 包括:

30 所述控制器根据所述需求, 向所述转发设备发送所述 BGP Flow Spec 协议报文, 所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在转发平面上关联所述第一资源与所述第二资源, 所述 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与所述第一资源相一致的数据报文, 按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息进行转发。

35 应理解, 在本实现方式中, 所述第一资源的特征信息为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址。

在本申请中, 通过控制器向 PE 设备 (即转发设备) 下发 BGP Flow Spec 协议报文, 指示 PE 设备针对源 IP 地址为第一 CE 设备的 IP 地址、且目的 IP 地址为第二 CE 设备的 IP 地址的数据报文, 按照 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由转发表进行转发, 从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道, 即实

现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此,相对于现有技术中的手工配置方式,本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。

结合第一方面的第十种可能的实现方式,在第一方面的第十一种可能的实现方式中,所述通信方法还包括:

所述控制器从所述转发设备上获取所述第三 CE 设备的 VPN 实例的属性信息,所述属性信息包括:VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息;

所述控制器为所述第三 CE 设备的 VPN 实例的属性信息分配映射标识,所述映射标识在所述转发设备中唯一指示所述第三 CE 设备的 VPN 实例的属性信息;

所述控制器向所述转发设备发送映射表,所述映射表包括所述第三 CE 设备的 VPN 实例的属性信息与所述映射标识之间的映射关系,

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

在本申请中,控制器通过搜集 PE 设备上建立的 VPN 实例的属性信息,并为其分配映射标识,然后将 VPN 实例的属性信息与映射标识之间的映射关系告知给所述 PE 设备,使得控制器与 PE 设备通过在 BGP Flow Spec 协议报文中仅携带映射标识,就能定位到对应的 VPN 实例,从而能够提供通信效率,同时也能够节省信令开销。

结合第一方面的第十一种可能的实现方式,在第一方面的第十二种可能的实现方式中,所述通信方法还包括:

所述控制器获取用于请求为所述转发设备上新建立的第四 CE 设备的 VPN 实例配置属性信息的 VPN 服务请求;

所述控制器为所述第四 CE 设备的 VPN 实例配置如下属性信息:VPN 实例名称、VPN 实例 RD、VPN 实例 RT 和 VPN 实例接口信息,其中,所述第四 CE 设备的 VPN 实例的下列属性信息与所述第一 CE 设备的 VPN 实例以及所述第三 CE 设备的 VPN 实例对应的属性信息互不冲突:VPN 实例名称、VPN 实例 RD、VPN 实例接口信息。

在本申请中,控制器通过获取 PE 设备上已有的 VPN 实例的属性信息,从而在为所述 PE 设备上增加的 VPN 实例配置属性信息时,能够避免不同 VPN 实例的属性信息之间的冲突。相比于现有技术中靠规划避免冲突,本申请能够有效地避免冲突,而且操作效率较高。

结合第一方面的第十种至第十二种可能的实现方式中的任何一种可能的实现方式,在第一方面的第十三种可能的实现方式中,所述第二 CE 设备为所述第三 CE 设备。

第二方面提供了一种基于流规则 Flow Spec 协议的通信方法,所述通信方法包括:

转发设备接收控制器发送的边界网关协议流规则 BGP Flow Spec 协议报文,所述 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段,所述网络层可达性信息字段携带用于指示所述转发设备上的第一资源的所述第一资源的特征信息,所述扩展团体属性字段携带用于指示所述转发设备上的第二资源的全局标识 GID,所述 BGP Flow Spec 协议报文用于指示关联所述第一资源与所述第二资源;

所述转发设备根据所述第一资源的特征信息,获取所述第一资源,根据所述 GID,获取所述第二资源;

所述转发设备关联所述第一资源与所述第二资源。

在本申请中,所述转发设备的第一资源与第二资源均指存储在所述转发设备上的用于

转发数据报文（数据流）的信息。通过关联所述第一资源与所述第二资源，能够引导数据报文进入相应的转发通道。例如所述第一资源指示所述转发设备上存储的第一节点的路由信息，第二资源指示所述转发设备上存储的第二节点的路由表，则关联所述第一资源与所述第二资源指的是，将所述第一节点的路由信息加入到所述第二节点的路由表中，这样，
5 就能够引导来源于所述第二节点的数据报文进入所述第一节点的转发通道。再例如，所述第一资源指示源 IP 地址为第一节点的 IP 地址，目的 IP 地址为第二节点的 IP 地址，其中，所述第一节点的 IP 地址以及所述第二节点的 IP 地址均存储在所述转发设备上，所述第二资源指示所述转发设备上存储的所述第二节点的路由表（转发表），则关联所述第一资源与
10 所述第二资源指的是，将源 IP 地址与目的 IP 地址与所述第一资源相一致的数据报文，按照所述第二节点的路由表进行转发，这样，也能够引导来源于所述第一节点的数据报文进入所述第二节点的转发通道。

因此，本申请中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通道。如上一
15 段所述，BGP Flow Spec 协议报文中携带的所述第一资源与所述第二资源可以是不同的资源组合，从而通过本申请的 BGP Flow Spec 协议报文，可以实现多种业务需求。传统技术中每扩展一个新的业务需求就需要给 BGP FlowSpec 协议打个补丁，即需要扩展 BGP FlowSpec 协议中的扩展团体属性，导致 BGP FlowSpec 协议始终处于变化状态。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，
20 从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。

在本申请中，所述扩展团体属性中携带的所述 GID 用于在所述转发设备中唯一指示所述第二资源。例如，所述控制器与所述转发设备上存储有映射表，该映射表包括所述第二资源与所述 GID 之间的映射关系，因此，通过所述 GID，所述控制器与所述转发设备都能够定位到所述第二资源。因此，在本申请中，通过在 BGP FlowSpec 协议报文的扩展团体
25 属性字段中携带简洁的 GID，就能够指示所述第二资源，这样能够节省信令开销。

结合第二方面，在第二方面的第一种可能的实现方式中，所述扩展团体属性字段包括 GID 字段与标志 Flags 字段，所述 GID 字段携带所述 GID，所述 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联所述第一资源与所述第二资源的信息。

传统技术中，扩展的应用通常仅局限在转发平面引导数据流进入相应的转发通道。在本申请中，不仅可以在转发平面引导数据流进入相应的转发通道，也可以在控制平面引导数据流进入相应的转发通道，从而本申请能够实现灵活地业务编排。

结合第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述 Flags 字段包括转发平面比特位与控制平面比特位，当所述转发平面比特位赋值为 0、
35 且所述控制平面比特位赋值为 1 时，用于指示在所述控制平面上关联所述第一资源与所述第二资源，当所述转发平面比特位赋值为 1、且所述控制平面比特位赋值为 0 时，用于指示在所述转发平面上关联所述第一资源与所述第二资源。

应理解，在上述实现方式中，所述 Flags 字段中的转发平面比特位与控制平面比特位，也可以用第一比特位替换，当该第一比特位赋值为 1 时，表示在所述控制平面上关联所述
40 第一资源与所述第二资源，当该第一比特位赋值为 0 时，表示在所述转发平面上关联所述

第一资源与所述第二资源。

结合第二方面的第一种或第二种可能的实现方式，在第二方面的第三种可能的实现方式中，所述转发设备为服务商边缘 PE 设备，所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例，所述转发设备上包括第二 CE 设备的路由信息，且所述第二 CE 设备的路由信息不在所述第一 CE 设备的 VPN 实例的 VPN 路由表中，所述转发设备接收所述控制器发送的 BGP Flow Spec 协议报文，包括：

所述转发设备接收所述控制器根据 VPN 服务请求发送的所述 BGP Flow Spec 协议报文，所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备，其中，所述第一资源为所述第二 CE 设备的路由信息，所述第二资源为所述第一 CE 设备的 VPN 实例，所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在控制平面上关联所述第一资源与所述第二资源，所述 BGP Flow Spec 协议报文用于指示将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中；

所述转发设备关联所述第一资源与所述第二资源，包括：

所述转发设备将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中。

在本申请中，PE 设备（即转发设备）通过接收控制器向下发的 BGP Flow Spec 协议报文，将 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由信息加入所述第一 CE 设备的路由表中，从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道，即实现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此，相对于现有技术中的手工配置方式，本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。此外，相对于传统技术中局限于在转发平面引导数据流进入相应的转发通道，本申请能够在控制平面引导数据流进入相应的转发通道，从而能够实现灵活的业务编排。

结合第二方面的第三种的实现方式，在第二方面的第四种可能的实现方式中，所述通信方法还包括：

所述转发设备向所述控制器发送所述第一 CE 设备的 VPN 实例的属性信息，所述属性信息包括：VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息；

所述转发设备接收所述控制器发送的映射表，所述映射表包括所述第一 CE 设备的 VPN 实例的属性信息与所述控制器为所述第一 CE 设备的 VPN 实例的属性信息分配的映射标识之间的映射关系，所述映射标识在所述转发设备中唯一指示所述第一 CE 设备的 VPN 实例的属性信息，

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

在本申请中，控制器通过搜集 PE 设备上建立的 VPN 实例的属性信息，并为其分配映射标识，然后将 VPN 实例的属性信息与映射标识之间的映射关系告知给所述 PE 设备，使得控制器与 PE 设备通过在 BGP Flow Spec 协议报文中仅携带映射标识，就能定位到对应的 VPN 实例，从而能够提供通信效率，同时也能够节省信令开销。

结合第二方面的第三种或第四种的实现方式，在第二方面的第五种可能的实现方式中，所述转发设备上建立有所述第二 CE 设备的 VPN 实例，所述第二 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息；

所述第一资源的特征信息为所述第二 CE 设备的 VPN 实例的下列属性信息中的至少一

种信息: VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID;
所述转发设备根据所述第一资源的特征信息, 获取所述第一资源, 包括:

所述转发设备根据所述第一资源的特征信息, 从所述第二 CE 设备的 VPN 实例的 VPN 路由表中获取所述第二 CE 设备的路由信息。

5 在上述实现方式中, 所述第一资源的特征信息为用于指示所述第二 CE 设备的 VPN 实例的 GID。

结合第二方面的第三种或第四种的实现方式, 在第二方面的第六种可能的实现方式中, 所述转发设备上没有建立所述第二 CE 设备的 VPN 实例, 所述转发设备的 VPN 公网路由表中包括所述第二 CE 设备的路由信息;

10 所述第一资源的特征信息为下列信息中的至少一种: 所述第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息;

所述转发设备根据所述第一资源的特征信息, 获取所述第一资源, 包括:

所述转发设备根据所述第一资源的特征信息, 从所述 VPN 公网路由表中获取所述第二 CE 设备的路由信息。

15 结合第二方面的第一种或第二种的实现方式, 在第二方面的第七种可能的实现方式中, 所述转发设备为服务商边缘 PE 设备, 所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例, 所述转发设备上还包括第二 CE 设备的路由信息, 且所述第一 CE 设备的 VPN 实例的 VPN 路由表中不包括所述第二 CE 设备的路由信息, 所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息, 所述
20 转发设备接收所述控制器发送的 BGP Flow Spec 协议报文, 包括:

所述转发设备接收所述控制器根据 VPN 服务请求发送的 BGP Flow Spec 协议报文, 所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备, 其中, 所述第一资源为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址, 所述第二资源为所述第三 CE 设备的 VPN 实例, 所述 BGP Flow Spec 协议报文中的所述 Flags
25 字段用于指示在转发平面上关联所述第一资源与所述第二资源, 所述 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与所述第一资源相一致的数据报文, 按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息进行转发;

所述转发设备关联所述第一资源与所述第二资源, 包括:

30 所述转发设备接收数据报文, 所述数据报文的源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址;

所述转发设备按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息转发所述数据报文。

应理解, 在本实现方式中, 所述第一资源的特征信息为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址。

35 在本申请中, PE 设备 (即转发设备) 通过接收控制器向下发的 BGP Flow Spec 协议报文, 针对源 IP 地址为第一 CE 设备的 IP 地址、且目的 IP 地址为第二 CE 设备的 IP 地址的数据报文, 按照 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由转发表进行转发, 从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道, 即实现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此, 相对于现有技术中的手工配置方式,
40 本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。

结合第二方面的第七种的实现方式，在第二方面的第八种可能的实现方式中，所述通信方法还包括：

所述转发设备向所述控制器发送所述第三 CE 设备的 VPN 实例的属性信息，所述属性信息包括：VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息；

所述转发设备接收所述控制器发送的映射表，所述映射表包括所述第三 CE 设备的 VPN 实例的属性信息与所述控制器为所述第三 CE 设备的 VPN 实例的属性信息分配的映射标识之间的映射关系，所述映射标识在所述转发设备中唯一指示所述第三 CE 设备的 VPN 实例的属性信息，

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

在本申请中，控制器通过搜集 PE 设备上建立的 VPN 实例的属性信息，并为其分配映射标识，然后将 VPN 实例的属性信息与映射标识之间的映射关系告知给所述 PE 设备，使得控制器与 PE 设备通过在 BGP Flow Spec 协议报文中仅携带映射标识，就能定位到对应的 VPN 实例，从而能够提供通信效率，同时也能够节省信令开销。

结合第二方面的第七种或第八种的实现方式，在第二方面的第九种可能的实现方式中，所述第二 CE 设备为所述第三 CE 设备。

在上述某些实现方式中，所述控制器为所述第一 CE 设备的 VPN 实例的属性信息分配映射标识，所述控制器可以为所述第一 CE 设备的 VPN 实例的各个属性信息（VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息）分别分配映射标识，也可以为所述第一 CE 设备的 VPN 实例的各个属性信息统一分配一个映射标识，只要能够使得控制器和 PE 设备通过映射标识定位到所述第一 CE 设备的 VPN 实例即可。

第三方面提供了一种控制器，该控制器用于执行上述第一方面或第一方面的任一可能的实现方式中的方法。

具体地，该控制器可以包括用于执行第一方面或第一方面的任一可能的实现方式中的方法的模块。

第四方面提供了一种转发设备，该转发设备用于执行上述第二方面或第二方面的任一可能的实现方式中的方法。

具体地，该转发设备可以包括用于执行第二方面或第二方面的任一可能的实现方式中的方法的模块。

第五方面提供了一种控制器，该控制器包括存储器和处理器，该存储器用于存储指令，该处理器用于执行该存储器存储的指令，并且对该存储器中存储的指令的执行使得该处理器执行第一方面或第一方面的任一可能的实现方式中的方法。

第六方面提供了一种转发设备，该转发设备包括存储器和处理器，该存储器用于存储指令，该处理器用于执行该存储器存储的指令，并且对该存储器中存储的指令的执行使得该处理器执行第二方面或第二方面的任一可能的实现方式中的方法。

第七方面提供了一种基于流规则 Flow Spec 的通信系统，所述通信系统包括控制器和转发设备，所述控制器如上述第三方面提供的控制器，所述转发设备如上述第四方面提供的转发设备。

在上述某些实现方式中，所述第一 CE 设备的 VPN 实例指的是 PE 设备上建立的能够与

所述第一 CE 设备保持联系的 VPN 实例。

在上述某些实现方式中，所述第二 CE 设备的路由信息的出口目标 Export Target 属性与所述第一 CE 设备的 VPN 实例的入口目标 Import Target 属性不匹配。

在上述某些实现方式中，所述第二 CE 设备的路由信息指示所述第二 CE 设备的 IPv4 地址信息或者 IPv6 地址信息。

因此，本申请中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通道。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所述第二资源，能够节省信令开销。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例或现有技术描述中需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 示出了本发明实施例的一个应用场景的示意图。

图 2 示出了根据本发明实施例提供的基于流规则 Flow Spec 的通信方法的示意性流程图。

图 3 示出了根据本发明实施例提供的扩展团体属性的格式的示意图。

图 4 示出了根据本发明实施例提供的基于流规则 Flow Spec 的通信方法的另一示意性流程图。

图 5 示出了根据本发明实施例提供的基于流规则 Flow Spec 的通信方法的示意图。

图 6 示出了根据本发明实施例提供的控制器的示意性框图。

图 7 示出了根据本发明实施例提供的转发设备的示意性框图。

图 8 示出了根据本发明实施例提供的控制器的另一示意性框图。

图 9 示出了根据本发明实施例提供的转发设备的另一示意性框图。

图 10 示出了根据本发明实施例提供的基于流规则 Flow Spec 的通信系统的示意性框图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

为了方便理解本发明实施例，首先在此介绍本发明实施例描述中会引入的几个概念。

多协议标签交换 (Multi-Protocol Label Switching, MPLS)，是新一代的 IP 高速骨

干网络交换标准，MPLS 是利用标签 (Label) 进行数据转发的。当分组进入网络时，为其分配固定长度的短的标签，并将标签与分组封装在一起转发，在整个转发过程中，交换节点仅根据标签进行转发。MPLS 在无连接的 IP 网络中增加了面向连接的控制平面，为 IP 网络增添了管理和运营的手段。

5 控制平面，指系统中用来传送指令、计算表项的部分，例如协议报文转发、协议表项计算、维护等都属于控制平面的范畴。再例如，在路由系统中，负责管理路由协议运行、路由学习、路由表项维护的进程就属于控制平面。

转发平面，指系统中用来进行数据报文的封装、转发的部分。例如数据报文的接收、解封、封装、转发等都属于转发平面的范畴。再例如，系统接收到 IP 报文后，负责对 IP 报文进行解封、根据 IP 报文查找路由表、从出接口将 IP 报文转发出去等行为的进程就属于转发平面。

BGP 流规则 (Flow Specification, Flow Spec) (RFC 5575)，表示通过传递 BGP Flow Specification 路由将流量策略传递给 BGP Flow Specification 对等体 (传递 BGP Flow Specification 路由的对端设备互为对方的对等体)，BGP Flow Specification 对等体收到 BGP Flow Specification 路由后，将该 BGP Flow Specification 路由对应的优选的路由转换为转发平面的流量控制策略，进而进行流量控制。其中，BGP Flow Specification 路由为 RFC5575 中定义的一种 BGP 路由，这种 BGP Flow Specification 路由包含 BGP 网络层可达信息类型 (BGP Flow Spec NLRI) 和扩展团体属性。通过网络层可达信息和扩展团体属性，BGP Flow Specification 路由可以携带流量的匹配条件和流量匹配后执行的动作。RFC 5575 定义了 12 种常用的流量匹配规则：目的地址、源地址、IP 协议号、端口号、目的端口号、源端口号、ICMP 类型、ICMP 编码、TCP 的标志位、DSCP、分片类型等，这 12 种流量匹配规则封装在 BGP Flow Specification 路由中，作为网络层可达信息传递。RFC 5575 定义了 4 种常用的流量处理行为：丢弃流量、流量限速、修改报文的 DSCP 值、重定向到 VPN，这 4 种流量处理行为封装在 BGP Flow Spec 路由中，作为扩展团体属性携带。

有时一个很大的机构有许多部门分布在相距较远的一些地点，而在每一个地点都有自己的专用网。假定这些分布在不同地点的专用网需要经常进行通信，可以利用因特网 (即公用互联网) 来实现本机构的专用网，因此这样的专用网称为虚拟专用网 (Virtual Private Network, VPN)。

目前典型的 VPN 为 BGP/MPLS IP VPN，通常也称为 MPLS L3VPN，MPLS L3VPN 的基本模型由 CE、PE 和 P 三部分组成。

CE 指的是用户边缘设备 (Customer Edge)，CE 具有直接与服务提供商 (Service Provider, SP) 网络相连的接口。CE 可以是路由器或交换机，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 指的是提供商边缘设备 (Provider Edge)，是服务提供商网络的边缘设备，与 CE 直接相连，负责 VPN 业务接入，处理 VPN-IPv4 路由。一个 PE 设备可以连接多个 CE 设备。一个 CE 设备也可以连接属于相同或不同服务提供商的多个 PE 设备。

P 指的是服务提供商网络中的骨干设备，不与 CE 直接相连。

VPN 实例 (VPN-instance)，是 PE 设备为与其直接相连的 CE 设备建立并维护的一个专门实体，每个 CE 设备在与其直连的 PE 设备上都有自己的 VPN 实例。VPN 实例也称为 VPN

路由转发表 (VPN Routing and Forwarding table, VRF)。VRF 的内容包括 IP 路由表, 标记转发表, 使用标记转发表的接口, 管理信息 (路由过滤策略, 成员接口列表等)。每个 VPN 实例包含到一个或多个与该 PE 直接相连的 CE 设备的路由和转发表。

PE 设备上具有多个路由转发表, 包括一个公网路由转发表与一个或多个 VPN 路由转发表 (也可称为私网路由转发表)。公网路由表包括所有 PE 设备的 IPv4 路由, 且是由骨干网的路由协议或静态路由产生的, 公网转发表是根据路由管理策略从公网路由表提取出来的最小转发信息。而一个 VPN 实例的 VPN 路由表包括属于该 VPN 实例的所有 CE 设备的路由, 是通过 CE 设备与 PE 设备之间或者两个 PE 设备之间的 VPN 路由信息交互获得的, 例如, 包括从该 VPN 实例对应的 CE 设备获得的路由, 还有可能包括通过 MP-iBGP 路由引入的路由, VPN 转发表是根据路由管理策略从对应的 VPN 路由表提取出来的最小转发信息。

Site (站点), 是指相互之间具备 IP 连通性的一组 IP 系统, 且这组 IP 系统的 IP 连通性不需通过服务提供商网络实现。Site 是根据设备的网络拓扑关系而非地理位置划分的, 尽管通常情况下一个 Site 中的设备的地理位置均相邻, 如果地理位置隔离的两组 IP 系统之间使用专线互联, 而不需要通过服务提供商网络就可以互通, 则这两组 IP 系统构成一个 Site。Site 通过用户边缘设备 (Customer Edge, CE) 与服务提供商 (Service Provider, SP) 网络相连。

VPN、Site、VPN 实例之间的关系为: VPN 是多个 Site 的组合。一个 Site 可以属于多个 VPN。每一个 Site 在 PE 设备上都关联一个 VPN 实例。一个 VPN 实例综合了该 VPN 实例的 VPN 成员关系与路由规则, 多个 site 根据 VPN 实例的路由规则组合成一个 VPN。

路由标识符 (Route Distinguisher, RD), 是说明 IP 路由属于哪个 VPN 实例的标志, 具有全局唯一性, 8 个字节, 用于区分使用相同地址空间的 IP 地址前缀 (例如, IPv4 前缀、IPv6 前缀等) 的不同 VPN, VPN 通过 RD 实现地址空间的独立。RD 的结构使得每个服务提供商可以独立地分配 RD。RD 和 VPN 路由转发表 (VRF) 之间具有一一对应的关系, 通常情况下, 对于不同 PE 设备上属于同一个 VPN 实例的接口, 为其所对应的 VRF 分配相同的 RD, 换句话说, 为每一个 VPN 实例分配一个全局唯一的 RD。

增加了 RD 的 IPv4 地址称为 VPN-IPv4 地址, 例如 PE 设备从与其直连的 CE 设备接收到该 CE 设备的 IPv4 地址后, 通过添加 RD, 将该 IPv4 地址转换为全局唯一的 VPN-IPv4 地址, 并在公网上发布。VPN-IPv6 结构与 VPN-IPv4 类似, 只是将 IPv4 前缀替换成了 IPv6 前缀。

BGP/MPLS IP VPN 使用 VPN 目标 (VPN Target) 属性来控制 VPN 路由信息的发布。通常, VPN 目标属性也被称为路由目标 (Route Target, RT) 属性。BGP/MPLS IP VPN 使用两种类型的 RT 属性:

出口目标 (Export Target, ERT), PE 设备从直接相连 CE 设备学到 IPv4 路由后, 通过添加 RD, 将该 IPv4 路由转换为 VPN IPv4 路由, 并为该 VPN IPv4 路由设置 Export Target 属性, 然后将该设置了 Export Target 属性的 VPN IPv4 路由通过公网发布给其他 PE 设备, 其中, Export Target 属性作为 BGP 的扩展团体属性随 BGP Flow Spec 路由发布。

入口目标 (Import Target, IRT), 本地 PE 设备收到其它 PE 设备通过公网发布的 VPN-IPv4 路由时, 检查该 VPN-IPv4 路由的 Export Target 属性。当该 VPN-IPv4 路由的 Export Target 属性与该本地 PE 设备上某个 VPN 实例的 Import Target 属性匹配时, 该本地 PE 设备则将该 VPN-IPv4 路由加入到该某个 VPN 实例的 VPN 路由表中。每个 VPN 实例可

以关联一个或多个 RT 属性。

本地 PE 在把从与自己直接相连的 CE 学到的 VPN-IPv4 路由发布给其他 PE 前，为这些路由设置 Export Target 属性，并作为扩展团体属性随 Flow Spec 路由发布。一个 PE 收到其他 PE 发布的 VPN-IPv4 路由时，检查其 Export Target 属性，只有当该 VPN-IPv4 路由的 Export Target 属性与该 PE 上某个 VPN 实例的 Import Target 属性匹配时，才会把该 VPN-IPv4 路由加入到该某个 VPN 实例相应的 VRF 中。也就是说，RT 属性定义了一条 VPN-IPv4 路由可以为哪些站点所接收，以及 PE 可以接收哪些站点发送来的路由。

应理解，RT 属性同样适用于同一 PE 上不同 VPN 实例之间的 VPN 路由发布控制，即同一 PE 上的不同 VPN 实例之间可以设置相同的 Import Target 与 Export Target，来实现不同 VPN 实例之间的 VPN 路由的互相引入。

VPN 路由信息的发布包括，本地 CE 设备到入口 PE 设备（本地 CE 设备与入口 PE 设备直连）、入口 PE 设备到出口 PE 设备、出口 PE 设备到远端 CE 设备（远端 CE 设备与出口 PE 设备直连），大致流程为：入口 PE 设备从本地 CE 设备学习 IPv4 路由信息，并为这些标准 IPv4 路由增加 RD 和 VPN Target 属性，形成 VPN-IPv4 路由，存放为为该 CE 设备创建的 VPN 实例中。应理解，该本地 CE 设备的 IPv4 路由信息可以直接配置到该入口 PE 设备上，或者该入口 PE 设备使用其他方法来获得。入口 PE 通过 MP-BGP 把该 VPN-IPv4 路由发布给出口 PE 设备。出口 PE 设备根据该 VPN-IPv4 路由的 Export Target 属性与自己维护的 VPN 实例的 Import Target 属性进行比较，判决是否将该 VPN-IPv4 路由加入到自己维护的某个 VPN 实例的 VPN 路由表中。入口 PE 设备与出口 PE 设备之间可以通过 IGP 来保证连通性。当该 VPN-IPv4 路由的 Export Target 属性与自己维护的某个 VPN 实例的 Import Target 属性相符时，出口 PE 设备将该 VPN-IPv4 路由加入到该某个 VPN 实例的 VPN 路由表中。远端 CE 设备从出口 PE 设备学习该 VPN-IPv4 路由对应的 IPv4 路由。远端 CE 可以通过多种方式从出口 PE 设备学习 VPN 路由，例如，包括静态路由、RIP、OSPF、IS-IS 或 BGP 等路方式，这个过程可以与本地 CE 设备与入口 PE 设备之间的 VPN 路由信息的交换过程相同。完成这三部分的路由交互之后，本地 CE 设备与远端 CE 设备之间将建立可达路由，保证了 VPN 私网路由信息能够在骨干网上传递。

为了便于理解和描述，下文以虚拟专用网 VPN 场景为例进行描述，对应地，转发设备以 PE 设备为例，但本发明实施例不限于此。本领域技术人员根据本发明实施例的教导可以很清楚地理解，本发明实施例的方法同样可以应用于其他的与引导数据流进入相应转发通道有关的场景，这样的应用均落入本发明的范围内。

图 1 示出了本发明实施例的一个具体应用场景，PE1、PE2 和 PE3 为部署 VPN 业务的 3 个 PE 设备，PE1、PE2 和 PE3 的 IP 地址分别为 1.1.1.1、2.2.2.2 与 3.3.3.3，例如在图 1 所示网络中，IP 地址 2.2.2.2 就可以代表 PE2。控制器（如图 1 中所示的软件定义网络（Software Define Network, SDN）控制器）接收用户设备（如图 1 中所示的协同器/网管/用户 APP）的 VPN 服务请求，基于该 VPN 服务请求，通过向 PE 设备下发信令，以实现用户所请求的 VPN 业务。

图 1 中示意性地给出了 4 个 Site，其中，Site1 通过 CE1 与 PE1 相连，PE1 上通过建立 VPN 实例 vpn1 与 CE1 保持联系；Site2 通过 CE2 与 PE1 相连，PE1 上通过建立 VPN 实例 vpn2 与 CE1 保持联系；Site3 通过 CE3 与 PE2 相连，PE2 上通过建立 VPN 实例 vpn1 与 CE3 保持联系；Site4 通过 CE4 与 PE3 相连，PE3 上通过建立 VPN 实例 vpn1 与 CE4 保持联系。

PE1 上建立的与 CE1 关联的 VPN 实例 vpn1 的属性信息如下:

VPN-Instance Name: vpn1

RD: 100 : 1

Import Target (下文简称 IRT): 100 : 1

5 Export Target (下文简称 ERT): 100 : 2

VPN 接口 (Interface): interface1 (如图 1 所示 PE1 上的 interface1)

VPN 索引 (VPN-Index): 101 (图 1 未示出)

PE1 上建立的与 CE2 关联的 VPN 实例 vpn2 的属性信息如下:

VPN-Instance Name: vpn2

10 RD: 100 : 2

IRT: 100 : 1

ERT: 100 : 2

Interface: interface2 (如图 1 所示 PE1 上的 interface2)

VPN-Index: 102 (图 1 未示出)

15 PE2 上建立的与 CE3 关联的 VPN 实例 vpn1 的属性信息如下:

VPN-Instance Name: vpn1

RD: 100 : 1

IRT: 100 : 1

ERT: 100 : 2

20 Interface: interface1 (如图 1 所示 PE2 上的 interface1)

VPN-Index: 201 (图 1 未示出)

PE3 上建立的与 CE4 关联的 VPN 实例 vpn1 的属性信息如下:

VPN-Instance Name: vpn1

RD: 100 : 1

25 IRT: 100 : 2

ERT: 100 : 1

Interface: interface1 (如图 1 所示 PE3 上的 interface1)

VPN-Index: 301 (图 1 未示出)

应理解, VPN 实例的名称 (例如图 1 中所示的 vpn1 与 vpn2) 仅在自己所在的 PE 设备上
30 有意义。虽然 PE1/2/3 上都建立有 VPN 实例 vpn1, 但并不一定表示它们均属于一个 VPN,
是否属于一个 VPN 是由每个 VPN 实例所配置的 Import Target、Export Target 的匹配关
系决定的。例如, 在图 1 中, PE1 上的 VPN 实例 vpn1 与 PE3 上的 VPN 实例 vpn1 所配置
的 Import Target、Export Target 相互匹配, 可以提供 VPN 服务, 因为它们属于一个 VPN。
但是 PE1 上的 VPN 实例 vpn1 与 PE2 上的 VPN 实例 vpn1 所配置的 Import Target、Export
35 Target 不匹配, 不能提供 VPN 服务, 因此他们不属于一个 VPN。

为了简洁起见, 下文中采用“CE1 的 VPN 实例”的描述方式来表示“PE1 上建立的与 CE1
关联的 VPN 实例”, 类似描述方式同样适用于 CE2、CE3 与 CE4。

由上可知, CE1、CE2 与 CE3 各自 VPN 实例的 RT 属性 (即 IRT 与 ERT) 分别与 CE4 的
VPN 实例的 RT 属性相匹配, 则 CE1、CE2 与 CE3 各自的 IPv4 可以被 PE3 引入到 CE4 的 VPN
40 实例的 VPN 路由转发表 (VRF) 中, CE4 的 IPv4 路由信息也可以分别被引入到 CE1、CE2 与

CE3 的 VPN 实例的 VRF 中。也就是说, CE1 与 CE4 之间可以互相访问, CE2 与 CE4 之间可以互相访问, CE3 与 CE4 之间可以互相访问。但是, CE1、CE2 与 CE3 之间各自的 VPN 实例的 RT 属性彼此都不匹配, 则 CE1 的 VPN 实例的 VRF 中不包括 CE2 与 CE3 的路由信息, CE2 的 VPN 实例的 VRF 中不包括 CE1 与 CE3 的路由信息, CE3 的 VPN 实例的 VRF 中不包括 CE1 与 CE2 的路由信息。因此, 基于当前的 VPN 路由转发表, CE1 与 CE2 之间、CE1 与 CE3、以及 CE2 与 CE3 之间无法进行互相访问。例如, 当用户提出要实现 CE1 与 CE2 进行互访的 VPN 服务请求时, 基于现有的 VPN 部署, 无法满足用户需求。

针对上述技术问题, 现有技术中, 通常通过人工配置分别与 CE1 与 CE2 关联的 VPN 实例的 Import Target、Export Target 的匹配关系, 以实现 CE1 与 CE2 的互访。但是人工配置方式操作繁琐, 效率较低。

针对上述技术问题, 本发明实施例提出一种基于流规则 Flow Spec 的通信方法, 能够灵活、高效地实现 RT 属性不匹配的 CE 设备之间的访问, 同时能够有效避免无限制地扩展 BGP Flow Spec 协议。

为了便于理解和描述, 下面以图 1 所示网络部署为例, 描述根据本发明实施例提供的基于流规则 Flow Spec 的通信方法 100。如图 2 所示, 该方法 100 包括:

S110, 控制器 (如图 1 所示的 SDN 控制器) 接收用户侧 (如图 1 所示的协同器/网管/用户 APP) 的 VPN 服务请求, 该 VPN 服务请求用于请求实现 CE1 到 CE2 的访问, 也就是引导源于 CE1 的数据报文进入 CE2 的转发通道。

S120, 控制器根据该 VPN 服务请求, 获取到第一资源需要关联第二资源的需求, 所述第一资源为 CE2 的路由信息, 所述第二资源为 CE1 的 VPN 实例。

S130, 控制器根据该需求, 向 PE1 发送 BGP Flow Spec 协议报文, 该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段, 该网络层可达性信息字段携带该第一资源的特征信息, 所述扩展团体属性字段携带用于指示第二资源的全局标识 GID, 所述第一资源的特征信息表示能够指示 CE2 的路由信息的信息, 该 BGP Flow Spec 协议报文用于指示将 CE2 的路由信息加入到 CE1 的 VPN 实例的 VRF 中。

S140, PE1 接收到控制器下发的该 BGP Flow Spec 协议报文后, 通过解析该 BGP Flow Spec 协议报文, 基于该第一资源的特征信息获取 CE2 的路由信息, 基于该 GID 获取 CE1 的 VPN 实例, 然后将 CE2 的路由信息加入到 CE1 的 VPN 实例的 VRF 中。

应理解, 在本发明实施例中, CE1 要访问的 CE2 与 PE1 直连, 因此, PE1 可以通过与 CE2 之间的直接通信获取到 CE2 的路由信息, 或者 CE2 的路由信息也可以配置在 PE1 上, 本发明实施例对此不作限定。

通过上述步骤打通了 CE1 到 CE2 的访问路径。

S150, PE1 从接口 (Interface) 1 接收到源于 CE1 要访问 CE2 的数据报文, 即该数据报文的源 IP 地址为 CE1 的 IP 地址、目的 IP 地址为 CE2 的 IP 地址。

S160, PE1 根据该数据报文的源 IP 地址, 查找 CE1 的 VPN 实例的 VRF, 获取到 CE2 的路由信息, 进而确定该数据报文的转发出口, 即 CE2 的 VPN 实例的接口 Interface2, 将该数据报文从 Interface2 转发出去, 使得该数据报文送达 CE2, 即实现了 CE1 到 CE2 的访问。

应理解, 如果 VPN 服务请求为 CE2 需要对 CE1 进行访问, 只需将上述步骤 S110 至 S160 中的 CE1 与 CE2 对换位置, 就能实现 CE2 对 CE1 的访问了。

在本发明实施例中，通过控制器向 PE 设备下发 BGP Flow Spec 协议报文，指示 PE 设备将 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由信息加入所述第一 CE 设备的路由表中，从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道，即实现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此，相对于现有技术中的手工配置方式，本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。此外，相对于传统技术中局限于在转发平面引导数据流进入相应的转发通道，本申请能够在控制平面引导数据流进入相应的转发通道，从而能够实现灵活的业务编排。

具体地，在图 1 所示场景中，被访问端 CE2 与 PE1 直连，即 PE1 设备上建立并维护有 CE2 的 VPN 实例，在本发明实施例中，该第一资源的特征信息可以是在 PE1 上存储的与 CE2 的 VPN 实例相关的信息。具体地，该第一资源的特征信息可以是下列信息：CE2 的 VPN 实例名称、RD、RT、VPN 索引、VPN 接口、IP 地址前缀、MAC 地址中的至少一个信息，或多个信息，当该第一资源的特征信息包括上述信息中的多个信息时，这个多个信息之间可以是和/或的关系。

具体地，在本发明实施例中，所述扩展团体属性中携带的用于指示第二资源的 GID 可以与所述 CE1 的 VPN 实例的属性信息具有映射关系。

可选地，在本发明实施例中，该方法 100 还包括：

S170，控制器分别获取 PE1、PE2、PE3 上维护的 VPN 实例的属性信息，该属性信息包括 VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息。

具体地，PE1、PE2、PE3 分别向控制器上报本地建立的 VPN 实例的属性信息，表 1 示意性地给出了 PE1、PE2、PE3 分别向控制器上报的 VPN 实例的属性信息：

表 1

PE 设备名称	PE 设备上的 VPN 实例的属性信息
PE1	IP 地址: 1.1.1.1 { VPN-Instance Name: vpn1 RD: 100:1 IRT: 100:1 ERT: 100:2 Interface: interface1 VPN-Index: 101 }, { VPN-Instance Name: vpn2 RD: 100:2 IRT: 100:1 ERT: 100:2 Interface: interface2

	VPN-Index: 102 }
PE2	IP 地址: 2.2.2.2 { VPN-Instance Name: vpn1 RD : 100:1 IRT: 100:1 ERT : 100:2 Interface: interface1 VPN-Index: 201 }
PE3	IP 地址: 3.3.3.3 { VPN-Instance Name: vpn1 RD: 100:1 IRT : 100:2 ERT : 100:1 Interface: interface1 VPN-Index : 301 }

应理解，以 PE2 为例，CE3 的 VPN 实例的属性信息 VPN-Instance Name、RD、IRT、ERT、Interface 是通过命令行配置到 PE2 设备上的，VPN-Index 是在 PE2 设备上配置 CE3 的 VPN 实例之后，PE2 设备为 CE3 的 VPN 实例分配的索引值。上述处理方式同样适用于 PE1 和 PE3，这里不再赘述。

S180，控制器获得 PE1、PE2、PE3 的 VPN 实例的属性信息后，为每个 PE 设备上的 VPN 实例的属性信息分配通用标识 (Generic ID, GID)。

具体地，该 GID 是针对每个 PE 设备而言的，例如，表 2 作为示例给出了控制器为 PE1 上的 VPN 实例的属性信息分配 GID 的情形，表 3 作为示例给出了控制器为 PE2 上的 VPN 实例的属性信息分配 GID 的情形，表 4 作为示例给出了控制器为 PE3 上的 VPN 实例的属性信息分配 GID 的情形。

从表 2、表 3 和表 4 可知，在一个 PE 设备内，控制器分配的 GID 与每个 VPN 实例的各个属性信息一一对应。应理解，表 2、表 3 和表 4 仅为示例而非限定，例如，针对 PE1，控制器也可以为 CE1 的 VPN 实例的全部属性信息统一分配一个 GID，例如 20，为 CE2 的 VPN 实例的全部属性信息统一分配一个 GID，例如 30。

表 2

PE1: 1.1.1.1	
GID	VPN 实例的属性信息
1	VPN-Instance Name: vpn1
2	vpn1 的 RD: 100:1

3	vpn1 的 IRT: 100: 1
4	vpn1 的 ERT: 100: 2
5	vpn1 的 Interface: interface1
6	vpn1 的 VPN-Index: 101
7	VPN-Instance Name: vpn2
8	vpn2 的 RD: 100: 2
9	vpn2 的 IRT: 100: 1
10	vpn2 的 ERT: 100: 2
11	vpn2 的 Interface: interface2
12	vpn2 的 VPN-Index: 102

表 3

PE2: 2. 2. 2. 2	
GID	资源描述
1	VPN-Instance Name: vpn1
2	vpn1 的 RD: 100: 1
3	vpn1 的 IRT: 100: 1
4	vpn1 的 ERT: 100: 2
5	vpn1 的 Interface: interface1
6	vpn1 的 VPN-Index: 201

表 4

PE3: 3. 3. 3. 3	
GID	资源描述
1	VPN-Instance Name: vpn1
2	vpn1 的 RD: 100: 1
3	vpn1 的 IRT: 100: 2
4	vpn1 的 ERT: 100: 1
5	vpn1 的 Interface: interface1
6	vpn1 的 VPN-Index: 301

5

表 2 也可称之为 PE1 的 VPN 实例-GID 映射表。表 3 也可称之为 PE2 的 VPN 实例-GID 映射表。表 4 也可称之为 PE3 的 VPN 实例-GID 映射表。这些 VPN 实例-GID 映射表包含了相关 VPN 实例属性信息与为其分配的 GID 之间的映射关系。

10 S190, 控制器分别向 PE1、PE2、PE3 下发对应 PE 所对应的 VPN 实例-GID 映射表。例如控制器仅向 PE1 设备发送“PE1: 1. 1. 1. 1”所对应的 VPN 实例-GID 映射表 (如表 2 所示); 仅向 PE2 设备发送“PE2: 2. 2. 2. 2”所对应的 VPN 实例-GID 映射表 (如表 3 所示); 仅向 PE3 设备发送“PE3: 3. 3. 3. 3”所对应的 VPN 实例-GID 映射表 (如表 4 所示)。

PE1 收到控制器下发的如表 2 所示的 VPN 实例-GID 映射表后, 在本地保存, 因此, 对

于 PE1 与控制器来说,二者公知 GID“1”映射 CE1 的 VPN 实例的属性信息“VPN-Instance Name: vpn1”。应理解,在 PE1 上,GID“1”(或 GID“2”至“6”中的任一个)能够唯一指示 CE1 的 VPN 实例;GID“7”(或 GID“8”至“12”中的任一个)能够唯一指示 CE2 的 VPN 实例。

5 可选地,在本发明实施例中,用于指示第二资源的 GID 为 CE1 的 VPN 实例的某个属性信息所对应的 GID,例如,GID“1”。第一资源的特征信息也可以为 CE2 的 VPN 实例的某个属性信息所对应的 GID,例如,GID“6”。

应理解,在本发明实施例中,控制器为 PE 设备(如图 1 中所示的 PE1/2/3)上的 VPN 实例的属性信息分配的全局标识也可称之为映射标签,BGP FlowSpec 协议报文的扩展团体属性字段的 GID 字段中携带的 GID 为该映射标签中的一个或多个标识。

10 因此,在本发明实施例中,通过所述 GID,所述 PE 设备能够定位到所述 CE1 的 VPN 实例。因此,在本发明实施例中,通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID,就能够指示所述 CE1 的 VPN 实例,这样能够节省信令开销。

具体地,在本发明实施例中,第一资源的特征信息可以为:CE2 的 VPN 实例名称、VPN RD、VPN RT、VPN 索引、VPN 接口、IP 地址前缀、MAC 地址,以及控制器为 CE2 的 VPN 实例的属性信息分配的 GID 中的任一种信息,或多个信息时,该第一资源的特征信息以 TLV (Type/Length/Value,类型/长度/值)的方式封装在 Flow Spec NLRI 中,如表 5 所示:

表 5

类 型 值 (Type)	Value 值所对应的信息
TLV1	Generic ID
TLV2	VPN 名字
TLV3	VPN 索引
TLV4	VPN RT
TLV5	VPN RD
TLV6	接口
TLV7	源 IP 地址前缀
TLV8	目的 IP 地址前缀
TLV9	源 MAC 地址
TLV10	目的 MAC 地址

20 可选地,在本发明实施例中,BGP Flow Spec 协议报文中的扩展团体属性字段包括标志 Flags 字段与 GID 字段,该 Flags 字段包括转发平面比特位、控制平面比特位,在该转发平面比特位赋值为 0、且该控制平面比特位赋值为 1 时,用于指示在控制平面上关联第一资源与第二资源,在该转发平面比特位赋值为 1、且该控制平面比特位赋值为 0 时,用于指示在转发平面上关联第一资源与第二资源,GID 字段携带该第二标识。

25 传统技术中,扩展的应用通常仅局限在转发平面引导数据流进入相应的转发通道。在本发明实施例中,不仅可以在转发平面引导数据流进入相应的转发通道,也可以在控制平面引导数据流进入相应的转发通道,从而本申请能够实现灵活地业务编排。

应理解,在本发明实施例中,所述 Flags 字段中的转发平面比特位与控制平面比特位,也可以用第一比特位替换,当该第一比特位赋值为 1 时,表示在所述控制平面上关联所述

第一资源与所述第二资源，当该第一比特位赋值为 0 时，表示在所述转发平面上关联所述第一资源与所述第二资源。

可选地，在本发明实施例中，扩展团体属性字段的 Flags 字段还包括增量比特位，当所述增量比特位赋值为 1 时，表示在所述转发设备上增加一个资源关联关系，当所述增量比特位赋值为 0 时，表示利用所述第一资源与所述第二资源之间的关联关系覆盖所述第一资源原有的与其他资源之间的关联关系。

具体地，如图 3 所示，该扩展团体属性格式包括 Type 字段、Sub-Type 字段、Flags 字段、Reserved 字段和 GID 字段。Type 字段与 Sub-Type 字段待 IETF 标准组织正式分配。Reserved 为保留字段，赋值为“0”。Flags 字段，占用 1 个字节，bit 7 为控制平面比特位（Control-Plane Bit，控制平面比特位），设置为 1 表示在控制平面上关联所述第一资源与所述第二资源，否则设置为 0；bit 6 为转发平面比特位（Forwarding-Plane Bit，F 比特位），设置为 1 表示在转发平面上关联所述第一资源与所述第二资源，否则设置为 0；bit 5 为增量比特位（Additive Bit，A 比特位），设置为 1 表示是在原有的基础上，增加一个关联关系；否则就是以新的关联关系覆盖原有的关联关系。GID 字段携带第二标识，该第二标识为 CE2 的 VPN 实例的某个属性信息所对应的 GID。

应理解，在本发明实施例中，控制器向 PE1 下发的 BGP Flow Spec 协议报文用于指示将 CE2 的路由信息加入到 CE1 的 VPN 实例的 VRF 中，该动作属于位于控制平面上的动作，因此，如图 3 所示扩展团体属性的 Flags 字段中的 C 比特为赋值为“1”，F 比特位赋值为“0”，A 比特的赋值可以根据具体业务需求确定。

在本发明实施例中，扩展团体属性的格式简单明了，利用 C 比特位、F 比特位以及 GID 字段，就向 PE 设备指明了要执行的动作。而且，通过 A、C、F 比特位的不同组合，能让该扩展团体属性指示不同的动作，避免了现有技术中对 BGP Flow Spec 协议的无限制扩展。

本发明实施例中包括第二标识的扩展团体属性可称之为名为“Redirect to GID Action”的扩展团体属性。

在本发明实施例中，通过控制器向 PE 设备（即转发设备）下发 BGP Flow Spec 协议报文，指示 PE 设备将 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由信息加入所述第一 CE 设备的路由表中，从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道，即实现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此，相对于现有技术中的手工配置方式，本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。此外，相对于传统技术中局限于在转发平面引导数据流进入相应的转发通道，本申请能够在控制平面引导数据流进入相应的转发通道，从而能够实现灵活的业务编排。

如图 4 所示，本发明实施例还提供了一种在转发平面上关联第一资源与第二资源的方法 200，还以图 1 所示场景为例，该方法 200 包括：

S210，控制器（如图 1 所示的 SDN 控制器）接收用户侧（如图 1 所示的协同器/网管/用户 APP）的 VPN 服务请求，该 VPN 服务请求用于请求实现 CE1 到 CE2 的访问，也就是引导源于 CE1 的数据报文进入 CE2 的转发通道。

S220，控制器根据该 VPN 服务请求，获取到第一资源需要关联第二资源的需求，所述第一资源为源 IP 地址为 CE1 的 IP 地址、且目的 IP 地址为 CE2 的 IP 地址，所述第二资源为 CE2 的 VPN 实例。

S230, 控制器根据该需求, 向 PE1 发送 BGP Flow Spec 协议报文, 该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段, 该网络层可达性信息字段携带该第一资源的特征信息, 所述扩展团体属性字段携带用于指示第二资源的全局标识 GID, 所述第一资源的特征信息表示源 IP 地址为 CE1 的 IP 地址、且目的 IP 地址为 CE2 的 IP 地址, 该 BGP Flow Spec 协议报文用于指示将源 IP 地址与目的 IP 地址与该第一资源的特征信息相一致的数据报文, 按照 CE2 的 VPN 实例的 VPN 路由转发表进行转发。

S240, PE1 接收到控制器下发的该 BGP Flow Spec 协议报文后, 解析该 BGP Flow Spec 协议报文, 获知要将源 IP 地址为 CE1 的 IP 地址、目的 IP 地址为 CE2 的 IP 地址的数据报文, 与 CE2 的 VPN 实例进行绑定。

S250, PE1 从 CE1 接收到数据报文, 该数据报文的源 IP 地址为 CE1 的 IP 地址、目的 IP 地址为 CE2 的 IP 地址。

S260, PE1 根据该数据报文的的目的 IP 地址, 查找 CE2 的 VPN 实例的 VRF, 确定该数据报文的转发出口, 即 CE2 的 VPN 实例的接口 Interface2, 将该数据报文从 Interface2 转发出去, 使得该数据报文送达 CE2, 即实现了 CE1 到 CE2 的访问。

具体地, 该扩展团体属性的格式如图 3 所示, 且 Flags 字段中的 C 比特为赋值为“0”, F 比特位赋值为“1”, GID 字段携带 CE2 的 VPN 实例的属性信息所对应的 GID (如表 2 中所示的控制器为 CE2 的 VPN 实例的属性信息分配的 GID)。

应理解, 如果 VPN 服务请求为 CE2 需要对 CE1 进行访问, 只需将上述步骤 S210 至 S250 中的 CE1 与 CE2 对换位置, 就能实现 CE2 对 CE1 的访问了。

在本发明实施例中, 通过控制器向 PE 设备下发 BGP Flow Spec 协议报文, 指示 PE 设备针对源 IP 地址为第一 CE 设备的 IP 地址、且目的 IP 地址为第二 CE 设备的 IP 地址的数据报文, 按照 VPN RT 属性与第一 CE 设备不匹配的第二 CE 设备的路由转发表进行转发, 从而能够引导来源于第一 CE 设备的数据报文进入第二 CE 设备的转发通道, 即实现了 VPN RT 属性不匹配的第一 CE 设备访问第二 CE 设备。因此, 相对于现有技术中的手工配置方式, 本申请能够灵活、高效地实现两个 VPN RT 属性不匹配的 CE 设备之间的 VPN 通信。

上文所述步骤 S170 至 S190 描述的方案同样适用于如图 4 所示在转发平面执行动作的方法 200, 为了避免重复, 这里不再赘述。

需要说明的是, 上述结合图 2 和图 4 描述的方法, 均是假设 VPN 服务请求为 CE1 访问 CE2, 或者 CE2 访问 CE1 为例进行说明, 即访问端 CE 与被访问端 CE 均与同一个 PE 设备直连, 但本发明实施例并非限于此, 本发明实施例提供的方法也可应用于访问端 CE 与被访问端 CE 分别与不同 PE 设备直连的应用场景。

在访问端 CE 与被访问端 CE 分别与不同 PE 设备直连的应用场景下, 利用本发明实施例提供的方法, 通过在控制平面执行动作来实现访问端 CE 对被访问端 CE 的访问的步骤如下:

还以图 1 所述网络部署为例进行描述, 控制器 (如图 1 所示的 SDN 控制器) 接收用户侧 (如图 1 所示的协同器/网管/用户 APP) 的 VPN 服务请求, 该 VPN 服务请求用于请求实现 CE1 到 CE3 的访问, 即引导源于 CE1 的数据报文进入 CE3 的转发通道。控制器根据该 VPN 服务请求, 获取到第一资源需要关联第二资源的需求, 所述第一资源为 CE3 的路由信息, 所述第二资源为 CE1 的 VPN 实例。控制器根据该需求, 向 PE1 发送 BGP Flow Spec 协议报文, 该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段, 该网络

层可达性信息字段携带该第一资源的特征信息，所述扩展团体属性字段携带用于指示第二资源的全局标识 GID，所述第一资源的特征信息表示能够指示 CE3 的路由信息的信息，该 BGP Flow Spec 协议报文用于指示将 CE3 的路由信息加入到 CE1 的 VPN 实例的 VRF 中。PE1 接收到控制器下发的该 BGP Flow Spec 协议报文后，通过解析该 BGP Flow Spec 协议报文，
5 基于该第一资源的特征信息获取 CE3 的路由信息，基于该 GID 获取 CE1 的 VPN 实例，然后将 CE3 的路由信息加入到 CE1 的 VPN 实例的 VRF 中。PE1 从接口 Interface1 接收到源于 CE1 要访问 CE2 的数据报文，即该数据报文的源 IP 地址为 CE1 的 IP 地址、目的 IP 地址为 CE2 的 IP 地址。PE1 根据该数据报文的目的 IP 地址，查找 CE1 的 VPN 实例的 VRF，获取到 CE3 的路由信息，根据 CE3 的路由信息的转发表项，将该数据报文导入 CE3 的转发通道。

10 应理解，虽然 PE1 不与 CE3 直连，但是 PE1 可以通过与 PE2 的通信，获取到 CE3 的路由信息。结合上文针对 VPN-IPv4 概念的描述，本领域技术人员可以了解到，PE2 获取到 CE2 的 IPv4（也可以是 IPv6）地址后，为该 IPv4 地址增加 CE3 的 VPN 实例的 RD 和 ERT 属性（应理解，在 PE2 上建立有 CE3 的 VPN 实例，如图 1 所示），得到 CE3 的 VPN-IPv4 路由，然后将该 VPN-IPv4 路由通过 PE2 与 PE1 之间的通信链路向 PE1 发布，从而，PE1 就获取到了
15 了 CE3 的路由信息。

应理解，实现 CE3 访问 CE1 的方法与上述描述类似，将 CE1 与 CE3 的位置互换，并将 PE1 与 PE2 的位置互换，即可。

在访问端 CE 与被访问端 CE 分别与不同 PE 设备直连的应用场景下，利用本发明实施例提供的方法，通过在转发平面执行动作来实现访问端 CE 对被访问端 CE 的访问的步骤如
20 下：

还以图 1 所述网络部署为例进行描述，并且假设 CE2 在 PE1 上的 VPN 实例的属性信息如下：

VPN-Instance Name: vpn2

RD: 100 : 2

25 IRT: 100 : 2

ERT: 100 : 1

Interface: interface2（如图 1 所示 PE1 上的 interface2）

VPN-Index: 102（图 1 未示出）

也就是说，CE3 的 VPN 实例与 CE2 的 VPN 实例的 RT 属性相匹配，PE1 维护的 CE2 的 VPN
30 实例的 VRF 中包括 CE3 的路由信息，也就是说，在 CE2 的 VPN 实例的 VPN 转发表中包括 CE3 的路由信息的转发表项。

控制器（如图 1 所示的 SDN 控制器）接收用户侧（如图 1 所示的协同器/网管/用户 APP）的 VPN 服务请求，该 VPN 服务请求用于请求实现 CE1 到 CE3 的访问，也就是引导源于 CE1 的数据报文进入 CE3 的转发通道。控制器根据该 VPN 服务请求，获取到第一资源需要关联
35 第二资源的需求，所述第一资源为源 IP 地址为 CE1 的 IP 地址、且目的 IP 地址为 CE2 的 IP 地址，所述第二资源为 CE3 的 VPN 实例。控制器根据该需求，向 PE1 发送 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，该网络层可达性信息字段携带该第一资源的特征信息，所述扩展团体属性字段携带用于指示第二资源的全局标识 GID，所述第一资源的特征信息表示源 IP 地址为 CE1 的 IP 地址、
40 且目的 IP 地址为 CE2 的 IP 地址，该 BGP Flow Spec 协议报文用于指示将源 IP 地址与目

的 IP 地址与该第一资源的特征信息相一致的数据报文, 按照 CE3 的 VPN 实例的 VPN 路由转发表进行转发。PE1 接收到控制器下发的该 BGP Flow Spec 协议报文后, 解析该 BGP Flow Spec 协议报文。PE1 从 CE1 接收到数据报文, 该数据报文的源 IP 地址为 CE1 的 IP 地址、目的 IP 地址为 CE2 的 IP 地址。PE1 根据该数据报文的目的 IP 地址, 查找 CE2 的 VPN 实例的 VPN 转发表, 定位到 CE3 的路由信息的转发表项, 按照该转发表项将该数据报文转发出去, 该数据报文就会到达 CE3, 从而实现了 CE1 到 CE3 的访问。

应理解, 在访问端 CE 与被访问端 CE 分别与不同 PE 设备直连的应用场景下, 利用本发明实施例提供的方法, 通过在转发平面执行动作来实现访问端 CE 对被访问端 CE 的访问的前提是, 与访问端 CE 直连的 PE 设备上具有一个 VPN 实例, 且该 VPN 实例的 VRF 中包括被访问端 CE 的路由信息。

本发明实施例提供的基于流规则 Flow Spec 的通信方法, 通过在控制平面修改 VPN 路由表, 能够灵活、高效地实现 RT 属性不匹配的 CE 设备之间的 VPN 通信。

因此, 本发明实施例中, 通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息, 扩展团体属性字段中携带用于指示第二资源的全局标识 GID, 能够指示转发设备关联所述第一资源与所述第二资源, 以引导数据流进入相应的转发通道。相对于传统技术, 本申请中的 BGP FlowSpec 协议通过统一的报文格式, 可以满足多种业务需求, 从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外, 通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID, 就能够指示所述第二资源, 能够节省信令开销。

可选地, 在本发明实施例中, 还包括:

该控制器获取第二 VPN 服务请求, 该第二 VPN 服务请求用于请求为 PE2 设备上新增的 CE5 (如图 5 所示) 的 VPN 实例配置属性信息, 为 PE3 设备上新增的 CE6 (如图 5 所示) 的 VPN 实例配置属性信息。

该控制器根据该第二 VPN 服务请求, 为 CE5 的 VPN 实例配置如下属性信息: VPN 实例名称、VPN 实例 RD、VPN 实例 RT、VPN 实例索引值和 VPN 实例接口信息, 并为 CE6 的 VPN 实例配置如下属性信息: VPN 实例名称、VPN 实例 RD、VPN 实例 RT、VPN 实例索引值和 VPN 实例接口信息, 其中, CE5 设备的 VPN 实例与 CE3 的 VPN 实例的下列属性信息不冲突: VPN 实例名称、VPN 实例 RD、VPN 实例索引信息, CE6 设备的 VPN 实例与 CE4 的 VPN 实例的下列属性信息不冲突: VPN 实例名称、VPN 实例 RD、VPN 实例索引信息。

具体地, 如图 5 所示, 用户有 CE5 和 CE6 两个设备, 现在需要通过运营商的网络以 VPN 的方式连通 CE5 和 CE6 这两个设备。

步骤 1: 用户向控制器发送 VPN 服务请求, VPN 服务请求用于请求通过 VPN 方式联通 CE5 和 CE6。

具体地, 该 VPN 服务请求中包括 CE5 和 CE6 的 IP 地址、MAC 地址等 CE 设备信息。

步骤 2: 控制器根据该 VPN 服务请求中携带的 CE 设备信息, 获知 CE5 与 PE2 连接, CE6 与 PE3 连接, 则确定要在 PE2 和 PE3 上部署 VPN, 以将 CE5 和 CE6 连通。

步骤 3, 控制器在 PE2 上配置对应于 CE5 的 VPN 实例, 并为该 CE5 的 VPN 实例的属性信息分配 GID, 如表 6 所示。由表 6 可知, 控制器为 PE2 上的 CE5 的 VPN 实例分配了与已有的 CE3 的 VPN 实例不冲突的属性信息 VPN-Instance Name、RD、IRT、ERT 及 VPN-Index, 同时也给 CE5 的 VPN 实例的每个属性信息分配了一个 GID 值。

步骤 4: 控制器将为 PE2 新分配的 CE5 的 VPN 实例的属性信息下发给 PE2。

步骤 5: 控制器将新增 CE5 的 VPN 实例的属性信息后的 GID 资源表（如表 6 所示）下发给 PE2，实现控制器和被控制设备上的 GID 资源表信息同步。

表 6

PE2: 2.2.2.2	
GID	资源描述
1	VPN-Instance Name: vpn1
2	vpn1 的 RD: 100:1
3	vpn1 的 IRT: 100:1
4	vpn1 的 ERT: 100:2
5	vpn1 的 Interface: interface1
6	vpn1 的 VPN-Index: 201
7	VPN-Instance Name: vpna
8	vpna 的 RD: 100:5
9	vpna 的 IRT: 100:5
10	vpna 的 ERT: 100:5
11	vpna 的 Interface: interface2
12	vpna 的 VPN-Index: 202

5

在如上步骤 3、4、5 中，仅描述了与 PE2 相关的处理过程，在实际实施过程中，对 PE3 的处理过程与 PE2 相同。

因此，在本发明实施例中，控制器通过获取 PE 设备上已有的 VPN 实例的属性信息，从而在为所述 PE 设备上增加的 VPN 实例配置属性信息时，能够避免不同 VPN 实例的属性信息之间的冲突。相比于现有技术中靠规划避免冲突，本申请能够有效地避免冲突，而且操作效率较高。

图 6 示出了根据本发明实施例提供的控制器 300 的示意性框图，如图 6 所示，该控制器 300 包括：

获取模块 310，用于获取转发设备上的第一资源需要关联该转发设备上的第二资源的需求；

发送模块 320，用于根据该获取模块获取的需求，向该转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，该网络层可达性信息字段携带第一资源的特征信息，该扩展团体属性字段携带用于指示该第二资源的全局标识 GID，该 BGP Flow Spec 协议报文用于指示关联该第一资源与该第二资源。

因此，在本发明实施例中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通道。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所

述第二资源，能够节省信令开销。

可选地，在本发明实施例中，该扩展团体属性字段包括GID字段与标志Flags字段，该GID字段携带该GID，该Flags字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联该第一资源与该第二资源的信息。

5 可选地，在本发明实施例中，该Flags字段包括转发平面比特位与控制平面比特位，当该转发平面比特位赋值为0、且该控制平面比特位赋值为1时，用于指示在该控制平面上关联该第一资源与该第二资源，当该转发平面比特位赋值为1、且该控制平面比特位赋值为0时，用于指示在该转发平面上关联该第一资源与该第二资源。

10 可选地，在本发明实施例中，该转发设备为服务商边缘PE设备，该转发设备上建立有第一用户边缘CE设备的虚拟专用网VPN实例，该转发设备上包括第二CE设备的路由信息，且该第二CE设备的路由信息不在该第一CE设备的VPN实例的VPN路由表中，该获取模块310用于，获取VPN服务请求，该VPN服务请求用于请求该第一CE设备访问该第二CE设备；根据该VPN服务请求，获取该第一资源需要关联该第二资源的需求，该第一资源为该第二CE设备的路由信息，该第二资源为该第一CE设备的VPN实例；

15 该发送模块320用于，根据该需求，向该转发设备发送该BGP Flow Spec协议报文，该BGP Flow Spec协议报文中的该Flags字段用于指示在控制平面上关联该第一资源与该第二资源，该BGP Flow Spec协议报文用于指示将该第二CE设备的路由信息加入到该第一CE设备的VPN实例的VPN路由表中。

20 可选地，在本发明实施例中，该获取模块310还用于，从该转发设备上获取该第一CE设备的VPN实例的属性信息，该属性信息包括：VPN实例名称、VPN实例路由标识符RD、VPN实例路由目标符RT、VPN实例索引值和VPN实例接口信息；

该控制器300还包括：

标识分配模块330，用于为该第一CE设备的VPN实例的属性信息分配映射标识，该映射标识在该转发设备中唯一指示该第一CE设备的VPN实例的属性信息；

25 该发送模块320还用于，向该转发设备发送映射表，该映射表包括该第一CE设备的VPN实例的属性信息与该映射标识之间的映射关系，

该GID字段中携带的该GID为该映射标识中的一个或多个标识。

可选地，在本发明实施例中，该获取模块310还用于，获取用于请求为该转发设备上新建的第三CE设备的VPN实例配置属性信息的VPN服务请求；

30 该控制器300还包括：

VPN实例配置模块340，用于为该第三CE设备的VPN实例配置如下属性信息：VPN实例名称、VPN实例RD、VPN实例RT和VPN实例接口信息，其中，该第三CE设备的VPN实例的下列属性信息与该第一CE设备的VPN实例对应的属性信息互不冲突：VPN实例名称、VPN实例RD、VPN实例接口信息。

35 可选地，在本发明实施例中，该转发设备上建立有该第二CE设备的VPN实例，该第二CE设备的VPN实例的VPN路由表中包括该第二CE设备的路由信息；

该第一资源的特征信息为该第二CE设备的VPN实例的下列属性信息中的至少一种信息：VPN实例名称、VPN实例RD、VPN实例索引值、VPN实例接口信息、VPN实例GID。

40 可选地，在本发明实施例中，该转发设备上没有建立该第二CE设备的VPN实例，该转发设备的VPN公网路由表中包括该第二CE设备的路由信息；

该第一资源的特征信息为下列信息中的至少一种：该第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息。

可选地，在本发明实施例中，该转发设备为服务商边缘 PE 设备，该转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例，该转发设备上还包括第二 CE 设备的路由信息，且该第一 CE 设备的 VPN 实例的 VPN 路由表中不包括该第二 CE 设备的路由信息，该第三 CE 设备的 VPN 实例的 VPN 路由表中包括该第二 CE 设备的路由信息，该获取模块 310 用于，获取 VPN 服务请求，该 VPN 服务请求用于请求该第一 CE 设备访问该第二 CE 设备；根据该 VPN 服务请求，获取该第一资源需要关联该第二资源的需求，该第一资源为源 IP 地址为该第一 CE 设备的 IP 地址、且目的 IP 地址为该第二 CE 设备的 IP 地址，该第二资源为该第三 CE 设备的 VPN 实例；

该发送模块 320 还用于，根据该需求，向该转发设备发送该 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文中的该 Flags 字段用于指示在转发平面上关联该第一资源与该第二资源，该 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与该第一资源相一致的数据报文，按照该第三 CE 设备的 VPN 实例的 VPN 路由表中包括的该第二 CE 设备的路由信息进行转发。

可选地，在本发明实施例中，该第二 CE 设备为该第三 CE 设备。

应理解，根据本发明实施例的控制器 300 可对应于本发明实施例的基于 Flow Spec 的通信方法中的控制器，并且控制器 300 中的各个模块的上述和其它操作和/或功能分别为了实现图 1 至图 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

图 7 示出了根据本发明实施例的转发设备 400 的示意性框图，如图 7 所示，该转发设备 400 包括：

接收模块 410，用于接收控制器发送的边界网关协议流规则 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，该网络层可达性信息字段携带用于指示该转发设备上的第一资源的该第一资源的特征信息，该扩展团体属性字段携带用于指示该转发设备上的第二资源的全局标识 GID，该 BGP Flow Spec 协议报文用于指示关联该第一资源与该第二资源；

获取模块 420，用于根据该接收模块接收的该第一资源的特征信息，获取该第一资源，根据该 GID，获取该第二资源；

关联模块 430，用于根据该接收模块接收的该 BGP Flow Spec 协议报文，关联该第一资源与该第二资源。

因此，在本发明实施例中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通道。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所述第二资源，能够节省信令开销。

可选地，在本发明实施例中，该扩展团体属性字段包括 GID 字段与标志 Flags 字段，该 GID 字段携带该 GID，该 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联该第一资源与该第二资源的信息。

可选地，在本发明实施例中，该 Flags 字段包括转发平面比特位与控制平面比特位，当该转发平面比特位赋值为 0、且该控制平面比特位赋值为 1 时，用于指示在该控制平面上关联该第一资源与该第二资源，当该转发平面比特位赋值为 1、且该控制平面比特位赋值为 0 时，用于指示在该转发平面上关联该第一资源与该第二资源。

5 可选地，在本发明实施例中，该转发设备 400 为服务商边缘 PE 设备，该转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例，该转发设备上包括第二 CE 设备的路由信息，且该第二 CE 设备的路由信息不在该第一 CE 设备的 VPN 实例的 VPN 路由表中，该接收模块 410 用于，接收该控制器根据 VPN 服务请求发送的该 BGP Flow Spec 协议报文，该 VPN 服务请求用于请求该第一 CE 设备访问该第二 CE 设备，其中，该第一资源为该第二
10 CE 设备的路由信息，该第二资源为该第一 CE 设备的 VPN 实例，该 BGP Flow Spec 协议报文中的该 Flags 字段用于指示在控制平面上关联该第一资源与该第二资源，该 BGP Flow Spec 协议报文用于指示将该第二 CE 设备的路由信息加入到该第一 CE 设备的 VPN 实例的 VPN 路由表中；

15 该关联模块 430，用于将该第二 CE 设备的路由信息加入到该第一 CE 设备的 VPN 实例的 VPN 路由表中。

可选地，在本发明实施例中，该转发设备 400 还包括：

发送模块 440，用于向该控制器发送该第一 CE 设备的 VPN 实例的属性信息，该属性信息包括：VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息；

20 该接收模块 410 用于，接收该控制器发送的映射表，该映射表包括该第一 CE 设备的 VPN 实例的属性信息与该控制器为该第一 CE 设备的 VPN 实例的属性信息分配的映射标识之间的映射关系，该映射标识在该转发设备中唯一指示该第一 CE 设备的 VPN 实例的属性信息，

该 GID 字段中携带的该 GID 为该映射标识中的一个或多个标识。

25 可选地，在本发明实施例中，该转发设备 400 上建立有该第二 CE 设备的 VPN 实例，该第二 CE 设备的 VPN 实例的 VPN 路由表中包括该第二 CE 设备的路由信息；

该第一资源的特征信息为该第二 CE 设备的 VPN 实例的下列属性信息中的至少一种信息：VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID；

30 该获取模块 420 用于，根据该第一资源的特征信息，从该第二 CE 设备的 VPN 实例的 VPN 路由表中获取该第二 CE 设备的路由信息。

可选地，在本发明实施例中，该转发设备 400 上没有建立该第二 CE 设备的 VPN 实例，该转发设备 400 的 VPN 公网路由表中包括该第二 CE 设备的路由信息；

该第一资源的特征信息为下列信息中的至少一种：该第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息；

35 该获取模块 420 用于，根据该第一资源的特征信息，从该 VPN 公网路由表中获取该第二 CE 设备的路由信息。

可选地，在本发明实施例中，该转发设备 400 为服务商边缘 PE 设备，该转发设备 400 上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例，该转发设备上还包括第二 CE 设备的路由信息，且该第一 CE 设备的 VPN 实例的 VPN 路由表中不包括该第二 CE 设备的路由信息，该第三 CE 设备的 VPN 实例的 VPN 路由表中包括该第二 CE
40

设备的路由信息，该接收模块 410 用于，接收该控制器根据 VPN 服务请求发送的 BGP Flow Spec 协议报文，该 VPN 服务请求用于请求该第一 CE 设备访问该第二 CE 设备，其中，该第一资源为源 IP 地址为该第一 CE 设备的 IP 地址、且目的 IP 地址为该第二 CE 设备的 IP 地址，该第二资源为该第三 CE 设备的 VPN 实例，该 BGP Flow Spec 协议报文中的该 Flags 5 字段用于指示在转发平面上关联该第一资源与该第二资源，该 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与该第一资源相一致的数据报文，按照该第三 CE 设备的 VPN 实例的 VPN 路由表中包括的该第二 CE 设备的路由信息进行转发；

该关联模块 430 包括：

接收单元，用于接收数据报文，该数据报文的源 IP 地址为该第一 CE 设备的 IP 地址、10 且目的 IP 地址为该第二 CE 设备的 IP 地址；

转发单元，用于按照该第三 CE 设备的 VPN 实例的 VPN 路由表中包括的该第二 CE 设备的路由信息转发该数据报文。

可选地，在本发明实施例中，该第二 CE 设备为该第三 CE 设备。

应理解，根据本发明实施例的转发设备 400 可对应于本发明实施例的基于 Flow Spec 15 的通信方法中的转发设备，并且转发设备 400 中的各个模块的上述和其它操作和/或功能分别为了实现图 1 至图 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

如图 8 所示，本发明实施例还提供了一种控制器 500，该控制器 500 包括处理器 510、存储器 520、总线系统 530、接收器 540 和发送器 550。其中，处理器 510、存储器 520、接收器 540 和发送器 550 通过总线系统 530 相连，该存储器 520 用于存储指令，该处理器 20 510 用于执行该存储器 520 存储的指令，以控制接收器 540 接收信号，并控制发送器 550 发送信号。其中，该处理器 510 用于，获取转发设备上的第一资源需要关联该转发设备上的第二资源的需求；发送器 550 用于，根据该需求，向该转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，该网络层可达性信息字段携带第一资源的特征信息，该扩展团体属性字 25 段携带用于指示该第二资源的全局标识 GID，该 BGP Flow Spec 协议报文用于指示关联该第一资源与该第二资源。

因此，在本发明实施例中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通 30 道。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所述第二资源，能够节省信令开销。

可选地，在本发明实施例中，该扩展团体属性字段包括 GID 字段与标志 Flags 字段，35 该 GID 字段携带该 GID，该 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联该第一资源与该第二资源的信息。

可选地，在本发明实施例中，该 Flags 字段包括转发平面比特位与控制平面比特位，当该转发平面比特位赋值为 0、且该控制平面比特位赋值为 1 时，用于指示在该控制平面上关联该第一资源与该第二资源，当该转发平面比特位赋值为 1、且该控制平面比特位赋 40 值为 0 时，用于指示在该转发平面上关联该第一资源与该第二资源。

可选地, 在本发明实施例中, 该转发设备为服务商边缘 PE 设备, 该转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例, 该转发设备上包括第二 CE 设备的路由信息, 且该第二 CE 设备的路由信息不在该第一 CE 设备的 VPN 实例的 VPN 路由表中, 该处理器 510 用于, 获取 VPN 服务请求, 该 VPN 服务请求用于请求该第一 CE 设备访问该第二 CE 设备; 根据该 VPN 服务请求, 获取该第一资源需要关联该第二资源的需求, 该第一资源为该第二 CE 设备的路由信息, 该第二资源为该第一 CE 设备的 VPN 实例; 该发送器 550 用于, 根据该需求, 向该转发设备发送该 BGP Flow Spec 协议报文, 该 BGP Flow Spec 协议报文中的该 Flags 字段用于指示在控制平面上关联该第一资源与该第二资源, 该 BGP Flow Spec 协议报文用于指示将该第二 CE 设备的路由信息加入到该第一 CE 设备的 VPN 实例的 VPN 路由表中。

可选地, 在本发明实施例中, 该处理器 510 用于, 从该转发设备上获取该第一 CE 设备的 VPN 实例的属性信息, 该属性信息包括: VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息; 为该第一 CE 设备的 VPN 实例的属性信息分配映射标识, 该映射标识在该转发设备中唯一指示该第一 CE 设备的 VPN 实例的属性信息; 该发送器 550 用于, 向该转发设备发送映射表, 该映射表包括该第一 CE 设备的 VPN 实例的属性信息与该映射标识之间的映射关系, 该 GID 字段中携带的该 GID 为该映射标识中的一个或多个标识。

可选地, 在本发明实施例中, 该处理器 510 用于, 获取用于请求为该转发设备上新建立的第三 CE 设备的 VPN 实例配置属性信息的 VPN 服务请求; 为该第三 CE 设备的 VPN 实例配置如下属性信息: VPN 实例名称、VPN 实例 RD、VPN 实例 RT 和 VPN 实例接口信息, 其中, 该第三 CE 设备的 VPN 实例的下列属性信息与该第一 CE 设备的 VPN 实例对应的属性信息互不冲突: VPN 实例名称、VPN 实例 RD、VPN 实例接口信息。

可选地, 在本发明实施例中, 该转发设备上建立有该第二 CE 设备的 VPN 实例, 该第二 CE 设备的 VPN 实例的 VPN 路由表中包括该第二 CE 设备的路由信息;

该第一资源的特征信息为该第二 CE 设备的 VPN 实例的下列属性信息中的至少一种信息: VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID。

可选地, 在本发明实施例中, 该转发设备上没有建立该第二 CE 设备的 VPN 实例, 该转发设备的 VPN 公网路由表中包括该第二 CE 设备的路由信息;

该第一资源的特征信息为下列信息中的至少一种: 该第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息。

可选地, 在本发明实施例中, 该转发设备为服务商边缘 PE 设备, 该转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例, 该转发设备上还包括第二 CE 设备的路由信息, 且该第一 CE 设备的 VPN 实例的 VPN 路由表中不包括该第二 CE 设备的路由信息, 该第三 CE 设备的 VPN 实例的 VPN 路由表中包括该第二 CE 设备的路由信息, 该处理器 510 用于, 获取 VPN 服务请求, 该 VPN 服务请求用于请求该第一 CE 设备访问该第二 CE 设备; 根据该 VPN 服务请求, 获取该第一资源需要关联该第二资源的需求, 该第一资源为源 IP 地址为该第一 CE 设备的 IP 地址、且目的 IP 地址为该第二 CE 设备的 IP 地址, 该第二资源为该第三 CE 设备的 VPN 实例; 该发送器 550 用于, 根据该需求, 向该转发设备发送该 BGP Flow Spec 协议报文, 该 BGP Flow Spec 协议报文中的该 Flags 字段用于指示在转发平面上关联该第一资源与该第二资源, 该 BGP Flow Spec 协议报文用

于指示将源 IP 地址、目的 IP 地址与该第一资源相一致的数据报文，按照该第三 CE 设备的 VPN 实例的 VPN 路由表中包括的该第二 CE 设备的路由信息进行转发。

可选地，在本发明实施例中，该第二 CE 设备为该第三 CE 设备。

5 应理解，在本发明实施例中，该处理器 510 可以是中央处理单元 (Central Processing Unit, 简称为“CPU”), 该处理器 510 还可以是其他通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现成可编程门阵列 (FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

10 该存储器 520 可以包括只读存储器和随机存取存储器，并向处理器 510 提供指令和数据。存储器 520 的一部分还可以包括非易失性随机存取存储器。例如，存储器 520 还可以存储设备类型的信息。

该总线系统 530 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统 530。

15 在实现过程中，上述方法的各步骤可以通过处理器 510 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本发明实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器、闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 520，处理器 510 读取存储器 520 中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

20 应理解，根据本发明实施例的控制器 500 可对应于本发明实施例的基于 Flow Spec 的通信方法中的控制器，以及可以对应于根据本发明实施例的控制器 300，并且控制器 500 中的各个模块的上述和其它操作和/或功能分别为了实现图 1 至图 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

25 如图 9 所示，本发明实施例还提供了一种转发设备 600，该转发设备 600 包括处理器 610、存储器 620、总线系统 630、接收器 640 和发送器 650。其中，处理器 610、存储器 620、接收器 640 和发送器 650 通过总线系统 630 相连，该存储器 620 用于存储指令，该处理器 610 用于执行该存储器 620 存储的指令，以控制接收器 640 接收信号，并控制发送器 650 发送信号。其中，接收器 640 用于接收控制器发送的边界网关协议流规则 BGP Flow Spec 协议报文，该 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，该网络层可达性信息字段携带用于指示该转发设备上的第一资源的该第一资源的特征信息，该扩展团体属性字段携带用于指示该转发设备上的第二资源的全局标识 GID，该 BGP Flow Spec 协议报文用于指示关联该第一资源与该第二资源；该处理器 610 用于，根据该第一资源的特征信息，获取该第一资源，根据该 GID，获取该第二资源；该转发设备关联该第一资源与该第二资源。

35 因此，在本发明实施例中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通道。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所

40

述第二资源，能够节省信令开销。

可选地，在本发明实施例中，该扩展团体属性字段包括GID字段与标志Flags字段，该GID字段携带该GID，该Flags字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联该第一资源与该第二资源的信息。

5 可选地，在本发明实施例中，该Flags字段包括转发平面比特位与控制平面比特位，当该转发平面比特位赋值为0、且该控制平面比特位赋值为1时，用于指示在该控制平面上关联该第一资源与该第二资源，当该转发平面比特位赋值为1、且该控制平面比特位赋值为0时，用于指示在该转发平面上关联该第一资源与该第二资源。

10 可选地，在本发明实施例中，该转发设备600为服务商边缘PE设备，该转发设备上建立有第一用户边缘CE设备的虚拟专用网VPN实例，该转发设备上包括第二CE设备的路由信息，且该第二CE设备的路由信息不在该第一CE设备的VPN实例的VPN路由表中，该接收器640用于，接收该控制器根据VPN服务请求发送的该BGP Flow Spec协议报文，该VPN服务请求用于请求该第一CE设备访问该第二CE设备，其中，该第一资源为该第二CE设备的路由信息，该第二资源为该第一CE设备的VPN实例，该BGP Flow Spec协议报文中
15 的该Flags字段用于指示在控制平面上关联该第一资源与该第二资源，该BGP Flow Spec协议报文用于指示将该第二CE设备的路由信息加入到该第一CE设备的VPN实例的VPN路由表中；

该处理器610用于，将该第二CE设备的路由信息加入到该第一CE设备的VPN实例的VPN路由表中。

20 可选地，在本发明实施例中，该发送器650用于，向该控制器发送该第一CE设备的VPN实例的属性信息，该属性信息包括：VPN实例名称、VPN实例路由标识符RD、VPN实例路由目标符RT、VPN实例索引值和VPN实例接口信息；该接收器640用于，接收该控制器发送的映射表，该映射表包括该第一CE设备的VPN实例的属性信息与该控制器为该第一CE设备的VPN实例的属性信息分配的映射标识之间的映射关系，该映射标识在该转发设备
25 中唯一指示该第一CE设备的VPN实例的属性信息，该GID字段中携带的该GID为该映射标识中的一个或多个标识。

可选地，在本发明实施例中，该转发设备600上建立有该第二CE设备的VPN实例，该第二CE设备的VPN实例的VPN路由表中包括该第二CE设备的路由信息；

30 该第一资源的特征信息为该第二CE设备的VPN实例的下列属性信息中的至少一种信息：VPN实例名称、VPN实例RD、VPN实例索引值、VPN实例接口信息、VPN实例GID；

该处理器610用于，根据该第一资源的特征信息，从该第二CE设备的VPN实例的VPN路由表中获取该第二CE设备的路由信息。

可选地，在本发明实施例中，该转发设备600上没有建立该第二CE设备的VPN实例，该转发设备的VPN公网路由表中包括该第二CE设备的路由信息；

35 该第一资源的特征信息为下列信息中的至少一种：该第二CE设备的路由信息对应的RD信息、出口目标Export Target信息或路由前缀信息；

该处理器610用于，根据该第一资源的特征信息，从该VPN公网路由表中获取该第二CE设备的路由信息。

40 可选地，在本发明实施例中，该转发设备600为服务商边缘PE设备，该转发设备上建立有第一用户边缘CE设备的虚拟专用网VPN实例和第三CE设备的VPN实例，该转发设

备上还包括第二 CE 设备的路由信息，且该第一 CE 设备的 VPN 实例的 VPN 路由表中不包括该第二 CE 设备的路由信息，该第三 CE 设备的 VPN 实例的 VPN 路由表中包括该第二 CE 设备的路由信息，该接收器 640 用于，接收该控制器根据 VPN 服务请求发送的 BGP Flow Spec 协议报文，该 VPN 服务请求用于请求该第一 CE 设备访问该第二 CE 设备，其中，该第一资源为源 IP 地址为该第一 CE 设备的 IP 地址、且目的 IP 地址为该第二 CE 设备的 IP 地址，该第二资源为该第三 CE 设备的 VPN 实例，该 BGP Flow Spec 协议报文中的该 Flags 字段用于指示在转发平面上关联该第一资源与该第二资源，该 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与该第一资源相一致的数据报文，按照该第三 CE 设备的 VPN 实例的 VPN 路由表中包括的该第二 CE 设备的路由信息进行转发；

该接收器 640 用于，接收数据报文，该数据报文的源 IP 地址为该第一 CE 设备的 IP 地址、且目的 IP 地址为该第二 CE 设备的 IP 地址；

该处理器 610 用于，按照该第三 CE 设备的 VPN 实例的 VPN 路由表中包括的该第二 CE 设备的路由信息转发该数据报文。

可选地，在本发明实施例中，该第二 CE 设备为该第三 CE 设备。

应理解，在本发明实施例中，该处理器 610 可以是中央处理单元 (Central Processing Unit, 简称为“CPU”)，该处理器 610 还可以是其他通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现成可编程门阵列 (FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

该存储器 620 可以包括只读存储器和随机存取存储器，并向处理器 610 提供指令和数据。存储器 620 的一部分还可以包括非易失性随机存取存储器。例如，存储器 620 还可以存储设备类型的信息。

该总线系统 630 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统 630。

在实现过程中，上述方法的各步骤可以通过处理器 610 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本发明实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 620，处理器 610 读取存储器 620 中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应理解，根据本发明实施例的转发设备 600 可对应于本发明实施例的基于 Flow Spec 的通信方法中的转发设备，以及可以对应于根据本发明实施例的转发设备 400，并且转发设备 600 中的各个模块的上述和其它操作和/或功能分别为了实现图 1 至图 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

如图 10 所示，本发明实施例还提出了一种基于流规则 Flow Spec 的通信系统 700，该通信系统 700 包括控制器 710 和转发设备 720，该控制器 710 对应于本发明实施例的控制器 300，该转发设备 720 对应于本发明实施例的转发设备 400。

因此，在本发明实施例中，通过在 BGP Flow Spec 协议报文的网络层可达性信息字段携带第一资源的特征信息，扩展团体属性字段中携带用于指示第二资源的全局标识 GID，能够指示转发设备关联所述第一资源与所述第二资源，以引导数据流进入相应的转发通

道。相对于传统技术，本申请中的 BGP FlowSpec 协议通过统一的报文格式，可以满足多种业务需求，从而能够有效避免无限制地扩展 BGP Flow Spec 协议中的扩展团体属性。此外，通过在 BGP FlowSpec 协议报文的扩展团体属性字段中携带简洁的 GID，就能够指示所述第二资源，能够节省信令开销。

5 还应理解，本文中涉及各种数字编号仅为描述方便进行的区分，并不用来限制本发明实施例的范围。

应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本发明实施例的实施过程构成任何限定。

10 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

15 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组
20 件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络
25 单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述通信方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介
35 质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

权利要求

1、一种基于流规则协议的通信方法，其特征在于，包括：

控制器获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求；

5 所述控制器根据所述需求，向所述转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文，所述 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，所述网络层可达性信息字段携带第一资源的特征信息，所述扩展团体属性字段携带用于指示所述第二资源的全局标识 GID，所述 BGP Flow Spec 协议报文用于指示关联所述第一资源与所述第二资源。

10 2、根据权利要求 1 所述的通信方法，其特征在于，所述扩展团体属性字段包括 GID 字段与标志 Flags 字段，所述 GID 字段携带所述 GID，所述 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联所述第一资源与所述第二资源的信息。

15 3、根据权利要求 2 所述的通信方法，其特征在于，所述 Flags 字段包括转发平面比特位与控制平面比特位，当所述转发平面比特位赋值为 0、且所述控制平面比特位赋值为 1 时，用于指示在所述控制平面上关联所述第一资源与所述第二资源，当所述转发平面比特位赋值为 1、且所述控制平面比特位赋值为 0 时，用于指示在所述转发平面上关联所述第一资源与所述第二资源。

20 4、根据权利要求 2 或 3 所述的通信方法，其特征在于，所述转发设备为服务商边缘 PE 设备，所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例，且所述第二 CE 设备的路由信息不在所述第一 CE 设备的 VPN 实例的 VPN 路由表中，所述通信方法还包括：

所述控制器获取 VPN 服务请求，所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备；

25 所述控制器获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求，包括：

所述控制器根据所述 VPN 请求，获取所述第一资源需要关联所述第二资源的需求，所述第一资源为所述第二 CE 设备的路由信息，所述第二资源为所述第一 CE 设备的 VPN 实例；

所述控制器根据所述需求，向所述转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文，包括：

30 所述控制器根据所述需求，向所述转发设备发送所述 BGP Flow Spec 协议报文，所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在控制平面上关联所述第一资源与所述第二资源，所述 BGP Flow Spec 协议报文用于指示将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中。

5、根据权利要求 4 所述的通信方法，其特征在于，所述通信方法还包括：

35 所述控制器从所述转发设备上获取所述第一 CE 设备的 VPN 实例的属性信息，所述属性信息包括：VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息；

所述控制器为所述第一 CE 设备的 VPN 实例的属性信息分配映射标识，所述映射标识在所述转发设备中唯一指示所述第一 CE 设备的 VPN 实例的属性信息；

所述控制器向所述转发设备发送映射表,所述映射表包括所述第一 CE 设备的 VPN 实例的属性信息与所述映射标识之间的映射关系,

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

6、根据权利要求 5 所述的通信方法,其特征在于,所述通信方法还包括:

5 所述控制器获取用于请求为所述转发设备上新建立的第三 CE 设备的 VPN 实例配置属性信息的 VPN 服务请求;

所述控制器为所述第三 CE 设备的 VPN 实例配置如下属性信息:VPN 实例名称、VPN 实例 RD、VPN 实例 RT 和 VPN 实例接口信息,其中,所述第三 CE 设备的 VPN 实例的下列属性信息与所述第一 CE 设备的 VPN 实例对应的属性信息互不冲突:VPN 实例名称、VPN 实例 RD、
10 VPN 实例接口信息。

7、根据权利要求 4 至 6 中任一项所述的通信方法,其特征在于,所述转发设备上建立有所述第二 CE 设备的 VPN 实例,所述第二 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息;

所述第一资源的特征信息为所述第二 CE 设备的 VPN 实例的下列属性信息中的至少一
15 种信息:VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID。

8、根据权利要求 4 至 6 中任一项所述的通信方法,其特征在于,所述转发设备上没有建立所述第二 CE 设备的 VPN 实例,所述转发设备的 VPN 公网路由表中包括所述第二 CE 设备的路由信息;

所述第一资源的特征信息为下列信息中的至少一种:所述第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息。

9、根据权利要求 2 或 3 所述的通信方法,其特征在于,所述转发设备为服务商边缘 PE 设备,所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例,且所述第一 CE 设备的 VPN 实例的 VPN 路由表中不包括所述第二 CE 设备的路由信息,所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息,
25 所述通信方法还包括:

所述控制器获取 VPN 服务请求,所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备;

所述控制器获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求,包括:

30 所述控制器根据所述 VPN 请求,获取所述第一资源需要关联所述第二资源的需求,所述第一资源为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址,所述第二资源为所述第三 CE 设备的 VPN 实例;

所述控制器根据所述需求,向所述转发设备发送 BGP Flow Spec 协议报文,包括:

所述控制器根据所述需求,向所述转发设备发送所述 BGP Flow Spec 协议报文,所述
35 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在转发平面上关联所述第一资源与所述第二资源,所述 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与所述第一资源相一致的数据报文,按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息进行转发。

10、根据权利要求 9 所述的通信方法,其特征在于,所述通信方法还包括:

40 所述控制器从所述转发设备上获取所述第三 CE 设备的 VPN 实例的属性信息,所述属

性信息包括: VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息;

所述控制器为所述第三 CE 设备的 VPN 实例的属性信息分配映射标识, 所述映射标识在所述转发设备中唯一指示所述第三 CE 设备的 VPN 实例的属性信息;

5 所述控制器向所述转发设备发送映射表, 所述映射表包括所述第三 CE 设备的 VPN 实例的属性信息与所述映射标识之间的映射关系,

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

11、根据权利要求 10 所述的通信方法, 其特征在于, 所述通信方法还包括:

10 所述控制器获取用于请求为所述转发设备上新建立的第四 CE 设备的 VPN 实例配置属性信息的 VPN 服务请求;

所述控制器为所述第四 CE 设备的 VPN 实例配置如下属性信息: VPN 实例名称、VPN 实例 RD、VPN 实例 RT 和 VPN 实例接口信息, 其中, 所述第四 CE 设备的 VPN 实例的下列属性信息与所述第一 CE 设备的 VPN 实例以及所述第三 CE 设备的 VPN 实例对应的属性信息互不冲突: VPN 实例名称、VPN 实例 RD、VPN 实例接口信息。

15 12、根据权利要求 9 至 11 中任一项所述的通信方法, 其特征在于, 所述第二 CE 设备为所述第三 CE 设备。

13、一种基于流规则协议的通信方法, 其特征在于, 包括:

20 转发设备接收控制器发送的边界网关协议流规则 BGP Flow Spec 协议报文, 所述 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段, 所述网络层可达性信息字段携带用于指示所述转发设备上的第一资源的所述第一资源的特征信息, 所述扩展团体属性字段携带用于指示所述转发设备上的第二资源的全局标识 GID, 所述 BGP Flow Spec 协议报文用于指示关联所述第一资源与所述第二资源;

所述转发设备根据所述第一资源的特征信息, 获取所述第一资源, 根据所述 GID, 获取所述第二资源;

25 所述转发设备关联所述第一资源与所述第二资源。

14、根据权利要求 13 所述的通信方法, 其特征在于, 所述扩展团体属性字段包括 GID 字段与标志 Flags 字段, 所述 GID 字段携带所述 GID, 所述 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联所述第一资源与所述第二资源的信息。

30 15、根据权利要求 14 所述的通信方法, 其特征在于, 所述 Flags 字段包括转发平面比特位与控制平面比特位, 当所述转发平面比特位赋值为 0、且所述控制平面比特位赋值为 1 时, 用于指示在所述控制平面上关联所述第一资源与所述第二资源, 当所述转发平面比特位赋值为 1、且所述控制平面比特位赋值为 0 时, 用于指示在所述转发平面上关联所述第一资源与所述第二资源。

35 16、根据权利要求 14 或 15 所述的通信方法, 其特征在于, 所述转发设备为服务商边缘 PE 设备, 所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例, 且所述第二 CE 设备的路由信息不在所述第一 CE 设备的 VPN 实例的 VPN 路由表中, 所述转发设备接收所述控制器发送的 BGP Flow Spec 协议报文, 包括:

40 所述转发设备接收所述控制器根据 VPN 服务请求发送的所述 BGP Flow Spec 协议报文, 所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备, 其中, 所述第一资源

为所述第二 CE 设备的路由信息, 所述第二资源为所述第一 CE 设备的 VPN 实例, 所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在控制平面上关联所述第一资源与所述第二资源, 所述 BGP Flow Spec 协议报文用于指示将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中;

5 所述转发设备关联所述第一资源与所述第二资源, 包括:

所述转发设备将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中。

17、根据权利要求 16 所述的通信方法, 其特征在于, 所述通信方法还包括:

10 所述转发设备向所述控制器发送所述第一 CE 设备的 VPN 实例的属性信息, 所述属性信息包括: VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息;

所述转发设备接收所述控制器发送的映射表, 所述映射表包括所述第一 CE 设备的 VPN 实例的属性信息与所述控制器为所述第一 CE 设备的 VPN 实例的属性信息分配的映射标识之间的映射关系, 所述映射标识在所述转发设备中唯一指示所述第一 CE 设备的 VPN 实例的属性信息,

15 所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

18、根据权利要求 16 或 17 所述的通信方法, 其特征在于, 所述转发设备上建立有所述第二 CE 设备的 VPN 实例, 所述第二 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息;

20 所述第一资源的特征信息为所述第二 CE 设备的 VPN 实例的下列属性信息中的至少一种信息: VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID;

所述转发设备根据所述第一资源的特征信息, 获取所述第一资源, 包括:

所述转发设备根据所述第一资源的特征信息, 从所述第二 CE 设备的 VPN 实例的 VPN 路由表中获取所述第二 CE 设备的路由信息。

25 19、根据权利要求 16 或 17 所述的通信方法, 其特征在于, 所述转发设备上没有建立所述第二 CE 设备的 VPN 实例, 所述转发设备的 VPN 公网路由表中包括所述第二 CE 设备的路由信息;

所述第一资源的特征信息为下列信息中的至少一种: 所述第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息;

30 所述转发设备根据所述第一资源的特征信息, 获取所述第一资源, 包括:

所述转发设备根据所述第一资源的特征信息, 从所述 VPN 公网路由表中获取所述第二 CE 设备的路由信息。

35 20、根据权利要求 14 或 15 所述的通信方法, 其特征在于, 所述转发设备为服务商边缘 PE 设备, 所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例, 且所述第一 CE 设备的 VPN 实例的 VPN 路由表中不包括所述第二 CE 设备的路由信息, 所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息, 所述转发设备接收所述控制器发送的 BGP Flow Spec 协议报文, 包括:

所述转发设备接收所述控制器根据 VPN 服务请求发送的 BGP Flow Spec 协议报文, 所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备, 其中, 所述第一资源为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址,

所述第二资源为所述第三 CE 设备的 VPN 实例,所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在转发平面上关联所述第一资源与所述第二资源,所述 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与所述第一资源相一致的数据报文,按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息进行转发;

5 所述转发设备关联所述第一资源与所述第二资源,包括:

所述转发设备接收数据报文,所述数据报文的源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址;

所述转发设备按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息转发所述数据报文。

10 21、根据权利要求 20 所述的通信方法,其特征在于,所述通信方法还包括:

所述转发设备向所述控制器发送所述第三 CE 设备的 VPN 实例的属性信息,所述属性信息包括:VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息;

15 所述转发设备接收所述控制器发送的映射表,所述映射表包括所述第三 CE 设备的 VPN 实例的属性信息与所述控制器为所述第三 CE 设备的 VPN 实例的属性信息分配的映射标识之间的映射关系,所述映射标识在所述转发设备中唯一指示所述第三 CE 设备的 VPN 实例的属性信息,

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

20 22、根据权利要求 20 或 21 所述的通信方法,其特征在于,所述第二 CE 设备为所述第三 CE 设备。

23、一种控制器,其特征在于,包括:

获取模块,用于获取转发设备上的第一资源需要关联所述转发设备上的第二资源的需求;

25 发送模块,用于根据所述获取模块获取的需求,向所述转发设备发送边界网关协议流规则 BGP Flow Spec 协议报文,所述 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段,所述网络层可达性信息字段携带第一资源的特征信息,所述扩展团体属性字段携带用于指示所述第二资源的全局标识 GID,所述 BGP Flow Spec 协议报文用于指示关联所述第一资源与所述第二资源。

30 24、根据权利要求 23 所述的控制器,其特征在于,所述扩展团体属性字段包括 GID 字段与标志 Flags 字段,所述 GID 字段携带所述 GID,所述 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联所述第一资源与所述第二资源的信息。

35 25、根据权利要求 24 所述的控制器,其特征在于,所述 Flags 字段包括转发平面比特位与控制平面比特位,当所述转发平面比特位赋值为 0、且所述控制平面比特位赋值为 1 时,用于指示在所述控制平面上关联所述第一资源与所述第二资源,当所述转发平面比特位赋值为 1、且所述控制平面比特位赋值为 0 时,用于指示在所述转发平面上关联所述第一资源与所述第二资源。

40 26、根据权利要求 24 或 25 所述的控制器,其特征在于,所述转发设备为服务商边缘 PE 设备,所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例,且所述第二 CE 设备的路由信息不在所述第一 CE 设备的 VPN 实例的 VPN 路由表中,所述获取模块用

于, 获取 VPN 服务请求, 所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备; 根据所述 VPN 服务请求, 获取所述第一资源需要关联所述第二资源的需求, 所述第一资源为所述第二 CE 设备的路由信息, 所述第二资源为所述第一 CE 设备的 VPN 实例;

所述发送模块用于, 根据所述需求, 向所述转发设备发送所述 BGP Flow Spec 协议报
5 文, 所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在控制平面上关联所述第一资源与所述第二资源, 所述 BGP Flow Spec 协议报文用于指示将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中。

27、根据权利要求 26 所述的控制器, 其特征在于,

所述获取模块还用于, 从所述转发设备上获取所述第一 CE 设备的 VPN 实例的属性信
10 息, 所述属性信息包括: VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息;

所述控制器还包括:

标识分配模块, 用于为所述第一 CE 设备的 VPN 实例的属性信息分配映射标识, 所述
映射标识在所述转发设备中唯一指示所述第一 CE 设备的 VPN 实例的属性信息;

15 所述发送模块还用于, 向所述转发设备发送映射表, 所述映射表包括所述第一 CE 设备的 VPN 实例的属性信息与所述映射标识之间的映射关系,

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

28、根据权利要求 27 所述的控制器, 其特征在于,

所述获取模块还用于, 获取用于请求为所述转发设备上新建立的第三 CE 设备的 VPN
20 实例配置属性信息的 VPN 服务请求;

所述控制器还包括:

VPN 实例配置模块, 用于为所述第三 CE 设备的 VPN 实例配置如下属性信息: VPN 实例
名称、VPN 实例 RD、VPN 实例 RT 和 VPN 实例接口信息, 其中, 所述第三 CE 设备的 VPN 实例的下列属性信息与所述第一 CE 设备的 VPN 实例对应的属性信息互不冲突: VPN 实例名称、
25 VPN 实例 RD、VPN 实例接口信息。

29、根据权利要求 26 至 28 中任一项所述的控制器, 其特征在于, 所述转发设备上建
立有所述第二 CE 设备的 VPN 实例, 所述第二 CE 设备的 VPN 实例的 VPN 路由表中包括所述
第二 CE 设备的路由信息;

所述第一资源的特征信息为所述第二 CE 设备的 VPN 实例的下列属性信息中的至少一
30 种信息: VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID。

30、根据权利要求 26 至 28 中任一项所述的控制器, 其特征在于, 所述转发设备上没
有建立所述第二 CE 设备的 VPN 实例, 所述转发设备的 VPN 公网路由表中包括所述第二 CE
设备的路由信息;

所述第一资源的特征信息为下列信息中的至少一种: 所述第二 CE 设备的路由信息对
35 应的 RD 信息、出口目标 Export Target 信息或路由前缀信息。

31、根据权利要求 24 或 25 所述的控制器, 其特征在于, 所述转发设备为服务商边缘
PE 设备, 所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设
备的 VPN 实例, 且所述第一 CE 设备的 VPN 实例的 VPN 路由表中不包括所述第二 CE 设备的
路由信息, 所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息,
40 所述获取模块用于, 获取 VPN 服务请求, 所述 VPN 服务请求用于请求所述第一 CE 设备访

问所述第二 CE 设备；根据所述 VPN 服务请求，获取所述第一资源需要关联所述第二资源的需求，所述第一资源为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址，所述第二资源为所述第三 CE 设备的 VPN 实例；

所述发送模块还用于，根据所述需求，向所述转发设备发送所述 BGP Flow Spec 协议报文，所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在转发平面上关联所述第一资源与所述第二资源，所述 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与所述第一资源相一致的数据报文，按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息进行转发。

32、根据权利要求 31 所述的控制器，其特征在于，所述第二 CE 设备为所述第三 CE 设备。

33、一种转发设备，其特征在于，包括：

接收模块，用于接收控制器发送的边界网关协议流规则 BGP Flow Spec 协议报文，所述 BGP Flow Spec 协议报文包括网络层可达性信息字段与扩展团体属性字段，所述网络层可达性信息字段携带用于指示所述转发设备上的第一资源的所述第一资源的特征信息，所述扩展团体属性字段携带用于指示所述转发设备上的第二资源的全局标识 GID，所述 BGP Flow Spec 协议报文用于指示关联所述第一资源与所述第二资源；

获取模块，用于根据所述接收模块接收的所述第一资源的特征信息，获取所述第一资源，根据所述 GID，获取所述第二资源；

关联模块，用于根据所述接收模块接收的所述 BGP Flow Spec 协议报文，关联所述第一资源与所述第二资源。

34、根据权利要求 33 所述的转发设备，其特征在于，所述扩展团体属性字段包括 GID 字段与标志 Flags 字段，所述 GID 字段携带所述 GID，所述 Flags 字段携带用于指示在所述转发设备的控制平面或所述转发设备的转发平面上关联所述第一资源与所述第二资源的信息。

35、根据权利要求 34 所述的转发设备，其特征在于，所述 Flags 字段包括转发平面比特位与控制平面比特位，当所述转发平面比特位赋值为 0、且所述控制平面比特位赋值为 1 时，用于指示在所述控制平面上关联所述第一资源与所述第二资源，当所述转发平面比特位赋值为 1、且所述控制平面比特位赋值为 0 时，用于指示在所述转发平面上关联所述第一资源与所述第二资源。

36、根据权利要求 34 或 35 所述的转发设备，其特征在于，所述转发设备为服务商边缘 PE 设备，所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例，且所述第二 CE 设备的路由信息不在所述第一 CE 设备的 VPN 实例的 VPN 路由表中，所述接收模块用于，接收所述控制器根据 VPN 服务请求发送的所述 BGP Flow Spec 协议报文，所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备，其中，所述第一资源为所述第二 CE 设备的路由信息，所述第二资源为所述第一 CE 设备的 VPN 实例，所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在控制平面上关联所述第一资源与所述第二资源，所述 BGP Flow Spec 协议报文用于指示将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中；

所述关联模块，用于将所述第二 CE 设备的路由信息加入到所述第一 CE 设备的 VPN 实例的 VPN 路由表中。

37、根据权利要求 36 所述的转发设备，其特征在于，所述转发设备还包括：

发送模块，用于向所述控制器发送所述第一 CE 设备的 VPN 实例的属性信息，所述属性信息包括：VPN 实例名称、VPN 实例路由标识符 RD、VPN 实例路由目标符 RT、VPN 实例索引值和 VPN 实例接口信息；

5 所述接收模块用于，接收所述控制器发送的映射表，所述映射表包括所述第一 CE 设备的 VPN 实例的属性信息与所述控制器为所述第一 CE 设备的 VPN 实例的属性信息分配的映射标识之间的映射关系，所述映射标识在所述转发设备中唯一指示所述第一 CE 设备的 VPN 实例的属性信息，

所述 GID 字段中携带的所述 GID 为所述映射标识中的一个或多个标识。

10 38、根据权利要求 36 或 37 所述的转发设备，其特征在于，所述转发设备上建立有所述第二 CE 设备的 VPN 实例，所述第二 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息；

所述第一资源的特征信息为所述第二 CE 设备的 VPN 实例的下列属性信息中的至少一种信息：VPN 实例名称、VPN 实例 RD、VPN 实例索引值、VPN 实例接口信息、VPN 实例 GID；

15 所述获取模块用于，根据所述第一资源的特征信息，从所述第二 CE 设备的 VPN 实例的 VPN 路由表中获取所述第二 CE 设备的路由信息。

39、根据权利要求 36 或 37 所述的转发设备，其特征在于，所述转发设备上没有建立所述第二 CE 设备的 VPN 实例，所述转发设备的 VPN 公网路由表中包括所述第二 CE 设备的路由信息；

20 所述第一资源的特征信息为下列信息中的至少一种：所述第二 CE 设备的路由信息对应的 RD 信息、出口目标 Export Target 信息或路由前缀信息；

所述获取模块用于，根据所述第一资源的特征信息，从所述 VPN 公网路由表中获取所述第二 CE 设备的路由信息。

40、根据权利要求 34 或 35 所述的转发设备，其特征在于，所述转发设备为服务商边缘 PE 设备，所述转发设备上建立有第一用户边缘 CE 设备的虚拟专用网 VPN 实例和第三 CE 设备的 VPN 实例，且所述第一 CE 设备的 VPN 实例的 VPN 路由表中不包括所述第二 CE 设备的路由信息，所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括所述第二 CE 设备的路由信息，所述接收模块用于，接收所述控制器根据 VPN 服务请求发送的 BGP Flow Spec 协议报文，所述 VPN 服务请求用于请求所述第一 CE 设备访问所述第二 CE 设备，其中，所述第一资源为源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址，所述第二资源为所述第三 CE 设备的 VPN 实例，所述 BGP Flow Spec 协议报文中的所述 Flags 字段用于指示在转发平面上关联所述第一资源与所述第二资源，所述 BGP Flow Spec 协议报文用于指示将源 IP 地址、目的 IP 地址与所述第一资源相一致的数据报文，按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息进行转发；

所述关联模块包括：

接收单元，用于接收数据报文，所述数据报文的源 IP 地址为所述第一 CE 设备的 IP 地址、且目的 IP 地址为所述第二 CE 设备的 IP 地址；

40 转发单元，用于按照所述第三 CE 设备的 VPN 实例的 VPN 路由表中包括的所述第二 CE 设备的路由信息转发所述数据报文。

41、根据权利要求 40 所述的转发设备，其特征在于，所述第二 CE 设备为所述第三 CE 设备。

42、一种基于流规则 Flow Spec 协议的通信系统，该通信系统包括如上述要求 23 至 32 中任一项所述的控制器与如上述权利要求 33 至 41 中任一项所述的转发设备。

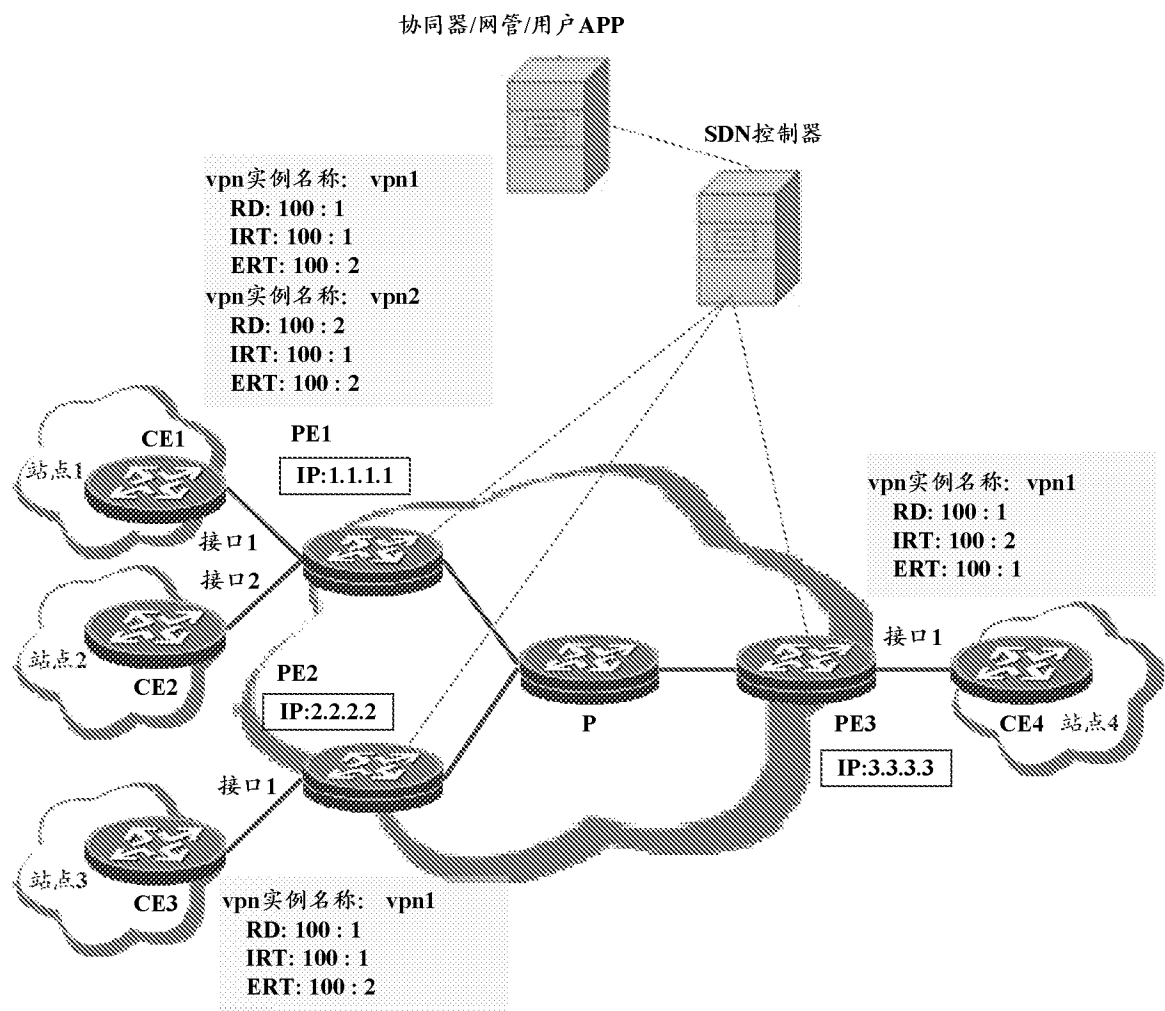


图 1

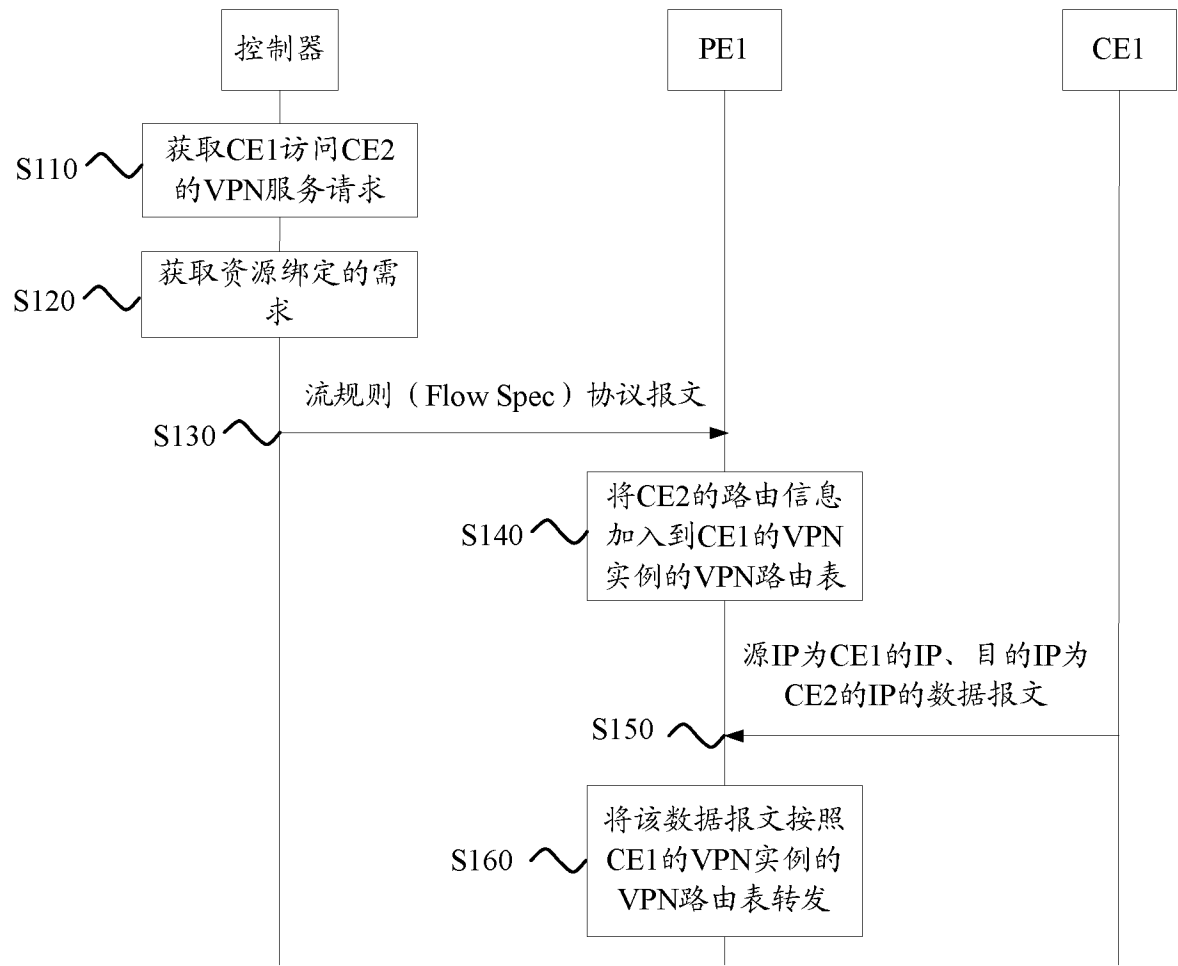


图 2

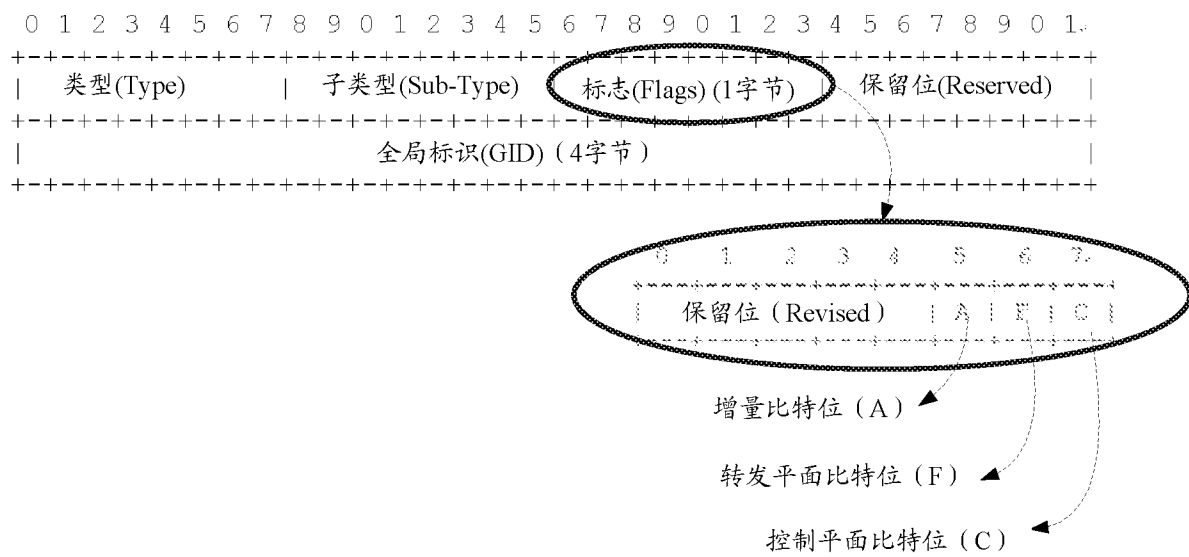


图 3

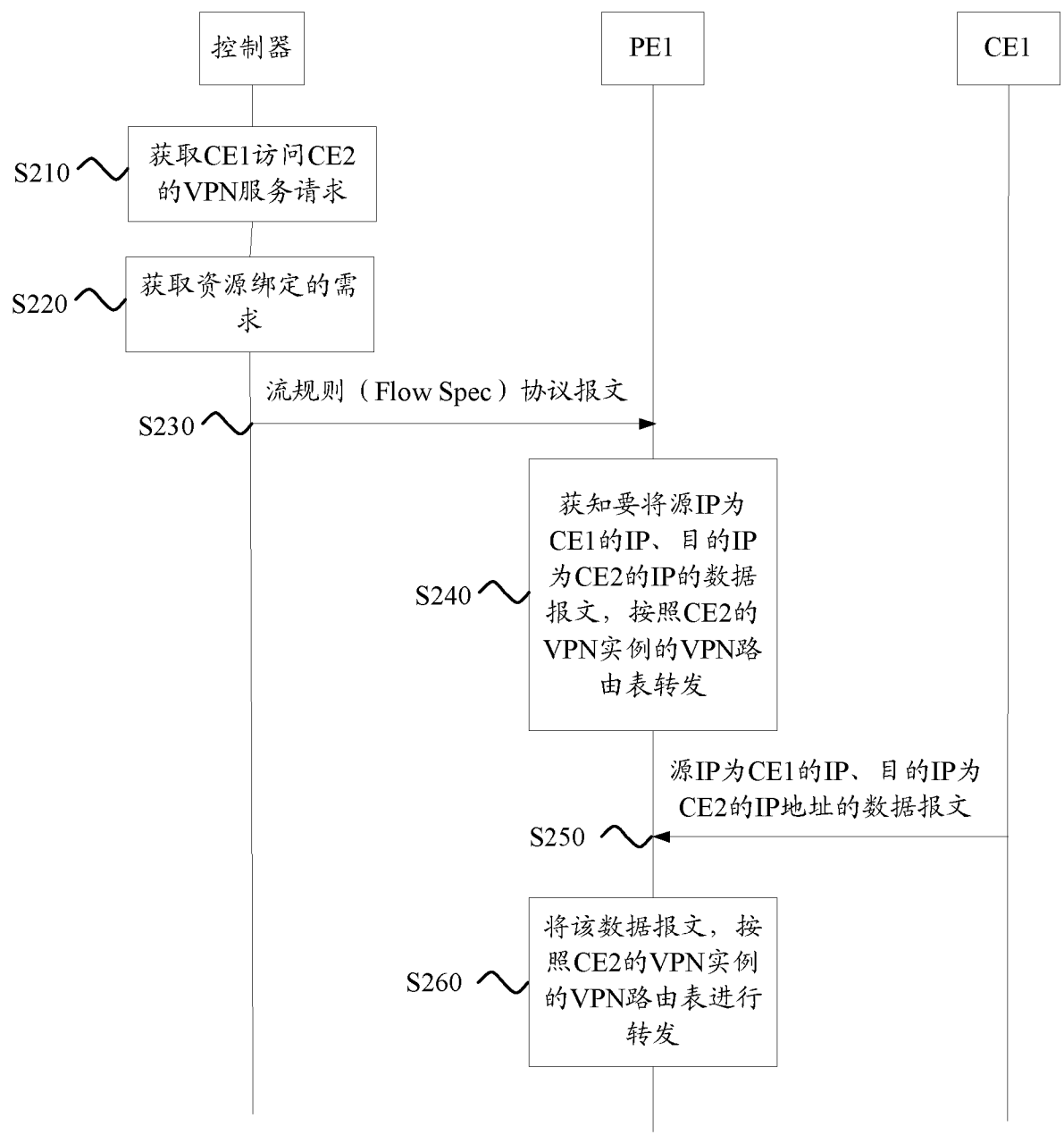


图 4

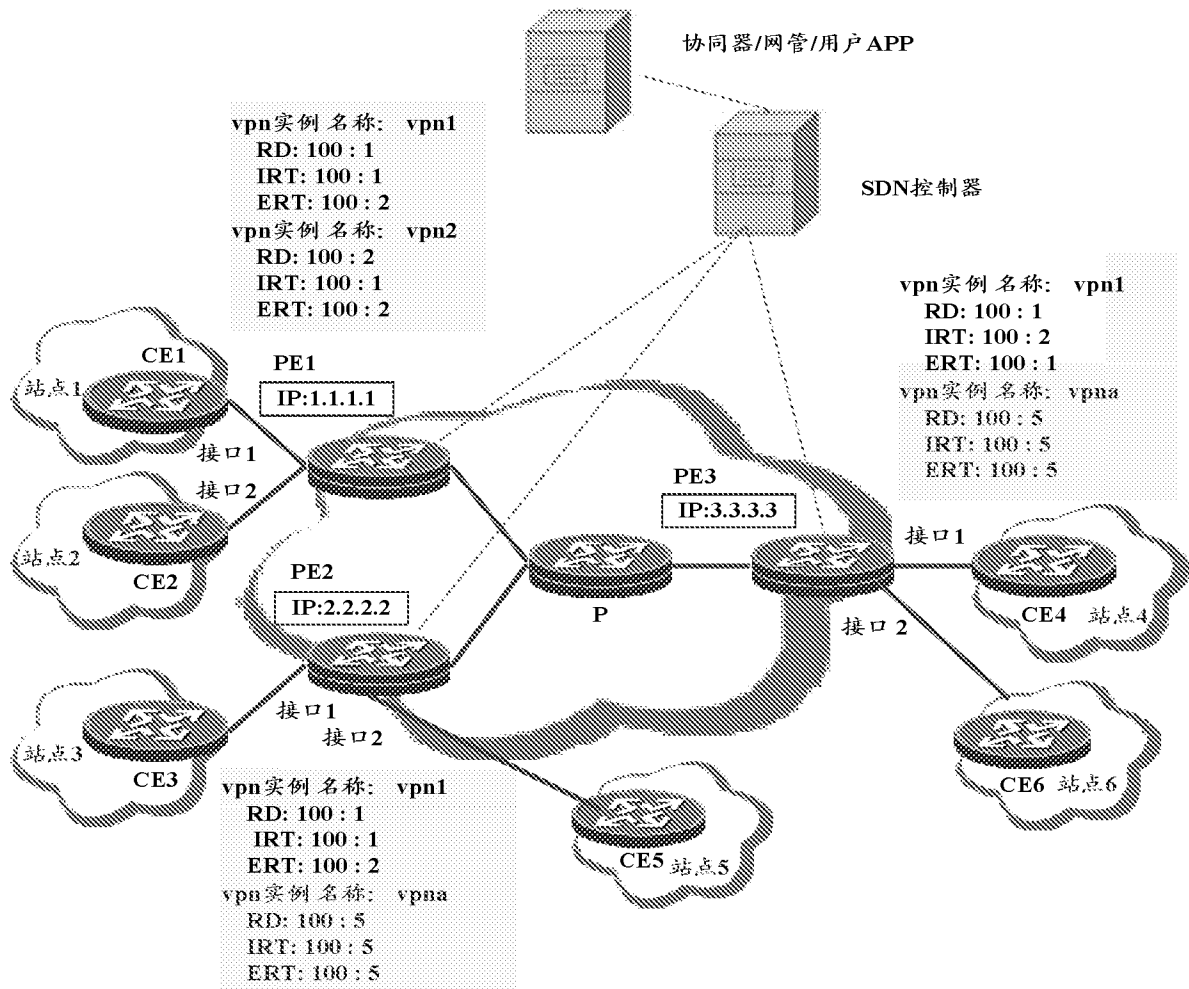


图 5

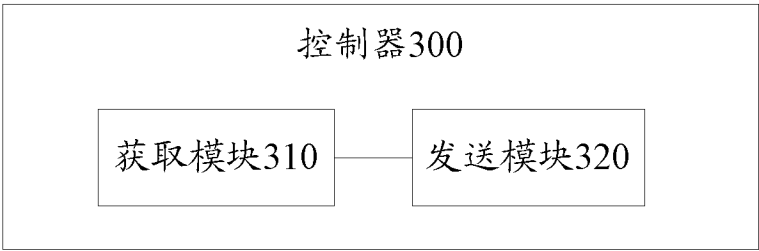


图 6



图 7

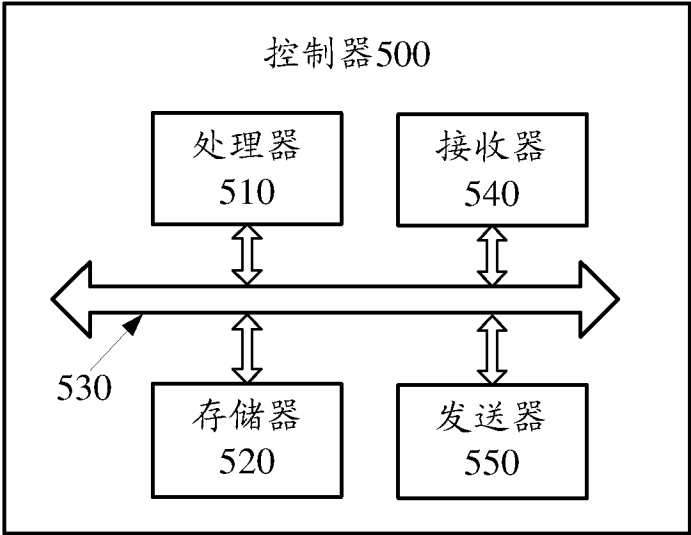


图 8

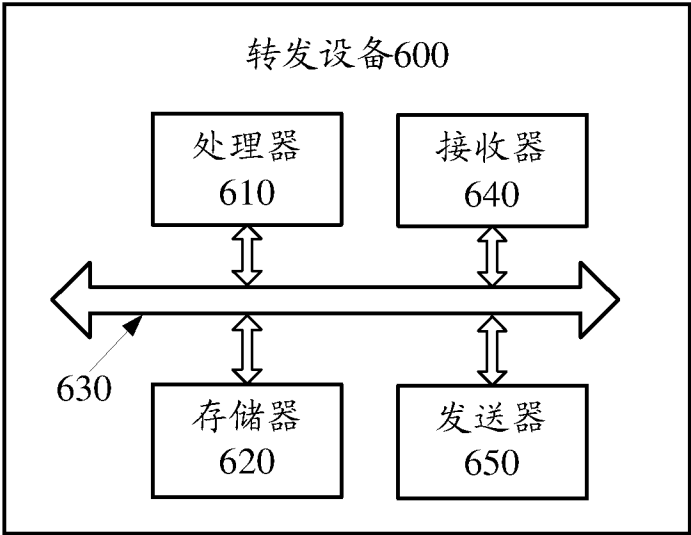


图 9

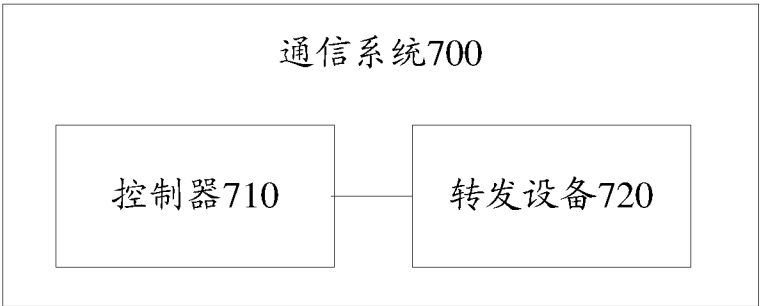


图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/076960

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, GOOGLE: BGP, VPN, GID, extend, community, attribute, reachability, information, VRF, router, stream, protocol, map, identify, global, accessibility, group, embodiment, device, forward, demand

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103684959 A (HUAWEI TECHNOLOGIES CO., LTD.) 26 March 2014 (26.03.2014) description, paragraphs [0070]-[0094]	1-42
A	CN 104468348 A (MAIPU COMMUNICATION TECHNOLOGY CO., LTD.) 25 March 2015 (25.03.2015) the whole document	1-42
A	CN 103731347 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 16 April 2014 (16.04.2014) the whole document	1-42
A	WO 2008089305 A2 (NORTEL NETWORKS LIMITED) 24 July 2008 (24.07.2008) the whole document	1-42

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 22 May 2107	Date of mailing of the international search report 14 June 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Ren Telephone No. (86-10) 62413242

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/076960

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103684959 A	26 March 2014	EP 2890060 A1	01 July 2015
		US 2015195105 A1	09 July 2015
		WO 2014044151 A1	27 March 2014
CN 104468348 A	25 March 2015	None	
CN 103731347 A	16 April 2014	None	
WO 2008089305 A2	24 July 2008	CA 2674201 A1	24 July 2008
		US 2012008630 A1	12 January 2012
		US 2008170573 A1	17 July 2008
		CN 101636724 A	27 January 2010
		CN 103840998 A	04 June 2014
		US 2014153578 A1	05 June 2014
		EP 2104897 A2	30 September 2009

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNKI, CNPAT, WPI, EPDOC, GOOGLE: 流, 协议, 边界网关, 需求, 路由, 转发, 设备, 虚拟, 实例, 扩展, 团体, 可达, 信息, 全局, 标识, 映射, BGP, VPN, GID, extended, community, attribute, reachability, information, VRF, router		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 103684959 A (华为技术有限公司) 2014年 3月 26日 (2014 - 03 - 26) 说明书第[0070]-[0094]段	1-42
A	CN 104468348 A (迈普通信技术股份有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文	1-42
A	CN 103731347 A (杭州华三通信技术有限公司) 2014年 4月 16日 (2014 - 04 - 16) 全文	1-42
A	WO 2008089305 A2 (NORTEL NETWORKS LIMITED) 2008年 7月 24日 (2008 - 07 - 24) 全文	1-42
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2107年 5月 22日		国际检索报告邮寄日期 2017年 6月 14日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 李韧 电话号码 (86-10)62413242

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/076960

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103684959	A	2014年 3月 26日	EP	2890060	A1	2015年 7月 1日
				US	2015195105	A1	2015年 7月 9日
				WO	2014044151	A1	2014年 3月 27日
CN	104468348	A	2015年 3月 25日	无			
CN	103731347	A	2014年 4月 16日	无			
WO	2008089305	A2	2008年 7月 24日	CA	2674201	A1	2008年 7月 24日
				US	2012008630	A1	2012年 1月 12日
				US	2008170573	A1	2008年 7月 17日
				CN	101636724	A	2010年 1月 27日
				CN	103840998	A	2014年 6月 4日
				US	2014153578	A1	2014年 6月 5日
				EP	2104897	A2	2009年 9月 30日