(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
2020 年 1 月 2 日 (02.01.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/001388 A1

(51) 国际专利分类号:
H04L 12/741 (2013.01)

(21) 国际申请号: PCT/CN2019/092443

(22) 国际申请日: 2019 年 6 月 23 日 (23.06.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810703112.1 2018年6月30日 (30.06.2018) 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: 高 远 (**GAO, Yuan**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 王 海 波 (**WANG, Haibo**); 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, JO, 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:** METHOD FOR SENDING BGP MESSAGE, METHOD FOR RECEIVING BGP MESSAGE, AND DEVICE

(54) 发明名称: 发送BGP消息的方法、接收BGP消息的方法以及设备

图 2

S201 A first network device determines that a host identified by a first MAC address is an attacker

S202 The first network device generates a BGP message

S203 The first network device sends the BGP message to a second network device

(57) **Abstract:** The present application provides a method for sending a BGP message. The method comprises: a first network device determining that a host identified by a first MAC address is an attacker; the first network device generating a BGP message, the BGP message comprising the first MAC address and indication information, the indication information being used to indicate that the host identified by the first MAC address is the attacker; and the first network device sending the BGP message to a second network device. In addition, further provided are another method and a device. The technical solutions above help to reduce the workload of an engineer performing manual configuration on a network device.

(57) **摘要**: 本申请提供了一种发送BGP消息的方法。该方法包括：第一网络设备确定第一MAC地址所标识的主机为攻击者。所述第一网络设备生成BGP消息，所述BGP消息包括所述第一MAC地址以及指示信息，所述指示信息用于指示所述第一MAC地址标识的的所述主机是所述攻击者。所述第一网络设备向第二网络设备发送所述BGP消息。此外，还提供了其他方法以及设备。上述技术方案中有助于减小工程师在网络设备上进行手工配置的工作量。

WO 2020/001388 A1

说 明 书

发送BGP消息的方法、接收BGP消息的方法以及设备

本申请要求于2018年06月30日提交中国国家知识产权局、申请号为201810703112.1、申请名称为“发送BGP消息的方法、接收BGP消息的方法以及设备”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。

技术领域

本申请涉及通信技术领域，尤其涉及一种发送边界网关协议（Border Gateway Protocol，BGP）消息的方法、接BGP消息的方法以及相关设备。

背景技术

网络设备可以连接多个主机。例如，网络设备可以是交换机。网络设备接收到来自主机的报文时，网络设备可以对报文进行转发。所述多个主机中可能包含了攻击者。例如，主机1是攻击者。工程师可以在网络设备上手工配置关于主机1的转发规则。所述转发规则包含了主机1的媒体访问控制（media access control，MAC）地址。例如，MAC地址具有48个比特。当网络设备检测到所述网络设备接收的报文的源MAC地址是主机1的MAC地址时，网络设备可以根据所述转发规则丢弃该报文。

上述技术方案中，工程师需要手工配置关于攻击者的转发规则，手工配置的工作量比较大。

发明内容

本申请提供了一种发送BGP消息的方法、接收BGP消息的方法以及相关设备。有助于降低手工配置的工作量。

本申请提供了如下技术方案。

第一方面，提供了一种发送BGP消息的方法。该方法包括：第一网络设备确定第一媒体访问控制MAC地址所标识的主机为攻击者。所述第一网络设备生成BGP消息，所述BGP消息包括所述第一MAC地址以及指示信息，所述指示信息用于指示所述第一MAC地址标识的的所述主机是所述攻击者。所述第一网络设备向第二网络设备发送所述BGP消息。

上述技术方案中，第一网络设备确定第一MAC地址所标识的主机为攻击者后，第一网络设备可以生成携带所述第一MAC地址以及指示信息的BGP消息，并向第二网络设备发送所述BGP消息。进而，第二网络设备可以根据BGP消息中的第一MAC地址以及指示信息，生成用于阻止第二网络设备向所述第一MAC地址标识的所述主机转发第二网络设备接收到的报文的转发规则。也就是说，第二网络设备可以利用第一网络设备发送的BGP消息生成转发规则，工程师不需要在第二网络设备上手工配置所述转发规则。因此，上述技术方案有助于减小工程师在网络设备上进行手工配置的工作量。

在一种可能的设计中，所述第一网络设备包括第一VTEP，所述第二网络设备包括

第二 VTEP。所述第一网络设备向第二网络设备发送所述 BGP 消息包括：所述第一 VTEP 向所述第二 VTEP 发送所述 BGP 消息。

上述技术方案中，可以利用 VTEP 实现 BGP 消息的传输。

在一种可能的设计中，第一 VTEP 地址标识所述第一 VTEP，第二 VTEP 地址标识所述第二 VTEP，所述 BGP 消息包括网际协议（internet protocol，IP）头以及净荷，所述 IP 头包括目的 IP 地址，所述净荷包括 MP_REACH_NLRI，所述 MP_REACH_NLRI 包括下一跳网络地址，所述目的 IP 地址等于所述第二 VTEP 地址，所述下一跳网络地址等于所述第一 VTEP 地址。

在一种可能的设计中，所述第一 VTEP 经由隧道向所述第二 VTEP 发送所述 BGP 消息，所述隧道是 VXLAN 隧道，或者 LSP。

在一种可能的设计中，所述第一网络设备生成 BGP 消息包括：所述第一网络设备确定 MAC 地址为所述第一 MAC 地址的主机是攻击者。所述第一网络设备接收数据报文，所述数据报文的源 MAC 地址为所述第一 MAC 地址。所述第一网络设备基于所述数据报文的源 MAC 地址标识的主机是攻击者，生成所述 BGP 消息。

上述技术方案中，所述第一网络设备基于所述数据报文的触发而生成所述 BGP 消息。也就是说，当第一网络设备确定第一 MAC 地址所标识的主机为攻击者时，所述第一网络设备不是必须立即生成 BGP 消息，并通知第二网络设备。当第一网络设备确定第一 MAC 地址所标识的主机为攻击者时，第一 MAC 地址所标识的主机可能并没有接入第一网络设备所管辖的网络。例如，第一 MAC 地址所标识的主机可能已下线，或者第一 MAC 地址所标识的主机可能已漫游到其他网络。因此，当第一网络设备确定第一 MAC 地址所标识的主机为攻击者时，第一网络设备和第二网络设备可能并没有遭到所述攻击者的攻击。在第一网络设备没有遭到所述攻击者攻击的情况下，第一网络设备暂时不生成以及发送 BGP 消息，有助于降低第一网络设备和第二网络设备的开销。当第一网络设备接收到源 MAC 地址为所述第一 MAC 地址的数据报文时，表明第一网络设备开始受到所述攻击者的攻击。第一网络设备开始受到所述攻击者的攻击时，第一网络设备通知第二网络设备所述攻击者的 MAC 地址，有助于获得降低开销和阻止攻击者的攻击的折中。

在一种可能的设计中，所述第一网络设备基于所述数据报文的源 MAC 地址标识的主机是攻击者，生成所述 BGP 消息，包括：所述第一网络设备确定所述数据报文来自第一 VXLAN，第一虚拟扩展局域网网络标识 VNI 标识所述第一 VXLAN。所述第一网络设备基于所述数据报文携带的源 MAC 地址，以及所述数据报文来自第一 VXLAN，确定所述第一 MAC 地址标识的主机位于所述第一 VXLAN。所述第一网络设备基于所述数据报文来自第一 VXLAN，生成所述 BGP 消息，所述 BGP 消息包括所述第一 VNI。

在一种可能的设计中，所述第一网络设备确定所述数据报文来自第一 VXLAN，包括：所述第一网络设备经由第一端口接收所述数据报文，所述第一端口配置了所述第一 VNI。所述第一网络设备基于用于接收所述数据报文的所述第一端口配置了所述第一 VNI，确定所述数据报文来自所述第一 VXLAN。

在一种可能的设计中，所述第一网络设备确定所述数据报文来自第一 VXLAN，包括：所述第一网络设备确定所述数据报文中包含的第一虚拟局域网标识 VLAN ID 配置

了所述第一 VNI。所述第一网络设备基于所述数据报文包含的所述第一 VLAN ID 配置了所述第一 VNI，确定所述数据报文来自所述第一 VXLAN。

第二方面，提供了一种接收 BGP 消息的方法。该方法包括：第二网络设备接收来自第一网络设备的 BGP 消息，所述 BGP 消息包括第一 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址所标识的主机是攻击者。所述第二网络设备接收第一报文，所述第一报文的目的 MAC 地址等于所述第一 MAC 地址。所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

在一种可能的设计中，所述第二网络设备接收第二报文，所述第二报文的源 MAC 地址等于所述第一 MAC 地址。所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第二报文中的所述源 MAC 地址，避免转发所述第二报文。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。所述第二网络设备接收来自第一网络设备的 BGP 消息包括：所述第二 VTEP 接收来自所述第一 VTEP 的所述路由信息。

在一种可能的设计中，所述第二 VTEP 接收来自所述第二 VTEP 的 BGP update 消息，所述 BGP 消息携带在所述 BGP update 消息中，所述 BGP update 消息包括 IP 头以及净荷，所述 IP 头包括目的 IP 地址，所述净荷包括 MP_REACH_NLRI，所述 MP_REACH_NLRI 包括下一跳网络地址，所述目的 IP 地址等于所述第二 VTEP 地址，所述下一跳网络地址等于所述第一 VTEP 地址。

在一种可能的设计中，所述第二 VTEP 经由隧道接收来自所述第二 VTEP 的所述 BGP update 消息，所述隧道是 VXLAN 隧道或者 LSP。

第三方面，提供了一种第一网络设备。所述第一网络设备包括处理器以及与所述处理器耦合的收发器。所述处理器用于确定第一 MAC 地址所标识的主机为攻击者。所述处理器还用于生成边界网关协议 BGP 消息，所述 BGP 消息包括所述第一 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址标识的的所述主机是所述攻击者。所述收发器用于向第二网络设备发送所述处理器生成的所述 BGP 消息。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。所述收发器用于向所述第二 VTEP 发送来自所述第一 VTEP 的所述 BGP 消息。

第四方面，提供了一种第二网络设备。所述第二网络设备包括第一收发器、第二收发器以及与所述第一收发器和所述第二收发器耦合的处理器。所述第一收发器用于接收来自第一网络设备的边界网关协议 BGP 消息，所述 BGP 消息包括第一媒体访问控制 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址所标识的主机是攻击者。所述第二收发器用于接收第一报文，所述第一报文的目的 MAC 地址等于所述第一 MAC 地址。所述处理器用于基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

在一种可能的设计中，所述第二收发器还用于接收第二报文，所述第二报文的源

MAC 地址等于所述第一 MAC 地址。所述处理器还用于基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第二报文中的所述源 MAC 地址，避免转发所述第二报文。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。所述第一收发器用于向所述第二 VTEP 发送来自所述第一 VTEP 的所述 BGP 消息。

第五方面，提供了一种系统。所述系统包括第三方面提供的第一网络设备以及第四方面提供第二网络设备。

第六方面，提供了一种计算机可读存储介质。所述计算机可读存储介质存储计算机程序。当所述计算机程序被网络设备执行时，使得网络设备执行第一方面提供的方法，或者第二方面提供的方法。举例来说，所述网络设备可以是第一方面涉及的第一网络设备，或者第二方面涉及的第二网络设备。

第七方面，提供了一种计算机程序产品。所述计算机程序产品包含计算机程序。所述计算机程序可以保存在计算机可读存储介质上。当所述计算机程序被网络设备执行时，使得网络设备执行第一方面提供的方法，或者第二方面提供的方法。举例来说，所述网络设备可以是第一方面涉及的第一网络设备，或者第二方面涉及的第二网络设备。

在第一方面至第七方面的一种可能的设计中，所述 BGP 消息包含 MAC/IP Advertisement route 以及 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

上述技术方案中，可以利用 IETF 已定义的 EVPN 路由消息发布攻击者的 MAC 地址。有助于使得本申请提供的技术方案兼容已有的网络，降低实现成本。

进一步地，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜（flags），所述指示信息携带在所述旗帜的最高有效位（most significant bit，MSB）上。

上述技术方案中，利用了 IETF 已定义的 EVPN 路由消息中的字段携带所述指示信息，有助于使得本申请提供的技术方案兼容已有的网络，降低实现成本。

在第一方面至第七方面的一种可能的设计中，所述 BGP 消息为 BGP 更新（update）消息。

附图说明

图 1 为本申请提供的一种数据中心网络的结构示意图；

图 1a 为本申请提供的一种交换机的结构示意图；

图 1b 为本申请提供的一种服务器的结构示意图；

图 2 为本申请提供的一种发送 BGP 消息的方法的流程示意图；

图 3 为本申请提供的一种接收 BGP 消息的方法的流程示意图；

图 4 为本申请提供的一种第一网络设备的结构示意图；

图 5 为本申请提供的一种第二网络设备的结构示意图；

图 6 为本申请提供的一种系统的结构示意图。

具体实施方式

图 1 为本申请提供的一种数据中心网络的结构示意图。参见图 1，数据中心网络包括服务器 1 至服务器 6、叶子交换机（leaf switch，LS）1、LS1、LS3 以及脊柱交换机（spine switch，SS）1、SS2 以及 SS3。其中，服务器 1 和服务器 2 连接到 LS1。服务器 3 和服务器 4 连接到 LS2。服务器 5 和服务器 6 连接到 LS3。LS1 连接到 SS1、SS2 以及 SS3。LS2 连接到 SS1、SS2 以及 SS3。LS3 连接到 SS1、SS2 以及 SS3。服务器 1 需要经由 LS1 与其他服务器进行通信。服务器 6 需要经由 LS3 与其他服务器进行通信。服务器 1 与服务器 6 进行通信时，服务器 1 发送的数据流可以经由不同的路径到达服务器 6。不同的路径包括：路径 1（LS1-SS1-LS3）、路径 2（LS1-SS2-LS3）以及路径 3（LS1-SS3-LS3）。

图 1a 为本申请提供的一种交换机的结构示意图。图 1 中的 LS 可以是交换机 100。图 1 中的 SS 可以是交换机 100。关于图 1 中的 LS 和 SS 的具体实现方式，可以参见本申请对交换机 100 的描述。

参见图 1a，交换机 100 包括端口 a 至端口 f、网络处理器 110、存储器 120、流量管理器 130 以及存储器 140。端口 a、端口 b 以及端口 c 与网络处理器 110 耦合。端口 a、端口 b 以及端口 c 为发送端口，可以将接收到的报文发送至网络处理器 110。交换机 100 可以包含更多或者更少的接收端口。端口 d、端口 e 以及端口 f 与流量管理器 130 耦合。网络处理器 110 和存储器 120 耦合。存储器 120 中可以保存计算机程序以及转发表。所述转发表可以是哈希表。网络处理器 110 可以通过执行存储器 120 中保存的计算机程序和/或查找转发表，对来自接收端口的报文进行处理。例如，网络处理器 110 可以通过执行计算机程序，对报文中的哈希键执行哈希运算，从而获得哈希值。再例如，网络处理器 110 可以通过查找哈希表，确定与哈希值匹配的表项。根据与哈希值匹配的表项，确定用于转发报文的发送端口。所述发送端口可以是端口 d、端口 e 或者端口 f。网络处理器 110 和流量管理器 130 耦合。流量管理器 130 与存储器 140 耦合。例如，网络处理器 110 确定用于转发报文的发送端口后，可以将报文发送至流量管理器 130。流量管理器 130 也可以称为调度器。流量管理器 130 中可以维护与端口 d、端口 e 以及端口 f 一一对应的三个发送缓存队列。流量管理器 130 接收到来自网络处理器 110 的报文后，可以根据用于转发报文的发送端口，将报文入队到与用于转发报文的发送端口对应的发送缓存队列。流量管理器 130 可以对位于发送缓存队列中的报文进行调度，从而通过发送端口发送报文。具体地，流量管理器 130 中可以维护与所述三个发送缓存队列一一对应的三个报文描述符队列。报文描述符队列中包含多个报文描述符。每个报文描述符包含报文存储在发送缓存队列中的地址。当流量管理器 130 需要将报文入队到发送缓存队列时，流量管理器 130 可以在报文描述符队列中增加该报文的存储地址。流量管理器 130 可以对存储器 140 执行写操作，从而将报文入队到发送缓存队列。当流量管理器 130 需要将报文从发送缓存队列出队时，流量管理器 130 可以将报文描述符队列中该报文的存储地址删除。流量管理器 130 可以对存储器 140 执行读操作，从而将报文从发送缓存队列出队。报文出队后，报文经由发送端口被发送。

需要说明的是，图 1a 所示的交换机可以包括控制平面以及转发平面。所述控制平面

可以用于路由学习，路由发布，生成转发规则，以及更新转发平面的转发表。所述转发平面可以用于根据转发表，对报文进行转发。所述转发平面可以包括网络处理器 110、存储器 120、流量管理器 130 以及存储器 140。所述控制平面可以包括中央处理单元（central processing unit，CPU）以及与所述中央处理单元耦合的存储器。所述与中央处理单元耦合的存储器中可以保存用于运行网络协议的计算机程序。所述网络协议可以是 BGP。所述中央处理单元可以通过执行所述计算机程序，实现 BGP 定义的功能。例如，所述中央处理单元可以学习服务器的 MAC 地址。可以基于服务器的 MAC 地址，生成路由消息。可以向远端交换机发送路由消息。另外，交换机接收到来自远端交换机的路由消息后，可以根据来自远端交换机的路由消息更新转发平面的转发表。例如，来自远端交换机的路由消息中包含远端服务器的 MAC 地址。所述中央处理单元可以在转发表中增加关于远端服务器的表项。因此，当服务器接收目的 MAC 地址为远端服务器的 MAC 地址的报文时，交换机的转发平面可以根据关于远端服务器的表项，对该报文进行转发。

图 1b 为本申请提供的一种服务器的结构示意图。图 1 中的服务器可以是服务器 1000。关于图 1 中的服务器的具体实现方式，可以参见本申请对服务器 1000 的描述。

参见图 1b，服务器 1000 包括中央处理单元 1100、存储器 1200、端口 1300 以及总线。处理单元 1100、存储器 1200 以及端口 1300 通过所述总线耦合。存储器 1200 存储软件。所述软件包含操作系统以及多个应用程序。中央处理单元 1100 通过访问存储器 1200 运行所述操作系统以及所述多个应用程序。所述操作系统可以是 Window 或者 Linux。基于所述操作系统，中央处理单元 1100 运行所述多个应用程序。端口 1300 可以用于接收报文以及发送报文。例如，当端口 1300 接收到来自交换机 100 的报文后，存储器 1200 可以保存报文。中央处理单元 1100 可以根据应用程序对报文进行处理。另外，中央处理单元 1100 可以根据应用程序生成报文，并经由端口 1300 将报文发送至交换机 100。

另外，图 1b 中的中央处理单元 1100 可以被替换为其他的处理器。所述其他处理器可以是数字信号处理器（digital signal processor，DSP）、专用集成电路（application-specific integrated circuit，ASIC）、现场可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本发明实施例公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等。

图 1 所示的数据中心网络具体可以是以太网虚拟专用网络（Ethernet Virtual Private Network，EVPN）。关于 EVPN，可以参见因特网工程任务组（英文：Internet Engineering Task Force，缩写：IETF）发布的请求评论（英文：Request For Comments，缩写：RFC）7432 的说明，所述 RFC7432 以全文引用的方式并入本申请中。如无相反的说明，本申请提及的以“RFC”开头的文档，都是 IETF 发布的。例如 RFC7348 也是 IETF 发布的。

例如，LS1 和 LS2 可以运行 RFC7348。具体地，LS1 和 LS2 可以分别包含一个虚拟扩展局域网隧道端点（VXLAN Tunnel End Point，VTEP）。VTEP 是用于创建（originate）和/或终结（terminate）VXLAN 隧道的实体。关于 VTEP，可以参考 RFC7348 中的相关描述。本申请中将 LS1 中包含的 VTEP 称为 VTEP1，将 LS2 中包含的 VTEP 称为 VTEP2。

VTEP1 对应 VTEP IP 地址 1。VTEP2 对应 VTEP IP 地址 2。工程师可以对 LS1 进行手工配置，从而使得 LS1 包含 VTEP1。工程师可以对 LS2 进行手工配置，从而使得 LS2 包含 VTEP2。例如，工程师可以进行如下配置：在 LS1 上配置 VTEP IP 地址 1（例如 1.1.1.9）。另外，LS1 和 LS2 可以位于同一个 VXLAN。例如，LS1 和 LS2 都位于虚拟扩展局域网网络标识（VXLAN Network Identifier，VNI）指示的 VXLAN。VNI 的值可以是 100。工程师可以在 LS1 上配置 VNI（例如 100）。在 LS1 上配置 RD（例如 1:1）。在 LS1 上配置 RT（例如 1:1）。在 LS2 上配置 VTEP IP 地址 2（例如 2.2.2.9）。在 LS2 上配置 VNI（例如 100）。另外，工程师可以在 LS2 上配置 LS1 和 LS2 之间的 VXLAN 隧道。例如，工程师在 LS2 上配置所述 VXLAN 隧道的信息。所述信息可以包括源 IP 地址（例如 2.2.2.9）以及目的 IP 地址（例如 1.1.1.9）。源 IP 地址为沿着 LS2 到 LS1 的方向，所述 VXLAN 隧道的入口节点（例如 VTEP2）的 IP 地址。目的 IP 地址为沿着 LS2 到 LS1 的方向，所述 VXLAN 隧道的出口节点（例如 VTEP1）的 IP 地址。工程师在 LS1 上配置所述 VXLAN 隧道的信息。所述信息可以包括隧道类型（TunnelType）。例如，当 TunnelType 的值等于 8 时，TunnelType 指示所述 VXLAN 隧道的隧道类型为 VXLAN。在一种可能的设计中，所述 VXLAN 隧道可以经过 SS1、SS2 以及 SS3 中的至少一个。也就是说，SS1、SS2 以及 SS3 中的至少一个可以所述 VXLAN 隧道的中间节点。

LS1 运行 BGP。LS2 运行 BGP。具体地，LS1 包含处理器以及存储器。存储器中保存实现 BGP 的功能的代码。LS1 中的处理器（例如中央处理单元）通过执行所述代码运行 BGP。LS2 也可以通过上述机制运行 BGP。LS2 是 LS1 的 BGP peer。也可以将 LS1 和 LS2 称为一对 BGP peer。LS1 可以学习 LS1 所管辖的网络中的服务器的 MAC 地址。例如，LS1 可以学习服务器 1 的 MAC 地址以及服务器 2 的 MAC 地址。LS2 可以学习 LS2 所管辖的网络中的服务器的 MAC 地址。例如，LS2 可以学习服务器 3 的 MAC 地址以及服务器 4 的 MAC 地址。LS1 可以经由所述 VXLAN 隧道向 LS2 发送 EVPN 路由。LS1 发送的 EVPN 路由可以包括服务器 1 的 MAC 地址以及服务器 2 的 MAC 地址。LS2 可以经由所述 VXLAN 隧道向 LS1 发送 EVPN 路由。LS2 发送的 EVPN 路由可以包括服务器 3 的 MAC 地址以及服务器 4 的 MAC 地址。

下文对 LS1 学习服务器 1 的 MAC 地址，并向 LS2 发送携带服务器 1 的 MAC 地址的 EVPN 路由进行举例说明。

LS1 包含接口 1。接口 1 为以太网接口。LS1 经由接口 1 连接服务器 1。工程师在 LS1 上配置了与接口 1 关联的 VNI（例如 100）。服务器 1 生成以太网帧 1 并经由接口 1 向 LS1 发送以太网帧 1。以太网帧 1 的源 MAC 地址为服务器 1 的 MAC 地址。LS1 经由接口 1 接收到以太网帧 1 后，确定接收以太网帧 1 的接口为接口 1。进而，LS1 确定与接口 1 管理的 VNI 的值等于 100。另外，LS1 对以太网帧 1 进行解析，从而获取服务器 1 的 MAC 地址。LS1 基于 RFC7432，根据 LS1 保存的配置信息，以及 LS1 从以太网帧 1 中获取的信息，生成路由消息 1。具体地，LS1 中的处理器（例如中央处理单元）可以通过执行实现 BGP 的功能的代码生成路由消息 1。下面对路由消息 1 进行举例说明：

具体地，路由消息 1 可以携带在 IP 报文中。所述 IP 报文包括 IP 头以及 IP 净荷。IP 头与 IP 净荷相邻。IP 净荷位于 IP 头的后面。IP 头包括源 IP 地址、目的 IP 地址以及协议（protocol）。源 IP 地址的值可以等于 VTEP IP 地址 1（例如 1.1.1.9）。

目的 IP 地址的值可以等于 VTEP IP 地址 2（例如 2.2.2.9）。IP 头中的协议用于指示 IP 头的下一个头的类型。例如，当协议的值等于 6 时，IP 头中的协议指示 IP 报文中，IP 头的下一个头是传输控制协议（Transmission Control Protocol，TCP）头。IP 净荷包括 TCP 头以及 TCP 净荷。TCP 头与 TCP 净荷相邻。TCP 净荷位于 TCP 头的后面。TCP 头与 IP 头相邻。TCP 头包括源端口（source port）。TCP 头中的源端口可以用于指示 TCP 净荷的类型。例如，当源端口的值等于 179 时，TCP 头中的源端口指示 TCP 净荷是 BGP 消息。

路由消息 1 可以是 BGP 消息。具体地，可以是 BGP update 消息。路由消息 1 可以包括多协议可达网络层可达信息（Multiprotocol Reachable Network Layer Reachability Information，MP_REACH_NLRI）。所述 MP_REACH_NLRI 是一种路径属性（path attribute）。关于 MP_REACH_NLRI，可以参考 RFC4760 中的相关描述。路由消息 1 还可以携带其他路径属性。例如，路由消息 1 还可以携带本地偏好（local preference）。所述 MP_REACH_NLRI 包括下一跳网络地址（next hop network address）字段。所述下一跳网络地址字段可以携带 LS1 上保存的 VTEP IP 地址 1（例如 1.1.1.9）。

路由消息 1 包含媒体访问控制/网际协议通告路由（MAC/IP Advertisement route）。关于 MAC/IP Advertisement route，可以参考 RFC7432 中的相关描述。此外，路由消息还可以包括媒体访问控制移动性扩展团体（MAC Mobility Extended Community）。关于 MAC Mobility Extended Community，可以参考 RFC7432 中的相关描述。

服务器 1 的 MAC 地址可以携带在所述 MAC/IP Advertisement route 中。具体地，所述 MAC/IP Advertisement route 包括 MAC 地址字段。所述 MAC 地址字段具有 6 个字节。服务器 1 的 MAC 地址可以携带在所述 MAC 地址字段。所述 MAC/IP Advertisement route 包括多协议标签交换标签（MPLS Label）1 字段。MPLS Label 1 字段具有 3 个字节。MPLS Label 1 字段可以携带 LS1 上保存的 VNI（例如 100）。所述 MAC/IP Advertisement route 包括 RD 字段。所述 RD 字段包括 8 个字节。所述 RD 字段可以携带 LS1 上保存的 RD（例如 1:1）。此外，所述 MAC/IP Advertisement route 还包括 MPLS Label 2 字段。此外，路由消息 1 中可以包括扩展团体属性（Extended Communities Attribute）。关于扩展团体属性，可以参考 RFC4360 中对 BGP Extended Communities Attribute 的描述。具体地，扩展团体属性可以包括 TunnelType 字段以及 RT 字段。TunnelType 字段可以携带 LS1 上保存的 TunnelType（例如 8）。RT 字段可以携带 LS1 上保存的 RT（例如 1:1）。

LS1 生成路由消息 1 后，可以通过所述 VXLAN 隧道向 LS2 发送路由消息 1。

LS2 接收到路由消息 1 后，对路由消息 1 进行解析，获得路由消息 1 中的下一跳网络地址字段的值。所述下一跳网络地址字段的值等于 VTEP IP 地址 1（例如 1.1.1.9）。LS2 根据从路由消息 1 中获取的所述下一跳网络地址字段的值，以及 LS2 保存的所述 VXLAN 隧道的信息，确定 LS2 能够通过所述 VXLAN 隧道向 LS1 发送目的地址为服务器 1 的 MAC 地址的以太网帧。所述信息包括源 IP 地址（例如 2.2.2.9）以及目的 IP 地址（例如 1.1.1.9）。具体地，LS2 根据所述下一跳网络地址字段的值等于所述 VXLAN 隧道的目的 IP 地址，确定路由消息 1 与所述 VXLAN 隧道是匹配的。进而，LS2 可以生成转发表项。所述转发表项包括 MAC 地址（例如服务器 1 的 MAC 地址）、VNI（例如

100）、源 IP 地址（例如 2.2.2.9）以及目的 IP 地址（例如 1.1.1.9）。

下文对 LS2 如何利用所述转发表项对以太网帧进行转发进行举例说明。

当 LS2 接收到目的 MAC 地址为服务器 1 的 MAC 地址的以太网帧（以太网帧 2）时，可以基于以太网帧 2 中的目的 MAC 地址等于转发表项中的 MAC 地址，确定以太网帧 2 与转发表项匹配。进而，LS2 可以对以太网帧 2 进行封装，得到封装的报文。具体地，LS2 可以为以太网帧 2 添加隧道头。所述隧道头可以包括源 IP 地址（例如 2.2.2.9）、目的 IP 地址（例如 1.1.1.9）以及 VNI（例如 100）。LS2 可以从所述转发表项中获取隧道头中的字段的值，从而实现对以太网帧 2 的封装。LS2 生成封装的报文后，可以经由所述 VXLAN 隧道向 LS1 发送所述封装的报文。在上述的举例中，LS1 和 LS2 之间的隧道为 VXLAN 隧道。可替换的，LS1 和 LS2 之间的隧道也可以是其他隧道。例如，LS1 和 LS2 之间的隧道可以是段路由流量工程（Segment Routing Traffic Engineering，SR-TE）路径。

上述的举例中描述了 LS1 学习服务器 1 的 MAC 地址，并通过路由消息向 LS2 发送服务器 1 的 MAC 地址。图 1 中的任意一个 LS 可以按照类似的方式学习该 LS 所管辖的网络中的服务器的 MAC 地址，并通过路由消息向远端的 LS 发送服务器的 MAC 地址。例如，LS3 和 LS2 之间可以存在一个 VXLAN 隧道。LS3 可以学习服务器 5 的 MAC 地址。然后，LS3 可以经由 LS3 和 LS2 之间的 VXLAN 隧道向 LS2 发送携带服务器 5 的 MAC 地址的路由消息。

上述举例中，图 1 中的 LS 和 SS 为交换机。可替换的，图 1 中的 LS 和 SS 也可以是其他网络设备。例如，图 1 中的 LS 和 SS 可以为路由器。在一种可能的设计中，LS 和 SS 可以是运营商边缘（provider edge，PE）路由器。PE 路由器位于核心网（core network）的边缘。PE 路由器可以用于连接 CE 路由器。在另一种可能的设计中，LS 可以是 PE 路由器。SS 可以是运营商（provider，P）路由器。P 路由器是一种标签交换路由器（Label Switch Router，LSR）。P 路由器是核心网中的传输路由器（transit router）。P 路由器可以用于连接的一个或者多个 PE 路由器。图 1a 为交换机的结构示意图。图 1a 也可以是其他网络设备的结构示意图。例如，图 1a 也可以是路由器的结构示意图。

上述举例中，图 1 中的 LS 用于连接服务器。在一种的可能的设计中，LS 可以通过电缆或者光缆直接连接服务器。在另一种可能的设计中，LS 可以经由中间设备间接连接服务器。所述中间设备可以是路由器、以太网交换机或者网关。可替换的，图 1 中的 LS 可以连接其他类型的主机。其他类型的主机可以是个人电脑或者虚拟机（virtual machine，VM）。所述虚拟机可以运行在物理服务器中。在一种可能的设计中，LS 可以经由接入设备连接到所述物理服务器。所述接入设备可以是网关或者以太网交换机。图 1b 是服务器的结构示意图。图 1b 也可以是其他主机的结构示意图。例如，图 1b 也可以是个人电脑的结构示意图。上述实施例以图 1 中的服务器 1 是合法用户为前提。LS1 学习了作为合法用户的服务器 1 的 MAC 地址后，会将包含服务器 1 的 MAC 地址的路由消息发送给 LS2。LS2 根据路由消息生成转发表项，从而使得 LS2 管辖的网络中的服务器（例如服务器 3）能够利用转发表项和服务器 1 进行通信。

在一种可能的场景中，图 1 中的服务器 1 是非法用户。具体地，服务器 1 可以是

攻击者。例如，服务器 1 可能会发起网络攻击（cyberattack）。所述网络攻击可以是拒绝服务（denial-of-service，DDoS）攻击、中间人（man in the middle）攻击、地址解析协议毒害（ARP poisoning）、乒泛洪（Ping flood）、窃听（wiretapping）、空闲扫描（idle scan）或者端口扫描（port scan）。

下文以所述网络攻击为 DDoS 攻击为例，对服务器 1 的攻击行为以及 LS1 识别服务器 1 为攻击者的过程进行说明：

在一种可能的设计中，服务器 1 的使用者在知晓某个软件能够发起 DDoS 攻击的情况下，在服务器 1 中安装并运行了该软件。服务器 1 在该软件的控制下，发送了多个报文，从而发起 DDoS 攻击。LS1 具有识别 DDoS 攻击的能力。例如，LS1 中包含了处理器和存储器。存储器中保存了用于识别 DDoS 攻击的计算机程序。LS1 接收到所述多个报文。LS1 中的处理器通过执行所述计算机程序，对所述多个报文的特征进行分析，从而确定服务器 1 是攻击者。进一步地，LS1 通过对所述多个报文的源 MAC 地址进行解析获得服务器 1 的 MAC 地址（例如 MAC 地址 1）。LS1 确定 MAC 地址 1 所标识的主机（例如服务器 1）是攻击者。

在另一种可能的设计中，由于使用者的误操作，服务器 1 被感染了计算机病毒。该计算机病毒能够发起 DDoS 攻击。服务器 1 中预先安装，并运行有计算机病毒监测软件。该计算机病毒监测软件对该计算机病毒（服务器 1 中的一个进程）的行为进行识别，确定服务器 1 被感染了计算机病毒。进一步地，服务器 1 在计算机病毒监测软件的控制下，确定服务器 1 是攻击者。服务器 1 向网管服务器（图 1 中未示出）发送消息 1。消息 1 用于通知网管服务器服务器 1 是攻击者。例如，消息 1 中携带服务器 1 的 MAC 地址（例如 MAC 地址 1）。网管服务器根据消息 1 确定服务器 1 是攻击者后，生成消息 2。网管服务器向 LS1 发送消息 2。消息 2 用于通知 LS1 服务器 1 是攻击者。例如，消息 2 中携带 MAC 地址 1。LS1 接收到消息 2 后，根据消息 2 中携带的 MAC 地址 1 确定 MAC 地址 1 标识的主机（例如服务器 1）是攻击者。

LS1 确定 MAC 地址 1 标识的主机（例如服务器 1）是攻击者后，LS1 生成路由消息 2。LS1 中的处理器（例如中央处理单元）可以通过执行实现 BGP 的功能的代码生成路由消息 2。路由消息 2 包含 MAC 地址 1 以及指示信息 1。指示信息 1 用于指示 MAC 地址 1 标识的主机（例如服务器 1）为攻击者。LS1 向 LS2 发送路由消息 2。LS1 可以根据 LS1 保存的配置信息，以及服务器 1 的 MAC 地址，生成路由消息 2。关于 LS1 基于服务器 1 的 MAC 地址，生成路由消息 2 的过程，可以参考上文关于路由消息 1 的生成过程的描述。MAC 地址 1 可以携带在路由消息 2 包含的 MAC/IP Advertisement route 中。具体地，MAC 地址 1 可以携带在 MAC/IP Advertisement route 的 MAC 地址字段上。关于路由消息 2 的格式，可以参考上文对路由消息 1 的格式的描述。

需要说明的是，路由消息 1 是 LS1 确定服务器 1 是合法用户时生成的。LS1 向 LS2 通告服务器 1 的 MAC 地址，使得 LS2 生成转发表项。进而，LS2 管辖的服务器（例如服务器 3）可以经由 LS2 和服务器 1 通信。路由消息 2 是 LS1 确定服务器 1 是攻击者时生成的。LS1 向 LS2 通告服务器 1 的 MAC 地址，使得 LS2 生成转发规则。进而，LS2 管辖的服务器（例如服务器 3）避免经由 LS2 和服务器 1 通信。

路由消息 2 的功能不同于路由消息 1。路由消息 2 的内容不同于路由消息 1 的内

容。具体地，路由消息 2 中包含了用于指示 MAC 地址 1 标识的主机（例如服务器 1）为攻击者的指示信息 1。路由消息 1 中不包含指示信息 1。在一种可能的设计中，指示信息 1 携带在路由消息 2 中的 MAC Mobility Extended Community 中。MAC Mobility Extended Community 包含旗帜（flags）字段。旗帜字段具有 8 个比特。指示信息 1 可以携带在旗帜字段的 MSB。例如，当旗帜字段的 MSB 等于 1 时，旗帜字段的 MSB 指示路由消息 2 中的 MAC 地址 1 标识的主机（例如服务器 1）为攻击者。

LS2 接收来自 LS1 的路由消息 2 后，LS2 可以根据路由消息 2 生成转发规则 1 以及转发规则 2。LS2 根据转发规则 1，避免向 MAC 地址 1 标识的主机（例如服务器 1）转发 LS2 收到的目的 MAC 地址为 MAC 地址 1 的报文。LS2 根据转发规则 2，避免转发 LS2 收到的源 MAC 地址为 MAC 地址 1 的报文。

转发规则 1 具体可以是转发表项 1。转发规则 2 具体可以是转发表项 2。LS2 的转发平面可以包括转发表。所述转发表可以包括转发表项 1 以及转发表项 2。所述转发平面的处理器（例如网络处理器）可以根据转发表，对接收到的报文进行处理。

转发表项 1 包括匹配域以及动作域。转发表项 1 的匹配域的值等于 MAC 地址 1。转发表项 1 的动作域可以包括丢弃指令。转发表项 1 的匹配域用于与 LS2 接收到的报文（例如报文 1）中的目的 MAC 地址进行匹配。当 LS2 确定报文 1 的目的 MAC 地址等于转发表项 1 的匹配域的值时，LS2 确定报文 1 与转发表项 1 匹配。进而，LS2 可以根据转发表项 1 的动作域的丢弃指令，对报文 1 进行丢弃处理。当然，转发表项 1 的动作域可以包括其他指令。其他指令可以指示将报文 1 发送至 LS2 的控制平面。所述控制平面的处理器可以是 CPU。所述 CPU 收到来自转发平面的报文 1 后，可以对报文 1 进行分析。另外，LS2 在所述 CPU 的控制下，还可以将报文 1 发送至网管服务器，以便网管服务器对报文 1 进行分析。LS2 遵循转发规则 1 对报文 1 进行处理时，并不是意味着 LS2 只能对报文 1 进行丢弃处理，LS2 也可以对报文 1 进行其他处理。只要 LS2 避免向 MAC 地址 1 标识的主机（例如服务器 1）转发报文 1 即可。

转发表项 2 包括匹配域以及动作域。转发表项 2 的匹配域的值等于 MAC 地址 1。转发表项 2 的动作域可以包括丢弃指令。转发表项 2 的匹配域用于与 LS2 接收到的报文（例如报文 2）中的源 MAC 地址进行匹配。当 LS2 确定报文 2 的源 MAC 地址等于转发表项 2 的匹配域的值时，LS2 确定报文 2 与转发表项 2 匹配。进而，LS2 可以根据转发表项 2 的动作域的丢弃指令，对报文 2 进行丢弃处理。可以理解，LS2 接收到报文 2 的源 MAC 地址等于 MAC 地址 1，可能是由于服务器 1 从 LS1 管辖的网络漫游到 LS2 管辖的网络。另一种可能是，LS2 管辖的网络中的主机盗用了服务器 1 的 MAC 地址。例如，服务器 4 构造以太网帧时，盗用了服务器 1 的 MAC 地址，将服务器 1 的 MAC 地址作为构造的以太网帧的源 MAC 地址。

图 2 为本申请提供的一种发送 BGP 消息的方法的流程示意图。图 2 所示的方法的执行主体为第一网络设备。例如，所述第一网络设备可以是图 1 中的 LS1。关于所述第一网络设备的结构和功能，可以参考上述实施例关于 LS1 的结构和功能的描述。所述第一网络设备可以执行上述实施例描述的 LS1 执行的动作。关于图 2 所示的方法的具体实现方式，可以参考上述实施例的相关描述。参见图 2，所述方法包括 S201、S202 以及 S203。

S201、第一网络设备确定第一 MAC 地址所标识的主机为攻击者。

举例来说，所述第一 MAC 地址可以是 MAC 地址 1。第一 MAC 地址所标识的主机可以是服务器 1。

S202、所述第一网络设备生成 BGP 消息。

所述 BGP 消息包括所述第一 MAC 地址以及指示信息。所述指示信息用于指示所述第一 MAC 地址标识的的所述主机是所述攻击者。

例如，所述 BGP 消息可以是路由消息 2。所述指示信息可以是指示信息 1。

S203、所述第一网络设备向第二网络设备发送所述 BGP 消息。

例如，所述第二网络设备可以是 LS2。LS1 可以经由 LS1 与 LS2 之间的 VXLAN 隧道向 LS2 发送所述 BGP 消息。

上述技术方案中，第一网络设备确定第一 MAC 地址所标识的主机为攻击者后，第一网络设备可以生成携带所述第一 MAC 地址以及指示信息的 BGP 消息，并向第二网络设备发送所述 BGP 消息。进而，第二网络设备可以根据 BGP 消息中的第一 MAC 地址以及指示信息，生成用于阻止第二网络设备向所述第一 MAC 地址标识的所述主机转发第二网络设备接收到的报文的转发规则。也就是说，第二网络设备可以利用第一网络设备发送的 BGP 消息生成转发规则，工程师不需要在第二网络设备上手工配置所述转发规则。因此，上述技术方案有助于减小工程师在网络设备上进行手工配置的工作量。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。

所述第一网络设备向第二网络设备发送所述 BGP 消息包括：所述第一 VTEP 向所述第二 VTEP 发送所述 BGP 消息。

举例来说，所述第一 VTEP 可以是 VTEP1。所述第二 VTEP 可以是 VTEP2。VTEP1 可以包含 LS1 的发送接口。所述发送接口可以是以太网接口。VTEP2 可以包含 LS2 的接收接口。所述接收接口可以是以太网接口。VTEP1 可以经由 LS1 和 LS2 之间的 VXLAN 隧道向 VTEP2 发送路由消息 2。

在一种可能的设计中，第一 VTEP 地址标识所述第一 VTEP，第二 VTEP 地址标识所述第二 VTEP。所述 BGP 消息包括 IP 头以及净荷。所述 IP 头包括目的 IP 地址，所述净荷包括 MP_REACH_NLRI。所述 MP_REACH_NLRI 包括下一跳网络地址。所述目的 IP 地址等于所述第二 VTEP 地址，所述下一跳网络地址等于所述第一 VTEP 地址。

举例来说，第一 VTEP 地址可以是 VTEP IP 地址 1。第二 VTEP 地址可以是 VTEP IP 地址 2。

在一种可能的设计中，所述第一 VTEP 经由隧道向所述第二 VTEP 发送所述 BGP update 消息。所述隧道是 VXLAN 隧道或者标签交换路径（label switched path，LSP）。所述 LSP 可以是段路由流量工程（Segment Routing Traffic Engineering，SR-TE）路径。

可选地，图 2 所示的方法中，所述 BGP 消息包含 MAC/IP Advertisement route 以及 MAC Mobility Extended Community。所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中。所述指示信息携带在所述 MAC Mobility Extended Community 中。

进一步地，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的 MSB 上。

进一步地，图 2 所示的方法中，所述 BGP 消息为 BGP 更新消息。

在一种可能的设计中，S202 包括：所述第一网络设备接收数据报文，所述数据报文的源 MAC 地址为所述第一 MAC 地址；以及，所述第一网络设备基于所述数据报文的源 MAC 地址标识的主机是攻击者，生成所述 BGP 消息。

上述技术方案中，所述第一网络设备基于所述数据报文的触发而生成所述 BGP 消息。也就是说，当第一网络设备确定第一 MAC 地址所标识的主机为攻击者时，所述第一网络设备不是必须立即生成 BGP 消息，并通知第二网络设备。当第一网络设备确定第一 MAC 地址所标识的主机为攻击者时，第一 MAC 地址所标识的主机可能并没有接入第一网络设备所管辖的网络。例如，第一 MAC 地址所标识的主机可能已下线，或者第一 MAC 地址所标识的主机可能已漫游到其他网络。因此，当第一网络设备确定第一 MAC 地址所标识的主机为攻击者时，第一网络设备和第二网络设备可能并没有遭到所述攻击者的攻击。在第一网络设备没有遭到所述攻击者攻击的情况下，第一网络设备暂时不生成以及发送 BGP 消息，有助于降低第一网络设备和第二网络设备的开销。当第一网络设备接收到源 MAC 地址为所述第一 MAC 地址的数据报文时，表明第一网络设备开始受到所述攻击者的攻击。第一网络设备开始受到所述攻击者的攻击时，第一网络设备通知第二网络设备所述攻击者的 MAC 地址，有助于获得降低开销和阻止攻击者的攻击的折中。

在一种可能的设计中，S202 包括：所述第一网络设备确定所述数据报文来自第一 VXLAN，第一 VNI 标识所述第一 VXLAN。所述第一网络设备基于所述数据报文携带的源 MAC 地址，以及所述数据报文来自第一 VXLAN，确定所述第一 MAC 地址标识的主机位于所述第一 VXLAN。所述第一网络设备基于所述第一 MAC 地址标识的主机位于所述第一 VXLAN，生成所述 BGP 消息，所述 BGP 消息包括所述第一 VNI。

在一种可能的实现方式中，所述第一网络设备确定所述数据报文来自第一 VXLAN，包括：所述第一网络设备经由第一端口接收所述数据报文，所述第一端口配置了所述第一 VNI。以及，所述第一网络设备基于用于接收所述数据报文的所述第一端口配置了所述第一 VNI，确定所述数据报文来自所述第一 VXLAN。

在另一种可能的实现方式中，所述第一网络设备确定所述数据报文来自第一 VXLAN，包括：所述第一网络设备确定所述数据报文中包含的第一虚拟局域网标识（VLAN ID）配置了所述第一 VNI。所述第一网络设备基于所述数据报文包含的所述第一 VLAN ID 配置了所述第一 VNI，确定所述数据报文来自所述第一 VXLAN。

上述技术方案中，所述第一网络设备根据配置信息，确定所述数据报文来自第一 VXLAN。进而，所述第一网络设备在 BGP 消息中携带用于标识所述第一 VXLAN 的第一 VNI。第二网络设备根据 BGP 消息中的第一 VNI，学习相应的 EVPN 路由。

图 3 是本申请提供的一种接收 BGP 消息的方法的流程示意图。图 3 所示的方法的执行主体为第二网络设备。例如，所述第二网络设备可以是图 1 中的 LS2。关于所述第二网络设备的结构和功能，可以参考上述实施例关于 LS2 的结构和功能的描述。所述第二网络设备可以执行上述实施例描述的 LS2 执行的动作。关于图 3 所示的方法的

具体实现方式，可以参考上述实施例的相关描述。参见图 3，所述方法包括：S301、S302 以及 S303。

S301、第二网络设备接收来自第一网络设备的 BGP 消息。

所述 BGP 消息包括第一 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址所标识的主机是攻击者。

举例来说，所述第一网络设备可以是 LS1。所述第一 MAC 地址可以是 MAC 地址 1。第一 MAC 地址所标识的主机可以是服务器 1。所述 BGP 消息可以是路由消息 2。所述指示信息可以是指示信息 1。

S302、所述第二网络设备接收第一报文。

所述第一报文的目的 MAC 地址等于所述第一 MAC 地址。

举例来说，所述第一报文可以是 LS2 管辖的网络中的主机生成的以太网帧。例如，所述第一报文可以是服务器 3 生成的以太网帧，或者服务器 4 生成的以太网帧。LS2 可以经由 LS2 的以太网接口接收所述第一报文。所述第一报文的目的 MAC 地址等于所述第一 MAC 地址，表明所述第一报文的生成者（例如服务器 3）想要和第一 MAC 地址所标识的主机（例如服务器 1）进行通信。

S303、所述第二网络设备避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

具体地，所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

举例来说，LS2 可以根据路由消息 2 生成转发表项 1。所述第一报文可以是报文 1。所述 LS2 可以根据转发表项 1 对报文 1 进行丢弃处理，或者其他处理。关于转发表项 1 的生成过程，转发表项 1 的结构以及如何根据转发表项 1 对报文 1 进行处理，可以参考上文的相关描述，此处不再赘述。

上述技术方案中，第二网络设备接收携带所述第一 MAC 地址以及指示信息的 BGP 消息后，所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

也就是说，第二网络设备可以利用第一网络设备发送的 BGP 消息，形成避免向所述第一 MAC 地址标识的所述主机转发所述第一报文的转发机制。因此，工程师不需要在第二网络设备上手工配置针对目的 MAC 地址为所述第一 MAC 地址的转发规则。因此，上述技术方案有助于减小工程师在网络设备上进行手工配置的工作量。

在一种可能的设计中，图 3 所示的技术方案中，还可以包括：

所述第二网络设备接收第二报文，所述第二报文的源 MAC 地址等于所述第一 MAC 地址。

所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第二报文中的所述源 MAC 地址，避免转发所述第二报文。

举例来说，LS2 可以根据路由消息 2 生成转发表项 2。所述第二报文可以是报文 2。所述 LS2 可以根据转发表项 2 对报文 2 进行丢弃处理。关于转发表项 2 的生成过程，

转发表项 2 的结构以及如何根据转发表项 2 对报文 2 进行处理，可以参考上文的相关描述，此处不再赘述。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。S301 包括：所述第二 VTEP 接收来自所述第二 VTEP 的边界网关协议 BGP update 消息。

所述 BGP 消息携带在所述 BGP update 消息中，所述 BGP update 消息包括 IP 头以及净荷，所述 IP 头包括目的 IP 地址，所述净荷包括 MP_REACH_NLRI，所述 MP_REACH_NLRI 包括下一跳网络地址，所述目的 IP 地址等于所述第二 VTEP 地址，所述下一跳网络地址等于所述第一 VTEP 地址。

举例来说，所述第一 VTEP 可以是 VTEP1。所述第二 VTEP 可以是 VTEP2。VTEP1 可以包含 LS1 的发送接口。所述发送接口可以是以太网接口。VTEP2 可以包含 LS2 的接收接口。所述接收接口可以是以太网接口。VTEP2 可以经由 LS1 和 LS2 之间的 VXLAN 隧道接收 VTEP1 发送路由消息 2。

举例来说，第一 VTEP 地址可以是 VTEP IP 地址 1。第二 VTEP 地址可以是 VTEP IP 地址 2。

在一种可能的设计中，所述第二 VTEP 经由隧道接收所述第一 VTEP 发送所述 BGP update 消息。所述隧道是 VXLAN 隧道或者标签交换路径（label switched path，LSP）。所述 LSP 可以是段路由流量工程（Segment Routing Traffic Engineering，SR-TE）路径。

可选地，图 3 所示的方法中，所述 BGP 消息包含 MAC/IP Advertisement route 以及 MAC Mobility Extended Community。所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中。所述指示信息携带在所述 MAC Mobility Extended Community 中。

进一步地，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的 MSB 上。

进一步地，图 3 所示的方法中，所述 BGP 消息为 BGP 更新消息。

图 4 为本申请提供的一种第一网络设备 400 的结构示意图。第一网络设备 400 包括处理器 410 以及收发器 420。处理器 410 与收发器 420 耦合。图 4 所示的第一网络设备 400 可以执行图 2 所示的方法。举例来说，第一网络设备 400 可以是图 1 中的 LS1。关于第一网络设备 400 的具体实现方式，可以参考图 2 所示的实施例，也可以参考本申请对 LS1 的描述。

处理器 410 用于确定第一 MAC 地址所标识的主机为攻击者。

举例来说，处理器 410 可以是处理器，也可以是专用集成电路（application-specific integrated circuit，ASIC）或者现场可编程门阵列（field programmable gate array，FPGA）。

处理器 410 还用于生成 BGP 消息，所述 BGP 消息包括所述第一 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址标识的的所述主机是所述攻击者。

举例来说，处理器 410 基于所述第一 MAC 地址所标识的主机为攻击者，生成所述 BGP 消息。

收发器 420 用于向第二网络设备发送处理器 410 生成的所述 BGP 消息。

举例来说，第二网络设备可以是图 1 中的 LS2。

在一种可能的设计中，第一网络设备 400 可以包括存储器 430。存储器 430 与处理器 410 耦合。存储器 430 可以保存计算机程序。例如，存储器 430 中保存了用于识别 DDoS 攻击的计算机程序。处理器 410 通过执行所述计算机程序，对来自攻击者的多个报文的特征进行分析，从而确定所述多个报文属于 DDoS 攻击。所述多个报文的源 MAC 地址为 MAC 地址 1。处理器 410 根据所述多个报文的源 MAC 地址确定 MAC 地址 1 所标识的主机（例如服务器 1）是攻击者。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。

收发器 420 用于向所述第二 VTEP 发送来自所述第一 VTEP 的所述 BGP 消息。

举例来说，所述第一 VTEP 和所述第二 VTEP 之间存在 VXLAN 隧道。收发器 420 位于所述 VXLAN 隧道。例如，收发器 420 包含以太网接口，收发器 420 可以接收和发送遵循以太网协议的报文（例如以太网帧）。

在一种可能的设计中，所述 BGP 消息包含媒体访问控制/网际协议通告路由 MAC/IP Advertisement route 以及媒体访问控制移动性扩展团体 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

在一种可能的设计中，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的 MSB 上。

在一种可能的设计中，所述 BGP 消息为 BGP 更新消息。

图 5 为本申请提供的一种第二网络设备 500 的结构示意图。第二网络设备 500 包括第一收发器 510、第二收发器 520 以及处理器 530。第一收发器 510 与处理器 530 耦合。第二收发器 520 与处理器 530 耦合。图 5 所示的第二网络设备 500 可以执行图 3 所示的方法。举例来说，第二网络设备 500 可以是图 1 中的 LS2。关于第二网络设备 500 的具体实现方式，可以参考图 3 所示的实施例，也可以参考本申请对 LS2 的描述。

第一收发器 510 用于接收来自第一网络设备的 BGP 消息，所述 BGP 消息包括第一媒体访问控制 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址所标识的主机是攻击者。

第二收发器 520 用于接收第一报文，所述第一报文的目的 MAC 地址等于所述第一 MAC 地址。

举例来说，第一收发器 510 可以包含以太网接口。第一收发器 510 可以接收和发送遵循以太网协议的报文（例如以太网帧）。第二收发器 520 可以包含以太网接口。第二收发器 520 可以接收和发送遵循以太网协议的报文（例如以太网帧）。

举例来说，第一收发器 510 可以位于 LS1 和 LS2 之间的 VXLAN 隧道上。第二收发器 520 可以用于连接 LS2 所管辖的网络。例如，第二收发器 520 可以用于连接服务器 3 以及服务器 4。

处理器 530 用于基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识

的所述主机转发所述第一报文。

举例来说，处理器 530 可以是中央处理单元，也可以是 ASIC 或者 FPGA。

在一种可能的设计中，第二网络设备 500 可以包括存储器 540。存储器 540 与处理器 530 耦合。存储器 540 可以保存计算机程序。例如，存储器 540 中保存了用于实现 BGP 的功能的计算机程序。处理器 530 通过执行所述计算机程序，基于所述 BGP 消息以及第二网络设备 500 的配置信息，生成转发表项 1。所述第一报文可以是报文 1。所述 LS2 可以根据转发表项 1 对报文 1 进行丢弃处理，或者其他处理。关于转发表项 1 的生成过程，转发表项 1 的结构以及如何根据转发表项 1 对报文 1 进行处理，可以参考上文的相关描述，此处不再赘述。

在一种可能的设计中，第二收发器 520 还用于接收第二报文，所述第二报文的源 MAC 地址等于所述第一 MAC 地址。

处理器 530 还用于基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第二报文中的所述源 MAC 地址，避免转发所述第二报文。

举例来说，LS2 可以根据路由消息 2 生成转发表项 2。所述第二报文可以是报文 2。所述 LS2 可以根据转发表项 2 对报文 2 进行丢弃处理。关于转发表项 2 的生成过程，转发表项 2 的结构以及如何根据转发表项 2 对报文 2 进行处理，可以参考上文的相关描述，此处不再赘述。

在一种可能的设计中，所述第一网络设备包括第一 VTEP，所述第二网络设备包括第二 VTEP。

第一收发器 510 用于向所述第二 VTEP 发送来自所述第一 VTEP 的所述 BGP 消息。

第一收发器 510 可以位于 LS1 和 LS2 之间的 VXLAN 隧道上。第一收发器 510 经由 VXLAN 隧道接收到来自第一 VTEP（包含在第一网络设备中）的 BGP 消息后，可以向第二网络设备中的第二 VTEP 发送所述 BGP 消息。

在一种可能的设计中，所述 BGP 消息包含媒体访问控制/网际协议通告路由 MAC/IP Advertisement route 以及媒体访问控制移动性扩展团体 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

在一种可能的设计中，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的 MSB 上。

图 6 为本申请提供的一种系统。参见图 6，系统 600 包括第一网络设备 601 以及第二网络设备 602。第一网络设备 601 可以是图 4 所示第一网络设备 400。第二网络设备 602 可以是图 5 所示的第二网络设备 500。例如，第一网络设备 601 可以执行图 2 所示的方法。第二网络设备 602 可以执行图 3 所示的方法。具体地，第一网络设备 601 可以是图 1 中的 LS1。第二网络设备 602 可以是图 1 中的 LS2。关于第一网络设备 601 的具体实现方式，可以参考图 2 所示的实施例，以及本申请对 LS1 的描述。关于第二网络设备 602 的具体实现方式，可以参考图 3 所示的实施例，以及本申请对 LS2 的描述。

本申请还提供了一种计算机可读存储介质。所述计算机可读存储介质存储计算机程序。当所述计算机程序被网络设备执行时，使得网络设备执行图 2 所示的方法，或

者图 3 所示的方法。举例来说，所述网络设备可以是图 2 所示的方法涉及的第一网络设备，或者图 3 所示的方法涉及的第二网络设备。

本申请还提供了一种计算机程序产品。所述计算机程序产品包含计算机程序。所述计算机程序可以保存在计算机可读存储介质上。当所述计算机程序被网络设备执行时，使得网络设备执行图 2 所示的方法，或者图 3 所示的方法。举例来说，所述网络设备可以是图 2 所示的方法涉及的第一网络设备，或者图 3 所示的方法涉及的第二网络设备。

本申请所描述的方法或者方法中的步骤可以硬件的方式来实现，也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成。软件模块可以被存放于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、移动硬盘、CD-ROM 或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于用户设备中。当然，处理器和存储介质也可以作为分立组件存在于用户设备中。

本领域技术人员应该可以意识到，本申请所描述的功能可以用硬件或者固件实现。本申请所描述的功能也可以用软件和硬件的组合来实现。所示软件可以存储在计算机可读介质中。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的介质。存储介质可以是通用或专用计算机能够存取的介质。

以上所述的具体实施方式，对本申请的目的、技术方案和有益效果进行了进一步详细说明。所应理解的是，以上所述仅为本申请的具体实施方式而已。

权 利 要 求 书

1、一种发送边界网关协议 BGP 消息的方法，其特征在于，包括：

第一网络设备确定第一媒体访问控制 MAC 地址所标识的主机为攻击者；

所述第一网络设备生成 BGP 消息，所述 BGP 消息包括所述第一 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址标识的的所述主机是所述攻击者；

所述第一网络设备向第二网络设备发送所述 BGP 消息。

2、根据权利要求 1 所述的方法，其特征在于，所述第一网络设备包括第一虚拟扩展局域网隧道端点 VTEP，所述第二网络设备包括第二 VTEP；

所述第一网络设备向第二网络设备发送所述 BGP 消息包括：

所述第一 VTEP 向所述第二 VTEP 发送所述 BGP 消息。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述 BGP 消息包含媒体访问控制/网际协议通告路由 MAC/IP Advertisement route 以及媒体访问控制移动性扩展团体 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

4、根据权利要求 3 所述的方法，其特征在于，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的最高有效位 MSB 上。

5、根据权利要求 1 至 4 中任一所述的方法，其特征在于，所述 BGP 消息为 BGP 更新消息。

6、一种接收边界网关协议 BGP 消息的方法，其特征在于，包括：

第二网络设备接收来自第一网络设备的 BGP 消息，所述 BGP 消息包括第一媒体访问控制 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址所标识的主机是攻击者；

所述第二网络设备接收第一报文，所述第一报文的目的 MAC 地址等于所述第一 MAC 地址；

所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

7、根据权利要求 6 所述的方法，其特征在于，还包括：

所述第二网络设备接收第二报文，所述第二报文的源 MAC 地址等于所述第一 MAC 地址；

所述第二网络设备基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的

所述指示信息以及所述第二报文中的所述源 MAC 地址，避免转发所述第二报文。

8、根据权利要求 6 或 7 所述的方法，其特征在于，所述第一网络设备包括第一虚拟扩展局域网隧道端点 VTEP，所述第二网络设备包括第二 VTEP；

所述第二网络设备接收来自第一网络设备的 BGP 消息包括：

所述第二 VTEP 接收来自所述第一 VTEP 的所述路由信息。

9、根据权利要求 6 至 8 中任一所述的方法，其特征在于，所述 BGP 消息包含媒体访问控制/网际协议通告路由 MAC/IP Advertisement route 以及媒体访问控制移动性扩展团体 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

10、根据权利要求 9 所述的方法，其特征在于，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的最高有效位 MSB 上。

11、一种第一网络设备，其特征在于，包括：处理器以及与所述处理器耦合的收发器；

所述处理器用于确定第一媒体访问控制 MAC 地址所标识的主机为攻击者；

所述处理器还用于生成边界网关协议 BGP 消息，所述 BGP 消息包括所述第一 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址标识的的所述主机是所述攻击者；

所述收发器用于向第二网络设备发送所述处理器生成的所述 BGP 消息。

12、根据权利要求 11 所述的第一网络设备，其特征在于，所述第一网络设备包括第一虚拟扩展局域网隧道端点 VTEP，所述第二网络设备包括第二 VTEP；

所述收发器用于向所述第二 VTEP 发送来自所述第一 VTEP 的所述 BGP 消息。

13、根据权利要求 11 或 12 所述的第一网络设备，其特征在于，所述 BGP 消息包含媒体访问控制/网际协议通告路由 MAC/IP Advertisement route 以及媒体访问控制移动性扩展团体 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

14、根据权利要求 13 所述的第一网络设备，其特征在于，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的最高有效位 MSB 上。

15、根据权利要求 11 至 14 中任一所述的第一网络设备，其特征在于，所述 BGP 消息为 BGP 更新消息。

16、一种第二网络设备，其特征在于，包括：第一收发器、第二收发器以及与所述第一收发器和所述第二收发器耦合的处理器；

所述第一收发器用于接收来自第一网络设备的边界网关协议 BGP 消息，所述 BGP 消息包括第一媒体访问控制 MAC 地址以及指示信息，所述指示信息用于指示所述第一 MAC 地址所标识的主机是攻击者；

所述第二收发器用于接收第一报文，所述第一报文的目的 MAC 地址等于所述第一 MAC 地址；

所述处理器用于基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第一报文中的所述目的 MAC 地址，避免向所述第一 MAC 地址标识的所述主机转发所述第一报文。

17、根据权利要求 16 所述的第二网络设备，其特征在于，所述第二收发器还用于接收第二报文，所述第二报文的源 MAC 地址等于所述第一 MAC 地址；

所述处理器还用于基于所述 BGP 消息中的所述第一 MAC 地址、所述 BGP 消息中的所述指示信息以及所述第二报文中的所述源 MAC 地址，避免转发所述第二报文。

18、根据权利要求 16 或 17 所述的第二网络设备，其特征在于，所述第一网络设备包括第一虚拟扩展局域网隧道端点 VTEP，所述第二网络设备包括第二 VTEP；

所述第一收发器用于向所述第二 VTEP 发送来自所述第一 VTEP 的所述 BGP 消息。

19、根据权利要求 16 至 18 中任一所述的第二网络设备，其特征在于，所述 BGP 消息包含媒体访问控制/网际协议通告路由 MAC/IP Advertisement route 以及媒体访问控制移动性扩展团体 MAC Mobility Extended Community，所述第一 MAC 地址携带在所述 MAC/IP Advertisement route 中，所述指示信息携带在所述 MAC Mobility Extended Community 中。

20、根据权利要求 19 所述的第二网络设备，其特征在于，所述 MAC Mobility Extended Community 包括具有 8 个比特的旗帜，所述指示信息携带在所述旗帜的最高有效位 MSB 上。

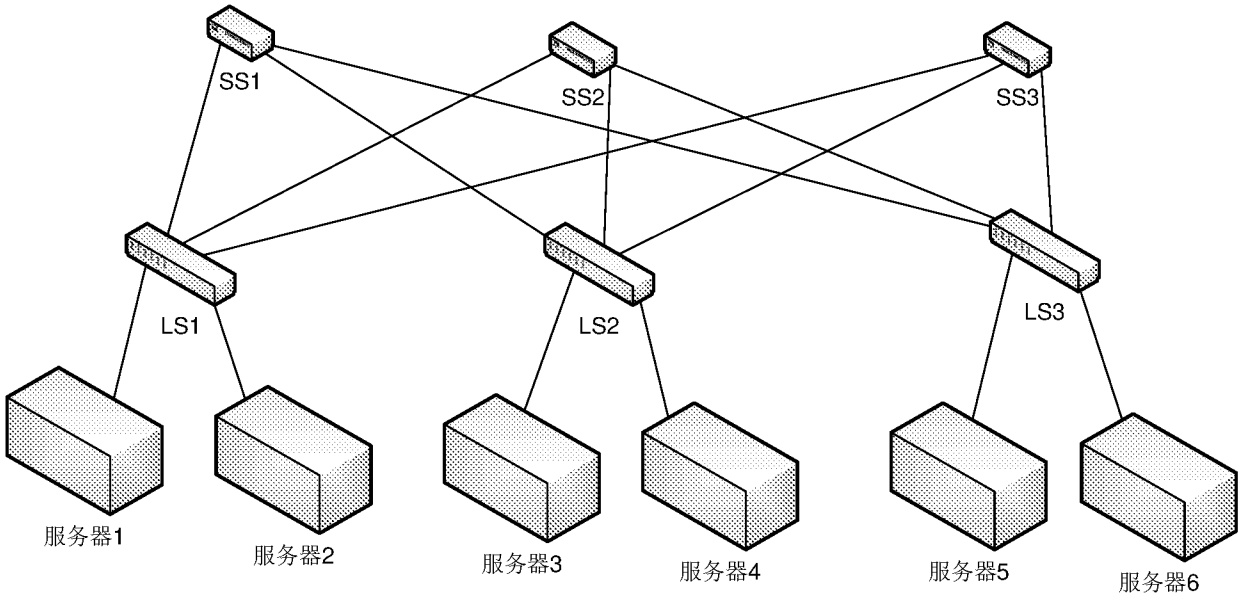
SS1
SS2
SS3
LS1
LS2
LS3
服务器1
服务器2
服务器3
服务器4
服务器5
服务器6

图 1

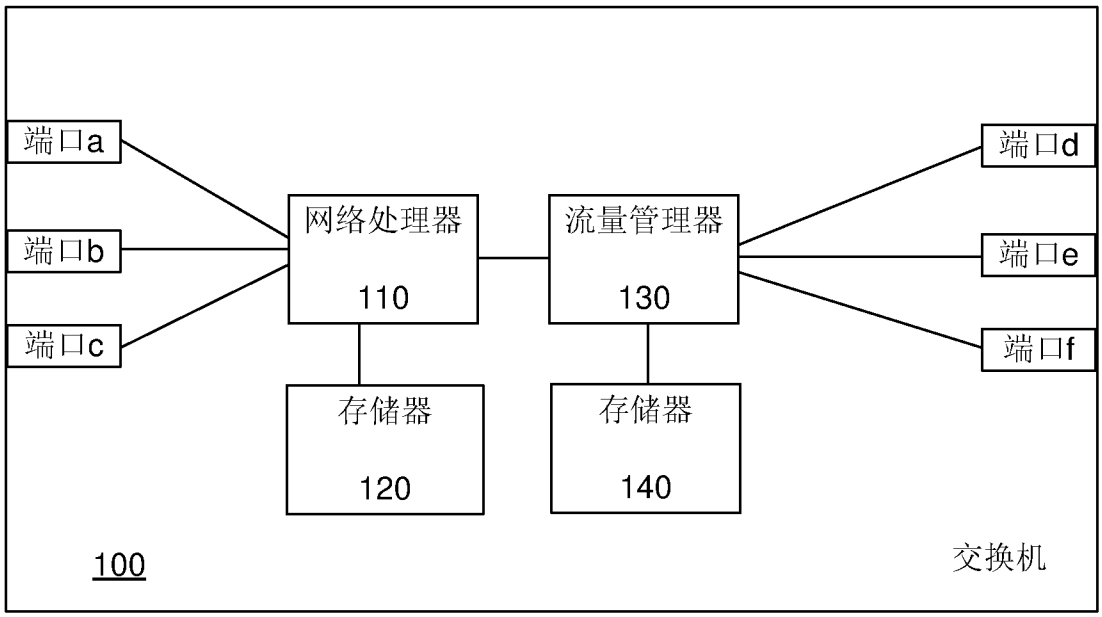
端口a
端口b
端口c
网络处理器
110
流量管理器
130
端口d
端口e
端口f
存储器
120
存储器
140
100
交换机

图 1a

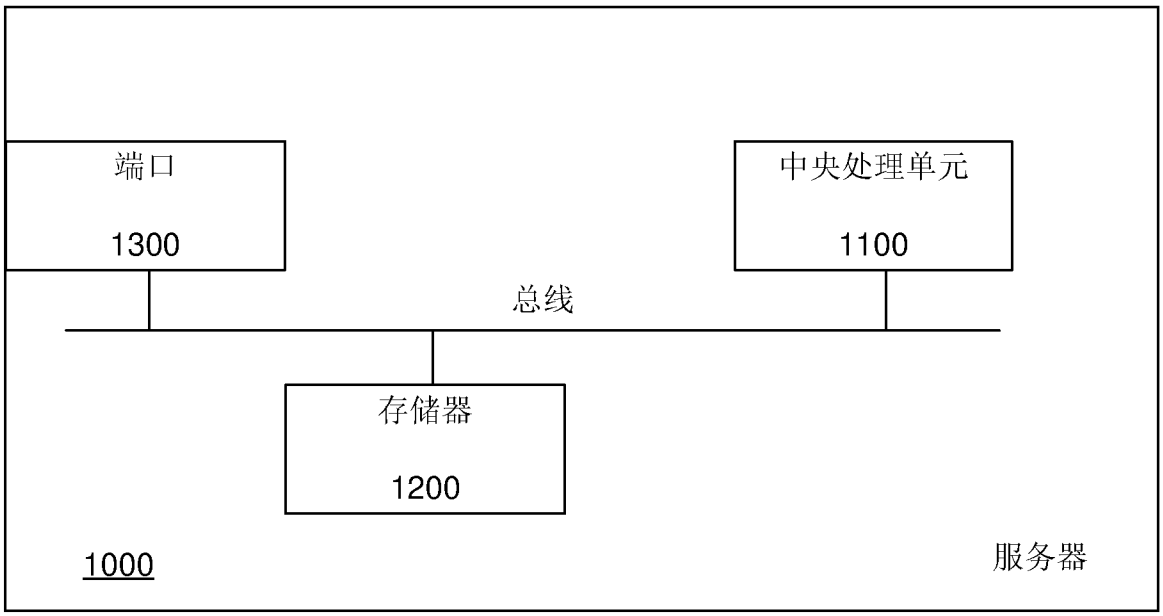
端口
1300
中央处理单元
1100
总线
存储器
1200
1000
服务器

图 1b

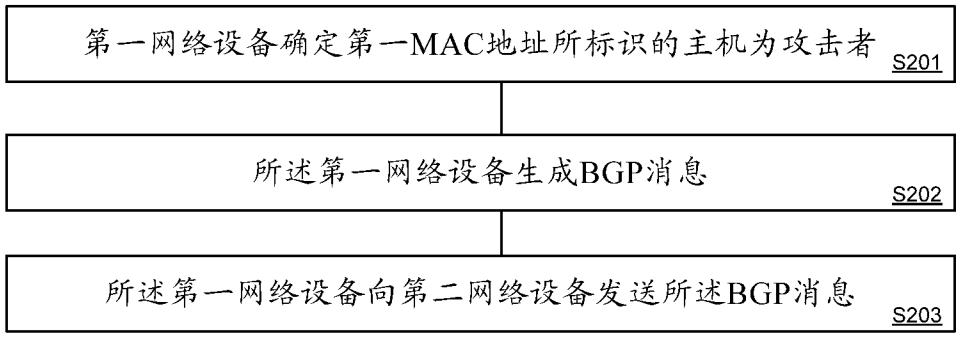
第一网络设备确定第一MAC地址所标识的主机为攻击者
S201
所述第一网络设备生成BGP消息
S202
所述第一网络设备向第二网络设备发送所述BGP消息
S203

图 2

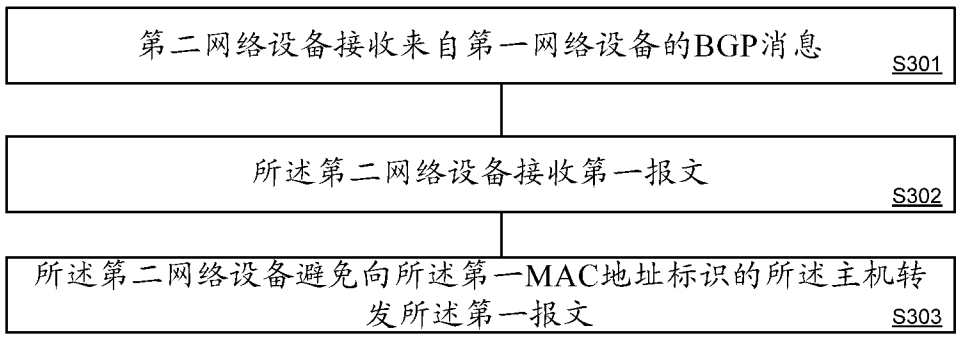
第二网络设备接收来自第一网络设备的BGP消息
S301
所述第二网络设备接收第一报文
S302
所述第二网络设备避免向所述第一MAC地址标识的所述主机转发所述第一报文
S303

图 3

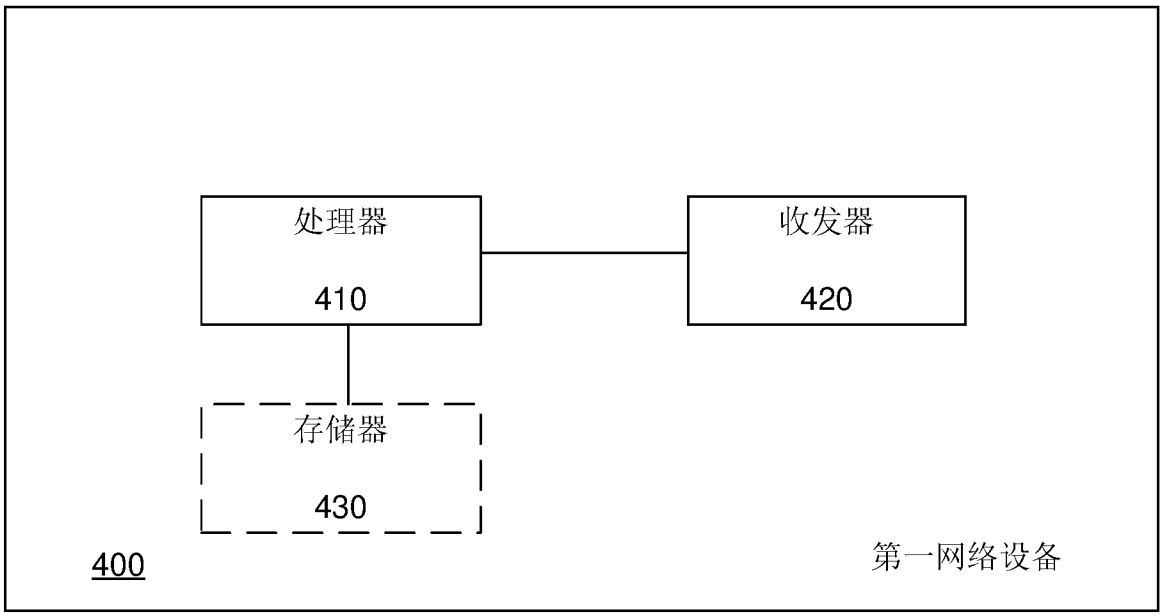
处理器
410
收发器
420
存储器
430
400
第一网络设备

图 4

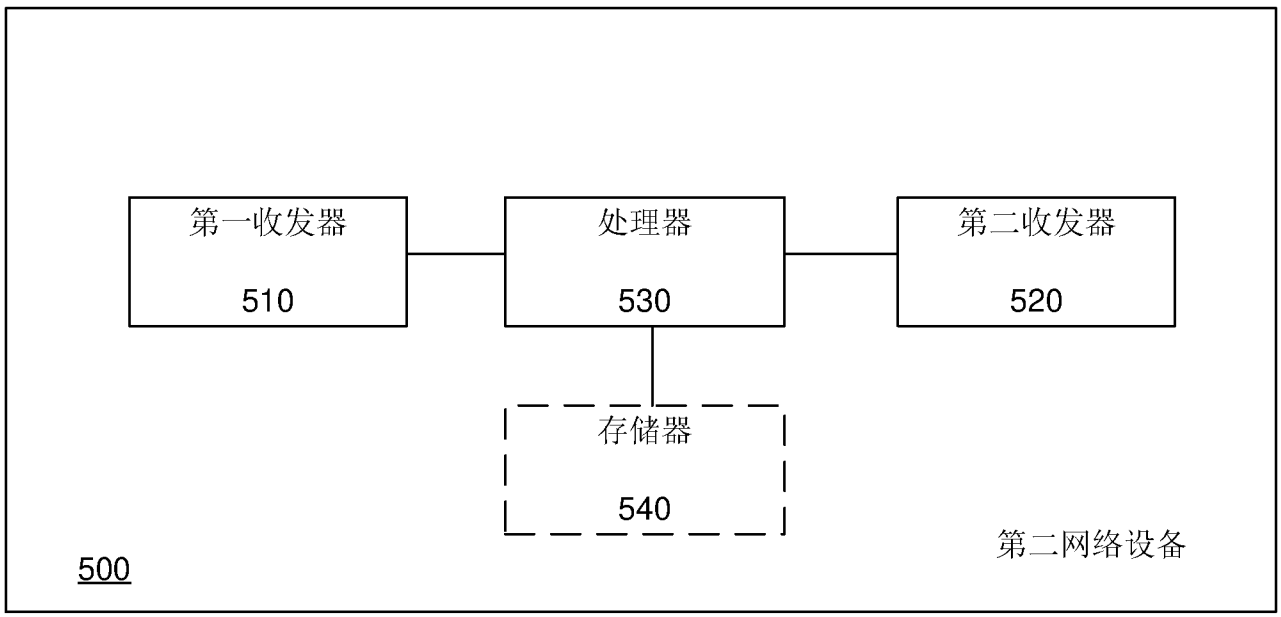
第一收发器
510
处理器
530
第二收发器
520
存储器
540
500
第二网络设备

图 5

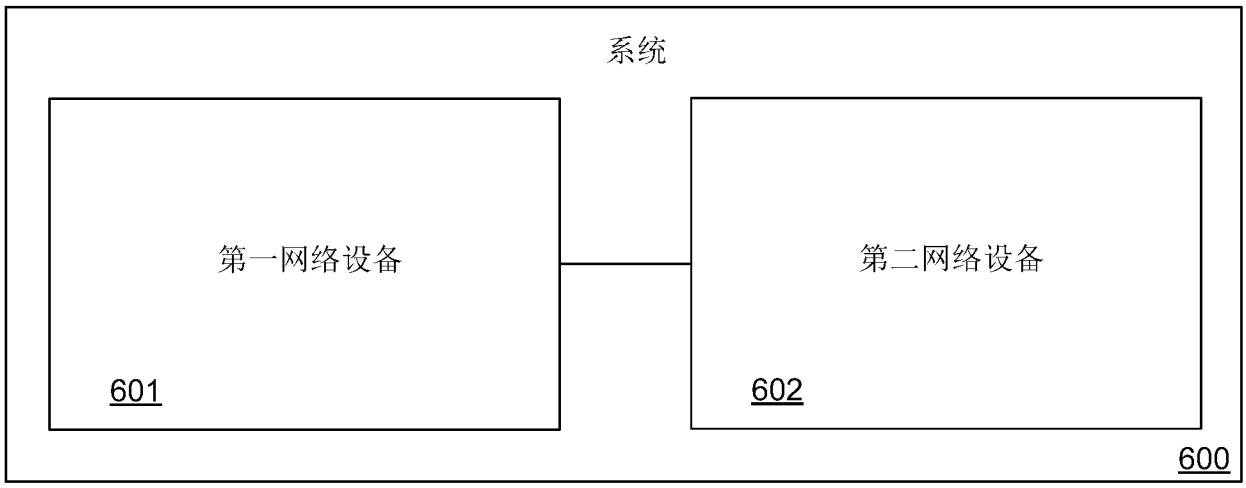

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/092443

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/741(2013.01)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)

CNPAT; WPI; EPODOC; CNKI; IEEE: 边界网关协议, 确定, 主机, 攻击者, 媒体访问控制, 地址, 指示, 转发, 虚拟扩展局域网隧道端点, 包含, 携带, BGP, determine, host, attacker, MAC, address, indicate, forward, VTEP, comprise, carry

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 107154939 A (SANGFOR TECHNOLOGIES INC.) 12 September 2017 (2017-09-12) description, paragraphs [0069]-[0122]	1-20
Y	CN 108023974 A (NEW H3C TECHNOLOGIES CO., LTD.) 11 May 2018 (2018-05-11) description, paragraphs [0004] and [0005]	1-20
A	CN 101621428 A (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 06 January 2010 (2010-01-06) entire document	1-20
A	US 2016373447 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 22 December 2016 (2016-12-22) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 September 2019	**27 September 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/092443

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 107154939 A	12 September 2017	None	
CN 108023974 A	11 May 2018	None	
CN 101621428 A	06 January 2010	WO 2011012056 A1	03 February 2011
		EP 2448211 A1	02 May 2012
US 2016373447 A1	22 December 2016	WO 2015001969 A1	08 January 2015
		JP WO2015001969 A1	23 February 2017
		CN 105359156 A	24 February 2016
		EP 2998901 A1	23 March 2016

国际检索报告

国际申请号
PCT/CN2019/092443

A. 主题的分类

H04L 12/741(2013.01)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））

CNPAT; WPI; EPODOC; CNKI; IEEE: 边界网关协议，确定，主机，攻击者，媒体访问控制，地址，指示，转发，虚拟扩展局域网隧道端点，包含，携带，BGP, determine, host, attacker, MAC, address, indicate, forward, VTEP, comprise, carry

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
Y	CN 107154939 A (深信服科技股份有限公司) 2017年 9月 12日 (2017-09-12) 说明书第[0069]-[0122]段	1-20
Y	CN 108023974 A (新华三技术有限公司) 2018年 5月 11日 (2018-05-11) 说明书第[0004]-[0005]段	1-20
A	CN 101621428 A (成都市华为赛门铁克科技有限公司) 2010年 1月 6日 (2010-01-06) 全文	1-20
A	US 2016373447 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 2016年 12月 22日 (2016-12-22) 全文	1-20

☐ 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	国际检索报告邮寄日期
2019年 9月 12日	2019年 9月 27日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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 林桂荣 电话号码 86-(10)-53961573

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/092443

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	107154939	A	2017年 9月 12日	无			
CN	108023974	A	2018年 5月 11日	无			
CN	101621428	A	2010年 1月 6日	WO	2011012056	A1	2011年 2月 3日
				EP	2448211	A1	2012年 5月 2日
US	2016373447	A1	2016年 12月 22日	WO	2015001969	A1	2015年 1月 8日
				JP	WO2015001969	A1	2017年 2月 23日
				CN	105359156	A	2016年 2月 24日
				EP	2998901	A1	2016年 3月 23日