

(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
2022 年 1 月 27 日 (27.01.2022)



(10) 国际公布号
WO 2022/017267 A1

- (51) 国际专利分类号:
G06F 15/16 (2006.01)
- (21) 国际申请号: PCT/CN2021/106689
- (22) 国际申请日: 2021 年 7 月 16 日 (16.07.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202010706089.9 2020年7月21日 (21.07.2020) CN
202010954759.9 2020年9月11日 (11.09.2020) 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: 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)。 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)。 顾钰楠 (GU, Yunan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 夏忠其 (XIA, Zhongqi); 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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) Title: ROUTING MANAGEMENT METHOD, APPARATUS AND SYSTEM

(54) 发明名称: 一种路由管理方法、装置及系统

300

获得对应关系, 包括第一自治系统AS标识和第二AS标识, 指示第一AS标识和第二AS标识为兄弟AS

S303

根据对应关系进行路由管理

S305

图 3a

- S303 Obtain a correlation, comprising a first autonomous system (AS) identifier and a second AS identifier, indicating that the first AS identifier and the second AS identifier are sibling ASs
- S305 Perform routing management according to the correlation

(57) Abstract: The present application discloses a routing management method and an autonomous system (AS) management solution. A device can obtain a correlation, the correlation comprising a first AS identifier and a second AS identifier, and the correlation being used to indicate that the first AS identifier and the second AS identifier are sibling ASs. The device also performs routing management according to the correlation, the routing management comprising direct routing management or indirect routing management.

(57) 摘要: 本申请公开了一种路由管理方法和AS管理方案, 设备可以获得对应关系, 这个对应关系包括第一自治系统AS标识和第二AS标识, 这个对应关系用于指示第一AS标识和第二AS标识为兄弟AS, 设备还根据该对应关系进行路由管理, 该路由管理包括直接的路由管理或间接的路由管理。

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))。

一种路由管理方法、装置及系统

本申请要求于 2020 年 07 月 21 日提交的申请号为 202010706089.9、申请名称为“一种路由校验方法、装置及系统”以及于申请号为 2020 年 09 月 11 日提交的申请号为 202010954759.9、申请名称为“一种路由管理方法、装置及系统”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。

技术领域

本申请涉及通信领域，一种路由管理方法、装置及系统。

背景技术

在当前的自治系统 (Autonomous System, AS) 管理方案中，通常会对 AS 或 AS 之间的商业通告关系或路由的源路由信息进行管理。但是这些管理方式，存在信息不全等问题。

发明内容

本申请实施例提供了一种路由管理方法、装置及系统，以减少信息不全等问题。

技术方案如下：

第一方面，提供了一种路由管理方法，该方法包括如下步骤：获得对应关系，对应关系包括第一自治系统 AS 标识和第二 AS 标识，该对应关系用于指示第一 AS 标识和第二 AS 标识为兄弟 AS；根据对应关系进行路由管理。

通过在路由管理中，将指示第一 AS 标识和第二 AS 标识为兄弟 AS 的信息考虑在内，可以使得路由管理的信息更全面。

在一种可能的设计中，上述根据对应关系进行路由管理，包括：根据对应关系确定路由消息有效。

通过在确定路由消息是否有效的过程中，将兄弟 AS 的信息考虑在内，减少出现误判的问题，并进一步使得路由消息判断的结果准确率更高。

在一种可能的设计中，在根据对应关系确定路由消息有效之前，还包括如下步骤：根据路由起源授权 ROA 信息确定路由消息无效，这里的路由消息无效包括：路由消息的路由被劫持；或根据商业关系信息确定路由消息无效，这里的路由消息无效包括：路由消息发生路由泄漏。

通过与已有的 ROA 或商业关系信息的结合，可以使得原有的可能被误判为无效的路由消息确定为有效，进一步使得路由消息判断的结果准确率更高。

在一种可能的设计中，上述路由消息包括第一路由前缀和第三 AS 标识，该路由消息指示第三 AS 为第一路由前缀的源 AS，上述根据 ROA 信息确定路由消息无效，包括如下步骤：根据 ROA 信息确定第一路由前缀被第三 AS 劫持，该 ROA 信息指示第二路由前缀的源 AS 为第二 AS，第一路由前缀与第二路由前缀对应；根据对应关系确定路由消息有效，包括如下步骤：根据第三 AS 标识与第一 AS 标识相同，确定路由消息未被第三 AS 标识劫持。

通过与已有的 ROA 信息的结合，可以使得原有的可能被误判为路由劫持的路由消息确

定为有效，进一步使得路由消息判断的结果准确率更高。

在一种可能的设计中，上述路由消息包括第一路由前缀、第三 AS 标识和第四 AS 标识，第三 AS 标识与第四 AS 标识在路由消息的 AS 路径中相邻，根据商业关系信息确定路由消息无效，包括：校验第一路由前缀由第三 AS 泄漏给第四 AS，上述根据对应关系确定路由消息有效，包括如下步骤：根据第四 AS 标识与第一 AS 标识相同以及满足第一条件确定路由消息未被第三 AS 泄漏，第一条件包括：第三 AS 标识与第二 AS 标识相同，或路由消息包括的源 AS ID 与所述第二 AS 标识相同。其中，该源 AS ID 可以为上述第四 AS，也可以为其他 AS。

通过与已有的 ROA 信息的结合，可以使得原有的可能被误判为路由泄漏的路由消息确定为有效，进一步使得路由消息判断的结果准确率更高。

在一种可能的设计中，在确定上述路由消息有效之后，还包括如下步骤：将路由消息对应的校验状态更新为有效。

将该路由消息的校验状态更新有效后，可以使得该路由消息不必被多次校验，进而可以减少其他设备或者其他功能模块再次校验或再次误判的可能。

在一种可能的设计中，上述获得对应关系，包括：接收第一消息，第一消息中包括上述对应关系。

可以通过接收的消息中直接携带上述对应管理的方式获得对应关系，减少本地处理的压力。

在一种可能的设计中，上述第一消息由资源公钥基础设施 RPKI 服务器发送，该第一消息中包括兄弟 AS 协议数据单元 PDU，PDU 中包括第一 AS 标识和第二 AS 标识。

在一种可能的设计中，该第一消息还包括组织标识 和/或兄弟 AS 数。

通过接收 RPKI 服务器发送的消息，将本技术方案融入已有系统，进一步提高本技术方案的实用性。通过定义与 RPKI 服务器直接交互的消息的格式，可以进一步降低本技术方案应用的难度。

在一种可能的设计中，该路由消息为边界网关协议 BGP 消息。

在一种可能的设计中，上述根据所述对应关系进行路由管理，包括如下步骤：向接收设备发送消息，消息包括对应关系，该消息用于使接收设备根据对应关系进行路由分析。

通过发送该指示兄弟 AS 的对应关系，进行间接的路由管理，可以使得接收该对应关系的设备进行路由管理时获得的信息更全面。

在一种可能的设计中，上述获得对应关系，包括如下步骤：获得第一 AS 标识和第二 AS 标识；确定第一 AS 标识和第二 AS 标识为兄弟 AS；生成上述对应关系。

通过获得的第一 AS 标识和第二 AS 标识确定兄弟 AS，生成对应关系，提供一种更智能化的方案。

在一种可能的设计中，第一方面以及第一方面的各种可能的设计的技术应用于资源公钥基础设施 RPKI 系统中。

通过将本技术方案融入已有的 RPKI 系统，可以进一步提高本技术方案的实用性。

第二方面，提供了一种路由管理方法，该方法包括如下步骤：获得第一自治系统 AS 标识和第二 AS 标识；发送消息，该消息包括第一 AS 标识和第二 AS 标识，该消息用于指示第

一 AS 标识和第二 AS 标识为兄弟 AS。

在一种可能的设计中，该消息还包括组织标识和/或 AS 数量。

在一种可能的设计中，第一 AS 标识和第二 AS 标识携带在该消息的兄弟 AS 协议数据单元 PDU 中。

通过发送该指示兄弟 AS 的对应关系，进行间接的路由管理，可以使得接收该对应关系的设备进行路由管理时获得的信息更全面。

第三方面，提供了一种路由管理装置，包括：处理单元，用于获得对应关系，该对应关系包括第一自治系统 AS 标识和第二 AS 标识，该对应关系用于指示第一 AS 标识和第二 AS 标识为兄弟 AS；该处理单元，还用于根据对应关系进行路由管理。

在一种可能的设计中，该处理单元，用于根据对应关系确定路由消息有效。

在一种可能的设计中，在处理单元用于确定路由消息有效之前，处理单元还用于：根据路由起源授权 ROA 信息确定路由消息无效，路由消息无效包括：路由消息的路由被劫持；或根据商业关系信息确定路由消息无效，路由消息无效包括：路由消息发生路由泄漏。

在一种可能的设计中，该路由消息包括第一路由前缀和第三 AS 标识，该路由消息指示第三 AS 为第一路由前缀的源 AS，该处理单元用于：根据 ROA 信息确定第一路由前缀被第三 AS 劫持，ROA 信息指示第二路由前缀的源 AS 为第二 AS，第一路由前缀与第二路由前缀对应；该处理单元还用于：根据第三 AS 标识与第一 AS 标识相同，确定路由消息未被第三 AS 标识劫持。

在一种可能的设计中，该路由消息包括第一路由前缀、第三 AS 标识和第四 AS 标识，第三 AS 标识与第四 AS 标识在路由消息的 AS 路径中相邻，处理单元用于：确定第一路由前缀由第三 AS 泄漏给第四 AS；该处理单元还用于：根据第四 AS 标识与第一 AS 标识相同以及满足第一条件确定路由消息未被第三 AS 泄漏，该第一条件包括：第三 AS 标识与第二 AS 标识相同，或路由消息包括的源 AS 标识与第二 AS 标识相同。

在一种可能的设计中，该处理单元，还用于：将路由消息对应的确定状态更新为有效。

在一种可能的设计中，该路由管理装置还包括接收单元，该接收单元用于接收第一消息，第一消息包括所述对应关系。

在一种可能的设计中，该路由管理装置还包括发送单元，用于向接收设备发送消息，该消息包括对应关系，该消息用于使接收设备根据对应关系进行路由分析。

在一种可能的设计中，该处理单元，还用于获得第一 AS 标识和第二 AS 标识；确定第一 AS 标识和第二 AS 标识为兄弟 AS；生成对应关系。

第四方面，提供了一种 AS 管理装置，该装置包括：处理单元，用于获得第一自治系统 AS 标识和第二 AS 标识；发送单元，用于发送消息，该消息包括第一 AS 标识和第二 AS 标识，该消息用于指示第一 AS 标识和第二 AS 标识为兄弟 AS。

在一种可能的设计中，该消息还包括组织标识和/或 AS 数量。

在一种可能的设计中，第一 AS 标识和第二 AS 标识携带在消息的兄弟 AS 协议数据单元 PDU 中。

第五方面，提供了一种路由管理设备，该路由管理设备包括处理器和通信接口，该处理器用于执行指令，使得该路由管理设备执行上述第一方面或第一方面任一种可选方式所

提供的方法，所述通信接口用于接收或发送报文。第五方面提供的路由管理设备的具体细节可参见上述第一方面或第一方面任一种可选方式，此处不再赘述。

第六方面，提供了一种 AS 管理设备，该 AS 管理设备包括处理器和通信接口，该处理器用于执行指令，使得该 AS 管理设备执行上述第二方面或第二方面任一种可选方式所提供的方法，所述通信接口用于接收或发送报文。第六方面提供的 AS 管理设备的具体细节可参见上述第二方面或第二方面任一种可选方式，此处不再赘述。

第七方面，提供了一种计算机可读存储介质，该存储介质中存储有至少一条指令，该指令由处理器读取以使路由管理设备执行上述第一方面或第一方面任一种可选方式所提供的方法。

第八方面，提供了一种计算机可读存储介质，该存储介质中存储有至少一条指令，该指令由处理器读取以使 AS 管理设备执行上述第二方面或第二方面任一种可选方式所提供的方法。

第九方面，提供了一种计算机程序产品，该计算机程序产品包括计算机指令，该计算机指令存储在计算机可读存储介质中。路由管理设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该路由管理设备执行上述第一方面或第一方面任一种可选方式所提供的方法。

第十方面，提供了一种计算机程序产品，该计算机程序产品包括计算机指令，该计算机指令存储在计算机可读存储介质中。AS 管理设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该 AS 管理设备执行上述第二方面或第二方面任一种可选方式所提供的方法。

第十一方面，提供了一种芯片，当该芯片在路由管理设备上运行时，使得路由管理设备执行上述第一方面或第一方面任一种可选方式所提供的方法。

第十二方面，提供了一种芯片，当该芯片在 AS 管理设备上运行时，使得 AS 管理设备执行上述第二方面或第二方面任一种可选方式所提供的方法。

第十三方面，提供一种路由管理设备，该路由管理设备包括：主控板和接口板，进一步，还可以包括交换网板。该路由管理设备用于执行第一方面或第一方面的任意可能的实现方式中的方法。具体地，该路由管理设备包括用于执行第一方面或第一方面的任意可能的实现方式中的方法的单元。

第十四方面，提供一种 AS 管理设备，该 AS 管理设备包括：主控板和接口板，进一步，还可以包括交换网板。该 AS 管理设备用于执行第二方面或第二方面的任意可能的实现方式中的方法。具体地，该 AS 管理设备包括用于执行第二方面或第二方面的任意可能的实现方式中的方法的单元。

第十五方面，提供了一种通信系统，该通信系统包括路由管理设备和/或 AS 管理设备。例如，该通信系统包括上述第三方面、第五方面、第十三方面中任一项提供的路由管理设备，或该通信系统包括上述第四方面、第六方面、第十四方面中任一项提供的 AS 管理设备。

附图说明

图 1 为本申请实施例提供的路由劫持误判场景示意图；

图 2 为本申请实施例提供的一种网络系统示意图；
图 3a 为本申请实施例提供的一种路由管理方法示意图；
图 3b 为本申请实施例提供的一种 AS 管理方法示意图；
图 4 为本申请实施例提供的一种协议数据单元格式示意图；
图 5 为本申请实施例提供的一种防止落劫持误判方法示意图；
图 6 为本申请实施例提供的一种路由管理装置结构示意图；
图 7 为本申请实施例提供的一种路由管理装置结构示意图；
图 8 为本申请实施例提供的一种 AS 管理装置结构示意图；
图 9 为本申请实施例提供的一种网络设备结构示意图；
图 10 为本申请实施例提供的一种网络设备结构示意图；
图 11 为本申请实施例提供的一种路由管理系统结构示意图。

具体实施方式

本申请的实施方式部分使用的术语仅用于对本申请的具体实施例进行解释，而非旨在限定本申请。

本申请中术语“第一”“第二”“第三”等字样用于对作用和功能基本相同的相同项或相似项进行区分，应理解，“第一”、“第二”和“第三”之间不具有逻辑或时序上的依赖关系，也不对数量和执行顺序进行限定。

以下，介绍本申请涉及的术语：

兄弟 (Sibling) 自治系统 (Autonomous System, AS)：由同一个或不同组织进行管理或运营的两个或两个以上 AS 可以称为兄弟 AS。所述组织可以包括运营商、网络集团、网络服务提供商 (Internet Service Provider, ISP)、公司等等。下面对兄弟 AS 进行示例性介绍：

1. A 组织存在两个子组织，这两个子组织分别管理或运营的两个或两个以上 AS 可以为兄弟 AS。
2. A 组织负责为 B、C 组织运营网络，这两个组织分别有不同的 AS 标识，在某些情况下，如获得了 B、C 组织的同意时，也可以将 A 组织运营的属于 B、C 组织的 AS 认为兄弟 AS。
3. A 组织和 B 组织分别拥有和管理不同的网络，对应不同的 AS 标识，在某些情况下，如经 A、B 组织的同意等，也可以将 A、B 组织对应的 AS 标识认为兄弟 AS。

源 AS：在一个路由通告消息或者路由信息中，通常包括路由前缀和 AS 路径 (Path) 信息，该 AS path 信息可以携带在 BGP 的对应属性中，在 AS path 中，包括了源 AS 标识。在一个示例中，可以把在 AS path 上的最后边第一个 AS 标识视为该路由前缀的源 AS，即，表明该路由前缀由该源 AS 发布。在一个示例中，AS path 上的最后边第一个 AS 标识常常可以为 AS path 中的最右侧的 AS，如当 AS path 为 (123456567) 时，可以将 567 视为源 AS。如当 AS path 为 (ABC ABC DEF DEF GHI GHI) 时，可以将 GHI 视为源 AS。

相邻 AS：在路由消息的 AS path 中，两个 AS 标识如果为前后顺序，则可以认为该两个 AS 标识相邻，如当 AS path 为 (123 456 567) 时，可以认为 123 与 456 相邻，456 区别于 123、567 相邻，567 与 456 相邻。如当 AS path 为 (ABC ABC DEF DEF GHI GHI) 时，

可以认为 ABC 与 DEF 相邻, DEF 分别与 ABC、GHI 相邻, GHI 与 DEF 相邻。

路由劫持: 在路由通告的过程中, 路由通告报文, 即路由消息中对应的路由的 AS path 的信息可能会被修改, 当该路由的源 AS 标识 ID 被途经的其他 AS 域或设备修改为其他 ID 值后, 可以认为发生了路由劫持, 即该路由被修改后的源 AS 劫持了。关于路由劫持的相关内容, 还可以参考下方相关技术部分的详细描述。

路由泄漏: 在 AS 邻居商业关系中, 规定了路由信息的发布规则, 一旦一条路由中的 AS path 中包括的至少 2 个 AS 标识中的内容与路由信息的发布规则不符, 则认为可能发生了路由泄漏。关于路由泄漏的相关内容, 还可以参考下方相关技术部分的详细描述。

以下, 简单介绍本申请实施例涉及的相关技术:

当前互联网 (Internet) 基础设施主要包括: 域间路由系统, 如边界网关协议 (Border Gateway Protocol, BGP)、域名系统 (Domain Name System, DNS) 和公钥证书体系, 如公钥基础设施 (Public Key Infrastructure, PKI)。几乎所有的 Internet 服务都依赖于基础设施来保证网络连通性、服务可用性和服务可信性。

在这个架构下, 基于 BGP 路由的安全攻击每天都在发生, 每年都存在数万起攻击。如源劫持、路径劫持、路由泄露等。而 BGP 本身对路由学习并无安全认证机制, 为了解决 BGP 路由被劫持等问题, 业界提出了通过验证 BGP 路由起源是否正确的解决方案——资源公钥基础设施 (Resource Public Key Infrastructure, RPKI), 通过分布式的 RPKI 服务器收集各个互联网服务提供商 (Internet Service Provider, ISP) 发起的 BGP 路由起源 AS 标识、路由前缀、掩码等信息。路由器跟 RPKI 服务器建立连接, 在本地保存一份路由起源授权 (Route Origination Authorization, ROA) 数据, 用以验证从外部邻居收到的 BGP 前缀是否有效或合法, 确保其管理域内主机能够安全访问外部的服务。

路由劫持误判场景, 可以参见如下描述:

路由器从外部 BGP 邻居收到 BGP 路由更新报文, 在将该报文中的路由加入 BGP 路由表前先根据路由前缀和 AS 标识验证 Origin AS 的正确性, 则可以根据验证结果调整路由的属性, 影响 BGP 的选路结果。如果该路由的验证结果为有效, 则路由器可以根据标准定义的扩展团体属性, 把优选路由及验证结果, 通过 BGP 路由发布给其内部邻居。如果该路由的验证结果为无效, 则可能认为该路由被路由劫持了, 则丢弃该路由或者降低该路由的优选顺序。

下面通过一个示例来介绍路由劫持误判的情况, 图 1 为本申请实施例提供的路由劫持误判场景示意图, 如图 1 所示:

如 ISP1 存在两张网络, 其中骨干网的 AS 标识为 AS1, 城域网的 AS 标识为 AS11。在一些情况中, 该骨干网发布一个包含较大地址块的路由前缀 (例如 10.132.0.0/17), 并且安排该 ISP 的子网如城域网发布该路由前缀的子路由前缀, 例如将 10.132.51.0/24 分配给该城域网。

ISP1 为 AS1 签发了 ROA: 10.132.0.0/17-17, AS1, 该 ROA 可被理解为: 路由前缀: 10.132.0.0, 掩码: 17, 允许的最大掩码长度: 17, 源 AS: AS1。而 ISP1 未为子网签发 ROA, 如: 10.132.51.0/24。签发的 ROA 信息如表 1 所示:

表1

	AS	前缀 (Prefix) /掩码 (Mask)	签发ROA
骨干网	AS1	10.132.0.0/17	10.132.0.0/17-17, AS1
子网1	AS11	10.132.51.0/24	未签发

骨干网 AS1 和子网 1 AS11 在网络中发布各自的路由前缀后，这些路由前缀会被连接到 Internet 的各个网络通过路由消息接收到，如 ISP2 的网络，其 AS 标识为 AS2。

当启用 ROA 的网络如上述 ISP2 的网络中 AS2 的设备接收到上述 2 条路由前缀对应的路由消息后，对接收到的路由消息做起源验证：

路由消息 1：路由前缀：10.132.0.0/17，该路由消息中包括的 ASpath 为如：(AS11 AS1)，表明路由前缀 10.132.0.0/17 对应的源 AS 为 AS1。则设备可以使用 (AS1, 10.132.0.0/17) 去查询 ROA 数据库，命中 ROA 表项：10.132.0.0/17-17, AS1，验证结果为：有效 (Valid)。

路由消息 2：路由前缀：10.132.51.0/24，其路由消息中包括的 AS path 为如 (AS2, AS11)，表明路由前缀 10.132.51.0/24 对应的源 AS 为 AS11。使用 (AS11, 10.132.51.0/24) 去查询 ROA 数据库，没有被命中的 ROA 表项，验证结果为：无效 (Invalid)，则可判定为路由劫持。

在这种情况下，骨干网 AS1 和城域网 AS11 属于同一个公司，只是 IP 地址空间的分配和 ROA 注册存在问题，导致城域网的路由前缀发布之后被判定为“路由劫持”，实际这是一个假的“路由劫持”，但这可能随之会带来严重的网络连通性问题。

路由泄漏误判场景，可以参见如下描述：

基于商业利益最大化原则，ISP 网络采用的路由发布策略规则概括如下：

- 1) 来自 Customer AS 宣告的路由允许传递给 customer、peer 和 provider。
- 2) 来自 Peer AS 宣告的路由允许传递给 customer，不允许通告给其他的 peer 和 provider。
- 3) 来自 Provider AS 宣告的路由允许传递给 customer，不允许通告给其他的 peer 和 provider。

如果违反了如上路由发布策略，就可以认为是出现了路由泄露。在相关技术中，可能存在属于相同公司的不同 AS 之间传递路由，被误判为路由泄露的问题。如：一个 provider A，购买了 ProviderB 的服务。如 B 公司通告给 A 的一条路由消息，其路由前缀为：10.132.51.0/24，而其 AS 路径 (Path) 的值为 (AS1AS11AS2)，其中，AS2 为该路由前缀的源 AS，表明，该路由由 AS2 通告到了 AS11，再经 AS11 通告到了 AS1。其中 AS2 为 B 公司的 AS，AS11 为 providerA 的 AS 标识。在网络设备或路由分析系统基于商业关系分析路由时，认为 providerB 通告的路由可以传递给 provider A，但是不允许通告给其他的 peer 和 provider，判断该路由前缀被 AS11 泄漏给了 AS1。但是，在这个示例中，AS1 也为 provider A 的另一个网络的 AS 标识。但是在这种情况下，该路由会被确定（这里的确定也可以称为：

校验)为发生了路由泄漏,违反了路由通告规则,可能随之会带来严重的网络连通问题。

本申请实施例提供了一种AS管理的技术方案,通过构建兄弟AS(sibling AS)信息,提高AS管理方案信息的全面性,并进一步避免出现路由泄漏/路由劫持的误判等问题,在本技术方案中,设备上处理路由(路由劫持或路由泄漏)分析时,将sibling AS数据集(Dataset)作为考虑的关键因素之一,提升分析的准确度。

图2为本申请提供的一种网络场景示意图,在该网络场景中包括3个AS,AS1、AS11和AS2,其中AS1和AS11属于同一个ISP,即,AS1和AS2互为sibling AS。AS1中包括网络设备1,AS11中包括网络设备2,AS2中包括网络设备3和网络设备4,其中,网络设备1和网络设备2、网络设备3相连,网络设备2和网络设备1、网络设备3相连,网络设备3和网络设备1、网络设备2和网络设备4相连。可以将网络设备1和网络设备2视为网络设备3的外部边界网关协议(External Border Gateway Protocol)对等体(peer),其中,peer也可以被称为邻居。网络设备4和网络设备3可以互为内部边界网关协议(Internal Border Gateway Protocol, IBGP) peer。以上,网络设备1、网络设备2、网络设备3和网络设备4,可以为路由器、交换机或其他任何支持路由功能的物理或虚拟网络设备。该网络中还可以包括更多的AS或更多的网络设备,在此不再一一示出。可选的,该网络中还可以包括RPKI存储服务器(RPKI cache server),该RPKI服务器,也可以被称为RP服务器,如RP1、RP2、RPn。网络设备1、网络设备2或网络设备3可以从相连的RPKI cache server获得ROA信息,用于校验其获得的BGP路由消息是否有效。在图2中RPKI cache server的存放位置仅做示例,RPKI cache server可以由各个ISP自行部署。可选的,该网络中还可以包括路由分析设备,该路由分析设备包括控制器、网络管理设备或路由集中分析设备中的任意一个或多个。路由分析设备可以是具有路由分析功能的服务器、路由器等设备,其可以是具体的实体设备,也可以是虚拟设备。路由分析设备可以结合从各个网络设备或其他任何地方(如:管理人员输入或导入,或其他系统)获得的包括路由和AS path的路由信息以及包括AS标识的AS信息,进行路由分析。可选的,该网络中还可以包括信任锚(trust anchors, TA),该TA可以与RP服务器同步信息,使得RP能够从TA获得AS相关的各种信息。

以上,简单介绍了本申请实施例的相关技术,以下,对本申请的方法实施例进行示例性介绍。参见图3a,图3a是本申请实施例提供的一种路由管理方法的流程图,图3a所示的方法实施例300包括如下步骤:

S303:获得对应关系,所述对应关系包括第一AS标识和第二AS标识,该对应关系用于指示第一AS标识和第二AS标识为兄弟AS。

在一个示例中,设备可以在获得第一AS标识和第二AS标识之后,确定第一AS标识和第二AS标识为兄弟AS,并生成对应关系,该对应关系包括第一AS标识和第二AS标识,该对应关系表明第一AS标识和第二AS标识为兄弟AS。

在另一个示例中,设备也可以接收其他设备发送的消息,该消息中包括第一AS标识和第二AS标识,该消息用于指示第一AS标识和第二AS标识为兄弟AS。即,在这里,可以将设备接收到的该消息认为接收了上述对应关系。设备可以在接收到消息后保存该对应关系。也可以在接收到该消息后即使用该对应关系。

以上两种示例中的设备可以包括路由管理设备。

以下，结合图2所示的场景，示例性介绍设备获得对应关系的步骤，本步骤可以包括但不限于以下四种情况：

情况1、互联网注册管理机构（regional Internet registry, RIR）的TA获得第一AS标识和第二AS标识。

在一个示例中，该过程为：各个拥有AS标识的组织将自己的AS数据信息上报给自己所在的RIR。在一个示例中，这些组织上报的信息包括：组织标识（Organization Identifier），兄弟AS列表，在该兄弟AS列表中，包括该组织管理的多个AS标识，即：包括上述第一AS标识和第二AS标识。

在另一个示例中，RIR也可以在为组织分配AS之后，即将该第一AS标识和第二AS标识信息保存于TA中，生成上述对应关系。

情况2、RP服务器获得第一AS标识和第二AS标识。

RP服务器获得第一AS标识和第二AS标识的方式包括但不限于如下两种方式：

方式一：RP服务器或RP服务器对应的管理人员通过分析全球互联网（Internet）路由表、各种Internet公开数据，生成1个或多个具有sibling关系的AS信息，该AS信息中包括第一AS标识和第二AS标识。如，Internet路由表中，两条路由的前缀几乎相同，且对应的掩码位数仅相差2位，对应的源AS分别为AS1、AS2，则RP服务器可以通过该路由表确定AS和AS2为兄弟AS。如Internet公开了某公司拥有AS1，其子公司拥有AS2，则RP服务器可以通过该信息确定AS1和AS2为兄弟AS。如果是由管理人员分析得到的上述第一AS标识和第二AS标识，则管理人员可以通过配置的方式将该第一AS标识和第二AS标识配置到RP服务器上。即：RP服务器可以通过分析的方式或者接收手动配置的方式获得第一AS标识和第二AS标识。RP服务器自行分析的情况下，RP服务器中可以预置有相关程序代码分析获得上述对应关系。

方式二：RP服务器可以与一个或多个上述TA服务器相连，并获得各个TA服务器发送的第一AS标识和第二AS标识。在一个示例中，TA可能通过发送证书的方式发送该第一AS标识和第二AS标识。即：RP服务器可以从TA发送的证书中获得该第一AS标识和第二AS标识，并根据该信息中的如组织信息相同，或该信息中包括了指明第一AS标识和第二AS标识为兄弟AS，生成上述兄弟AS关系。

情况3、网络中的网络设备获得第一AS标识和第二AS标识。

应用于图2所示的场景中，该网络设备可以为图2中的网络设备1、网络设备2、网络设备3或网络设备4。

网络设备获得第一AS标识和第二AS标识的方式包括但不限于如下两种方式：

方式一：网络设备获得配置的第一AS标识和第二AS标识，如：接收管理人员通过网络管理系统、设备管理接口、命令行或其他形式配置的第一AS标识和第二AS标识，并将第一AS标识和第二AS标识配置为兄弟AS。

方式二：网络设备可以获得RP服务器发送的对应关系。

可选的，RP服务器向网络设备发送第一AS标识和第二AS标识时，可以通过RPKI路由协议（RPKI Router Protocol）将第一AS标识和第二AS标识信息发送给网络设备，RP服务器发送的消息表明第一AS标识和第二AS标识为兄弟AS，即，网络设备获得上述对应关系的方式

包括：接收RP服务器发送的该对应关系。RPKI路由协议的具体细节请参考扩展请求注解（Request For Comments, RFC）8210的定义，RFC8210的全部内容通过引用结合在本申请中。

在一个示例中，可以定义一个Sibling AS协议数据单元（protocol data unit, PDU），携带上述对应关系，该sibling AS PDU的格式可如图4所示。

其中各字段定义如下：

Protocol Version: 协议版本号，占1字节，其值为一个待标准组织正式分配的数值，目前已经分配到2。

PDU Type: 协议数据单元类型，占1字节，其值为一个待标准组织正式分配的数值，目前已经分配到 11。

zero1: 零区域1，可占2字节，可填充为0。

Length: 长度字段

zero2: 零区域2，可占1字节，可填充为0。

兄弟AS数量（Sibling AS Count）: 本PDU中封装Sibling AS的个数，可占2字节。

组织标识（Organization Identifier）: 占4字节。

Sibling Autonomous System Number(s): 一个或多个AS编号，这里的AS编号即本申请实施例中的AS标识，也可以将这个部分理解为兄弟AS列表，其包括的AS编号的个数由前面的Sibling AS Count确定，每个AS编号占4字节。

这里的Sibling AS PDU仅为对应关系携带方式可能的示例之一，格式可以变化，能在协议报文中携带表明第一AS标识和第二AS标识为兄弟AS的信息即可。

情况4、网络中的路由分析设备获得第一AS标识和第二AS标识。

同样，路由分析设备获得第一AS标识和第二AS标识的方式包括但不限于如下几种方式：

方式一：获得上述网络设备发送的上述第一AS标识和第二AS标识。在一个示例中，网络设备还发送与第一AS标识和第二AS标识对应的组织标识，路由分析设备可以通过获得的第一AS标识、第二标识和组织标识确定第一AS标识和第二AS标识为兄弟AS，并生成对应关系，指示第一AS标识和第二AS标识为兄弟AS。在另一个示例中，网络设备发送的消息中即包括了对应关系，该对应关系指示第一AS标识和第二AS标识为兄弟AS，路由分析设备从该消息获得对应关系。

方式二：获得RP服务器发送的上述第一AS标识和第二AS标识。在一个示例中，RP服务器还发送与第一AS标识和第二AS标识对应的组织标识，路由分析设备可以通过获得的第一AS标识、第二标识和组织标识确定第一AS标识和第二AS标识为兄弟AS，并生成对应关系，指示第一AS标识和第二AS标识为兄弟AS。在另一个示例中，RP服务器发送的消息中即包括了对应关系，该对应关系指示第一AS标识和第二AS标识为兄弟AS，路由分析设备从该消息获得该对应关系。

方式三：获得TA发送的上述第一AS标识和第二AS标识。在一个示例中，TA还发送与第一AS标识和第二AS标识对应的组织标识，路由分析设备可以通过获得的第一AS标识、第二标识和组织标识确定第一AS标识和第二AS标识为兄弟AS，并生成对应关系，指示第一AS标识和第二AS标识为兄弟AS。在另一个示例中，T发送的消息中即包括了对应关系，该对应关

系指示第一AS标识和第二AS标识为兄弟AS，路由分析设备从该消息获得该对应关系。

方式四：获得管理人员配置的对应关系，该对应关系包括上述第一AS标识和第二AS标识。

方式五：获得各组织的人员上报的第一AS标识和第二AS标识，并通过获得的第一AS标识和第二标识生成对应关系，或从上报的消息中获得该对应关系。

这几种方式与上述3种情况中获得第一AS标识和第二AS标识的相关部分的内容类似，本申请在此不再赘述。

以上，当获得第一AS标识和第二AS标识的方式有多种时，也可以通过以上的多种方式获得对应关系，以及更多的SiblingAS信息。

在一个示例中，当设备接收到相关设备发送的第一AS标识和第二AS标识时，该信息可能为加密信息，设备可以通过解密等操作获得明文的第一AS标识和第二AS标识。

可选的，该第一AS标识和第二AS标识携带在兄弟AS列表中。

设备可以通过一个消息中获得第一AS标识和第二AS标识，也可以通过不同的消息获得第一AS标识和第二AS标识。当设备通过同一个消息获得第一AS标识和第二AS标识时，设备可能在获得第一AS标识或第二AS标识时即确定该第一AS标识和第二AS标识为兄弟AS。当设备通过不同的消息获得第一AS标识和第二AS标识时，设备也可以根据其他相关的信息分析出第一AS标识和第二AS标识为兄弟AS。如根据第一AS标识和第二AS标识对应的组织信息相同、或第一AS标识与第二AS标识相关的路由前缀信息是包括关系等等。

对应于上述多种情况，设备在获得上述对应关系之后，可以保存相应的对应关系，表明第一AS和第二AS为兄弟AS。以上情况1-情况4中的设备生成的对应关系的方式类似，在此仅做示例性介绍，不再针对各种情况一一赘述。在一个示例中，该保存的对应关系包括第一AS标识和第二AS标识，该对应关系可以被称为siblingAS dataset，其形式可如下表1所示：

表1

Organization Identifier (ID)	Sibling AS号 (Numbers)
ID1	AS11 AS12 AS13
ID2	AS21 AS22
ID3	AS31 AS32 AS33 AS34
...	...

如第一行所示，组织ID为ID1的组织，其包括有3个AS号：AS11，AS12和AS13，这3个AS互为兄弟AS，即第一AS标识和第二AS标识可以为其中的任意一个AS。其中，AS号为AS标识的一种具体示例。如第二行所示，组织ID为ID2的组织，其包括有2个AS：AS21和AS22，这2个AS互为兄弟AS，即第一AS标识和第二AS标识可以为其中的任意一个AS。如第三行所示，组织ID为ID3的组织，其包括有4个AS：AS31，AS32，AS33和AS34，这4个AS互为兄弟AS，

即第一AS标识和第二AS标识可以为其中的任意一个AS。

应用到图2所示的场景中，网络设备3保存的对应关系可如下表2所示：

表2

Organization Identifier	Sibling AS Number (s)
ID1	AS1 AS11

其表明AS1和AS2为ID号为ID1组织的兄弟AS，其中第一AS标识可以为AS1，也可以为AS2，第二AS标识为该兄弟AS列表中的与第一AS标识不同的任一AS。

在另一个可能的示例中，设备保存的对应关系还可如下表3所示：

表3

Prefix/mask	源AS	Sibling AS Number (s)
10.132.0.0/17	AS1	AS11

其表明，AS1为发布10.132.0.0/17的源AS，而AS11为AS1的兄弟AS。在这种示例中，设备在接收的消息中还可以包括该路由前缀，或设备已获得该路由前缀和源AS信息。

在另一个可能的示例中，设备保存的对应关系还可如下表4和表5所示：

表4

Organization Identifier	AS Number
ID1	AS1

表5

Organization Identifier	AS Number
ID1	AS11

表4表明，ID1的组织对应AS号为AS1，表5表明，ID1的组织对应的AS号为AS11。即，设备获得的对应关系可以是直接通过一个表或一个具体的形式表示，也可以通过两个或两个以上的表或其他任何形式表示。只要该设备可以通过对应关系确定两个AS为AS兄弟AS即可。

S305：根据对应关系进行路由管理。

设备获得上述兄弟AS的对应关系后，可以基于该对应关系进行路由管理，设备基于对应关系进行路由管理包括该设备进行直接的路由管理或进行间接的路由管理。

在一个示例中，设备进行间接的路由管理可以包括：设备在获得对应关系后，还发送该对应关系给其他设备，比如路由分析设备，使得接收该对应关系的设备可以基于该对应关系进行直接的路由管理，如路由分析。如网络设备3可以将其获得的对应关系发送给路由分析设备，使得路由分析设备可以根据该对应关系进行路由分析。或RP服务器可将其获得的对应关系发送给网络设备3，使得网络设备3可以根据该对应关系进行路由消息校验。

在另一个示例中，设备根据该对应关系进行直接的路由管理可以包括：根据对应关系

进行路由分析，以减少由于设备上的AS信息不足，导致的分析不全面、或路由劫持、路由泄漏误判等情况。下面结合S307-S311对这种直接路由管理的场景进行介绍。

S307: 获得路由消息，该路由消息包括路由前缀和第三AS标识。

设备在执行S305之前，可以先执行S307。

对应于以上情况1-情况4中的各种设备获得路由消息的方式类似，包括但不限于以下一种或多种：接收其他设备，如网络设备发送的路由消息，或获得管理人员导入、配置的一条或多条路由消息。获得的路由消息中包括路由前缀和第三AS标识。在一个示例中该路由消息为BGP更新消息。设备在获得路由消息后，可以存储该路由消息以备使用或校验，或是，在接收到该路由消息后即进行校验。

本申请对S307与S303的执行顺序不做限定，即，设备可以先获得第一AS标识和第二AS标识，也可以先获得路由消息。

在一个示例中，设备进行直接的路由管理可以包括以下内容，即S305可以包括以下S309和/或S311。

S309: 根据ROA或商业关系信息校验路由消息无效。

设备可以根据获得的ROA信息校验路由消息中包括的路由前缀是否被路由劫持。在这种场景中，第三AS标识为该路由消息中的源AS。

在设备获得的ROA信息中也包括一个路由前缀，为便于理解，将设备获得路由消息中的路由前缀称为第一路由前缀，将设备获得的ROA中的路由前缀称为第二路由前缀。该第一路由前缀与第二路由前缀对应，这些路由前缀中均包括掩码，这里的两个路由前缀对应可理解为：第一路由前缀和第二路由前缀的掩码长度不同，但其对应的IP地址范围为包含关系，即：第二路由前缀可最长匹配到第一路由前缀，或第一路由前缀可最长匹配到第二路由前缀。

示例A: 如上相关技术部分所述的路由劫持误判场景中，设备根据ROA信息错误的校验该路由前缀10.132.51.0/24被AS11劫持。

设备也可以根据商业关系信息校验该路由消息是否发生了路由泄漏。在这种场景中，第三AS标识为该路由消息中的被判定为泄漏了路由的AS。该路由消息中还包括第四AS，该第四AS可以为该路由消息中的源AS，也可以为该与第三AS标识相邻，在该第三AS标识之后的AS。

下面，示例性介绍AS的相邻和前后关系，如：AS path为(AS1AS11AS2)，则可以认为AS1和AS11相邻，AS11和AS2相邻，其中，AS1在AS11之后，AS11在AS2之后。这里的前后主要以该路由前缀通告经过的AS的顺序来定义。即，在这个示例中，路由前缀的通告路径为：起源于AS2，后通告给AS11，后经AS11通告给AS1。

示例B: 在如上相关技术部分所述的路由泄漏误判场景中，设备根据商业关系信息错误的校验该路由前缀10.132.51.0/24，该路由消息中的as path为(AS1AS11AS2)，设备校验该路由前缀由AS11泄漏给了AS1。即在这个示例中，该第三AS标识为AS11，第四AS为AS1。

示例C: 假设该路由消息的路由前缀为10.132.51.0/24，该路由消息中的AS path为(AS1AS2 AS11)，其中，AS1和AS11属于同一个组织，为兄弟AS。而该路由前缀被校验为由AS2泄漏给了AS1。

可选的，设备在校验该路由消息无效后，还将该路由消息的校验状态修改为无效。

S311：根据对应关系校验路由消息是否有效。

设备在接收到路由消息后、校验路由消息无效后或需要进行路由分析时，可以根据上述步骤S305部分生成的对应关系校验该路由消息是否有效。

设备可以在校验路由消息无效后执行本步骤，也可以不执行S309而执行本步骤，在这种情况下，该对应关系可如表3所示，则设备可有根据路由前缀和兄弟AS的关系，确定该路由消息有效。

下面结合步骤S309中的示例进行对本步骤进行讲解。

对应于示例A：设备可以在校验路由前缀10.132.51.0/24被AS11劫持之后。根据ROA中该路由前缀的源AS应该为AS1，进一步的根据表2所示的对应关系，通过AS11和AS1为兄弟AS，而确定该路由消息有效，未被路由劫持。即，在这里，该对应关系中的第一AS标识为AS11，第二AS标识为AS1，ROA中包括的源AS为上述第二AS标识，即：AS1，其路由前缀为10.132.0.0/17。路由消息中的第三AS标识为AS11。设备可以根据第三AS标识和第一AS标识相等，第一AS标识和第二AS标识为兄弟AS，确定该路由消息有效，未被路由劫持。

对应于示例B：设备可以在校验该路由前缀10.132.51.0/24由AS11泄漏给了AS1之后。进一步的根据表2所示的对应关系，通过AS11和AS1为兄弟AS，而确定该路由消息有效，未发生路由泄漏。即，在这里，该对应关系中的第一AS标识为AS11，第二AS标识为AS1。路由消息中包括的第三AS标识为AS11，第四AS为AS1。设备可以根据第四AS和第一AS标识相同，第三AS标识和第二AS标识相同，第一AS标识和第二AS标识为兄弟AS，确定该路由消息有效，未发生路由泄漏。

可选的，该第三AS标识也可以为该路由消息中路由前缀对应的源AS。即，该路由消息中可以仅包括上述第三AS标识和第四AS。

对应于示例C：设备可以在校验该路由前缀10.132.51.0/24由AS2泄漏给了AS1之后。进一步的根据表2所示的对应关系，通过AS11和AS1为兄弟AS，而确定该路由消息有效，未发生路由泄漏。即，在这里，该对应关系中的第一AS标识为AS11，第二AS标识为AS1。路由消息中包括的第三AS标识为AS11，第四AS为AS1。设备可以根据第四AS和第一AS标识相同，第三AS标识和第二AS标识相同，第一AS标识和第二AS标识为兄弟AS，确定该路由消息有效，未发生路由泄漏。

以上，设备校验路由消息的方式包括S309和S311两个步骤中的一种或多种，即设备可以先执行S309，后执行S311；也可以不执行S309，而执行S311；或是在执行S311的过程中，还根据ROA或商业关系信息校验路由消息。

以上，示例性介绍了采用本申请实施例的技术方案为基础的路由管理方法。参见图3b，图3b是本申请实施例提供的一种AS管理方法的流程图，图3b所示的方法实施例400包括如下步骤：

本方法可以应用于AS管理设备，方法实施例300中的路由管理设备也可以是AS管理设备。AS管理设备也可以是方法实施例300中的路由管理设备。

S401：获得第一AS标识和第二AS标识。

AS管理设备获得第一AS标识和第二AS标识，并确定第一AS标识和第二AS标识为兄弟AS。

AS管理设备获得第一AS标识和第二AS标识的方式，可以参考上述方法300中路由管理设备获得第一AS标识和第二AS标识的相关描述，本申请在此不再赘述。

S402：发送消息，该消息中包括第一AS标识和第二AS标识，该消息用于指示第一AS标识和第二AS标识为兄弟AS。

AS管理设备向接收设备发送消息，该消息中包括第一AS标识和第二AS标识，该消息用于指示第一AS标识和第二AS标识为兄弟AS。该消息可以用于使接收设备根据该消息获得对应关系，使得接收设备根据该消息对路由消息进行直接的路由管理，如路由分析等。

AS管理设备发送指示第一AS标识和第二AS标识为兄弟AS的消息的方式的详细描述，可以参见方法实施例300中的相关描述，在此不再赘述。

下面，结合图5所示的路由管理方法流程图详细介绍将上述方法实施例300和方法实施例400的方法应用于防路由劫持误判的场景，图5所示的方法实施例500包括如下步骤：

在本方法实施例中，以RP服务器作为AS管理设备，第一网络设备作为路由管理设备进行示例性讲解。应理解，AS管理设备可以是上述方法实施例300中提到的RP服务器、TA服务器、网络设备、路由分析设备或其他具备AS管理功能的设备，路由管理设备也可以是上述方法实施例300中提到的RP服务器、TA服务器、网络设备、路由分析设备或其他具备路由管理功能的设备。

S501：RP服务器向第一网络设备发送第一消息，第一消息中包括第一AS标识和第二AS标识。

应用于图2所示的场景中，以网络设备3为第一网络设备，RP服务器为此处的服务器对方法实施例500进行示例性讲解。

RP服务器通过上述图3a所述的方法实施例300（下面简称方法300）中的RPKI路由协议向网络设备3发送该第一消息。该第一消息可以包括sibling AS PDU，该PDU中还可以包括兄弟AS数、组织标识等信息。

该第一消息用于指示该第一AS标识和第二AS标识为sibling AS。

S503：第一网络设备获得对应关系。

网络设备3接收该第一消息，并从该第一消息中获得上述对应关系，并保存上述对应关系，该对应关系用于指示第一AS标识和第二AS标识为兄弟AS。

以上步骤S501和S503的详细描述详见方法300中步骤S303处的相关描述，在此不再赘述。

S507：第二网络设备向第一网络设备发送路由消息，该路由消息包括第一路由前缀和第三AS标识。

相应的，第一网络设备接收第二网络设备发送的该路由消息。

应用于图2所示的场景中，第二网络设备可以为网络设备1。则网络设备3可以接收网络设备1发送的路由消息，该路由消息可以为BGP更新消息。在该更新消息中，该路由前缀可以为10.132.51.0/24，该更新消息中的as path可为(AS1, AS11)。该路由消息表明AS11为10.132.51.0/24的源AS，经网络设备2通告到AS1后，再经网络设备1通告到网络设备3。在这个示例中第三AS标识即为AS11。

S509：第一网络设备根据获得的ROA信息校验该路由消息是否有效。如果无效，则执行步骤S511。

本步骤为可选步骤。关于网络设备3如何根据获得ROA信息以及如何根据获得的ROA信息校验该路由消息无效的详细描述可参见上方方法300中步骤S309处的描述，在此不再赘述。

可选的，网络设备3在校验该路由消息无效后，可能将该路由消息对应的路由信息的校验状态置为无效。在相关技术中，如果无下述步骤S511~S513等，则网络设备3可能根据该检验状态为无效而降低该路由消息的优先级，进而不通告该路由。或网络设备3也可能向其BGP对等体等设备通告该路由，并在通告该路由时，将该路由的某个属性，如原始路由属性置为无效。

S511：第一网络设备根据对应关系确定该路由消息有效。

关于网络设备3如何根据对应关系确定该路由消息有效，可参见方法300步骤S311处的相关描述，本申请在此不再赘述。

S513：第一网络设备将该路由消息的状态置为有效。

网络设备3可以在S309中将该路由信息的校验状态置为无效之后，在本步骤可以再将该路由信息的检验状态置为有效。

如果网络设备3需要向其对等体通告该路由信息，则网络设备3可以将通告该路由信息的路由消息中的相关属性部分的状态置为有效。

S515：第一网络设备向第三网络设备发送该路由消息。

可选的，当网络设备3还需要向其对等体通告上述路由消息对应的路由信息时，则网络设备3可以向其对等体，如图2中的网络设备4发送该路由消息，即发送该路由消息对应的路由信息。

以上，主要以AS标识为示例介绍了本申请实施例，应理解，本方案也可以应用于其他类似或相关场景，如，其他非BGP自治系统的场景、或其他已经存在或未来可能存在的分域管理的场景。

图6是本申请实施例提供的一种路由管理装置600的结构示意图，装置600具有上述方法300的路由管理设备，或方法500中的第一网络设备的任意功能。如图6所示，装置600包括：处理单元601，用于执行S303、S305、S509、S511或S513等；可选的，该装置600还包括：接收单元602，用于执行S303、S503中的接收包括第一AS标识和第二AS标识的相关步骤或接收路由消息的相关步骤；发送单元603，用于执行S515。

路由管理装置600对应于上述方法实施例中的路由管理设备，如：第一网络设备，路由管理装置600中的各模块和上述其他操作和/或功能分别为了实现方法实施例中的路由管理设备所实施的各种步骤和方法，具体细节可参见上述方法300或方法500，为了简洁，在此不再赘述。

路由管理装置600在进行路由管理时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将路由管理装置600的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。

如图7所示，图7是本申请实施例提供的一种路由管理装置700的一种结构示意图，装置700具有上述方法300的路由管理设备，或方法500中的第一网络设备的任意功能。装置700包括BGP模块、路由校验模块和RPKI模块，其中，RPKI模块可以用于执行S303、S503中的接收包括第一AS标识和第二AS标识的相关步骤或接收路由消息的相关步骤和

获得对应关系的对应步骤；路由校验模块可用于执行 S305、S509、S511 或 S513 等，BGP 模块可用于执行 S507、S515 等步骤。将装置 700 与装置 600 对应，则可以认为装置 600 的接收单元 602 和发送单元 603 可以包括装置 700 的 BGP 模块和 RPKI 模块，装置 700 的 BGP 模块和 RPKI 模块可以具备收发功能，装置 600 的处理单元 601 可以包括装置 700 的路由校验模块。装置 700 是对上述方法实施例中的路由管理设备和第一网络设备的另一种装置划分模式。路由管理装置 700 中的各模块和上述其他操作和/或功能分别为了实现方法实施例中的路由管理设备所实施的各种步骤和方法，具体细节可参见上述方法 300 或方法 500，为了简洁，在此不再赘述。

图 8 是本申请实施例提供的一种 AS 管理装置 800 的结构示意图，装置 800 具有上述方法 400 的 AS 管理设备，或方法 500 中的 RP 服务器的任意功能。如图 8 所示，装置 800 包括：处理单元 801，用于执行 S401，获得第一 AS 标识和第二 AS 标识的相关步骤，发送单元 803，用于执行 S402 或 S501。可选的，装置 800 还包括接收单元 802，用于接收其他设备发送的第一 AS 标识和第二 AS 标识。

装置 800 对应于上述方法实施例 400 中和方法实施例 500 中的 AS 管理设备，如 RP 服务器，装置 800 中的各模块和上述其他操作和/或功能分别为了实现方法实施例中的 AS 管理设备所实施的各种步骤和方法，具体细节可参见上述方法 400 或方法 500，为了简洁，在此不再赘述。

装置 800 在进行 AS 管理时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置 800 的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的装置 800 与上述方法 400 或方法 500 属于同一构思，其具体实现过程详见方法 400 或方法 500，这里不再赘述。

与本申请提供的方法实施例以及虚拟装置实施例相对应，本申请实施例还提供了一种网络设备，下面对网络设备的硬件结构进行介绍。

下面描述的网络设备 900 或网络设备 1000 对应于上述方法实施例中的路由管理设备或 AS 管理设备，网络设备 900 或网络设备 1000 中的各硬件、模块和上述其他操作和/或功能分别为了实现方法实施例中的网络设备 900 或网络设备 1000 所实施的各种步骤和方法，关于网络设备 900 或网络设备 1000 如何基于兄弟 AS 实现 AS 管理或路由管理的详细流程，具体细节可参见上述方法实施例，为了简洁，在此不再赘述。其中，上文方法 300、方法 400 或方法 500 的各步骤通过网络设备 900 或网络设备 1000 处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以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，处理器读取存储器中的信息，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。

网络设备 900 或网络设备 1000 对应于上述虚拟装置实施例中的装置 600、装置 700 或装置 800，装置 600、装置 700 或装置 800 中的每个功能模块采用网络设备 900 或网络设备 1000 的软件实现。换句话说，装置 600、装置 700 或装置 800 包括的功能模块为网络设

备 900 或网络设备 1000 的处理器读取存储器中存储的程序代码后生成的。

参见图 9，图 9 示出了本申请一个示例性实施例提供的网络设备 900 的结构示意图，该网络设备 900 可以配置为路由管理设备或 AS 管理网络设备。该网络设备 900 可以由一般性的总线体系结构来实现。

网络设备 900 包括至少一个处理器 901、通信总线 902、存储器 903 以及至少一个通信接口 904。

处理器 901 可以是一个通用 CPU、NP、微处理器、或者可以是一个或多个用于实现本申请方案的集成电路，例如，专用集成电路（application-specific integrated circuit, ASIC），可编程逻辑器件（programmable logic device, PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic device, CPLD），现场可编程逻辑门阵列（field-programmable gate array, FPGA），通用阵列逻辑（generic array logic, GAL）或其任意组合。

通信总线 902 用于在上述组件之间传送信息。通信总线 902 可以分为地址总线、数据总线、控制总线等。为便于表示，图中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 903 可以是只读存储器（read-only memory, ROM）或可存储静态信息和指令的其它类型的静态存储设备，也可以是随机存取存储器（random access memory, RAM）或者可存储信息和指令的其它类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only Memory, EEPROM）、只读光盘（compact disc read-only memory, CD-ROM）或其它光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其它磁存储设备，或者是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其它介质，但不限于此。存储器 903 可以是独立存在，并通过通信总线 902 与处理器 901 相连接。存储器 903 也可以和处理器 901 集成在一起。

通信接口 904 使用任何收发器一类的装置，用于与其它设备或通信网络通信。通信接口 904 包括有线通信接口，还可以包括无线通信接口。其中，有线通信接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线通信接口可以为无线局域网（wireless local area networks, WLAN）接口，蜂窝网络通信接口或其组合等。

在具体实现中，作为一种实施例，处理器 901 可以包括一个或多个 CPU，如图 9 中所示的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，网络设备 900 可以包括多个处理器，如图 9 中所示的处理器 901 和处理器 905。这些处理器中的每一个可以是一个单核处理器（single-CPU），也可以是一个多核处理器（multi-CPU）。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（如计算机程序指令）的处理核。

在具体实现中，作为一种实施例，网络设备 900 还可以包括输出设备 906 和输入设备 907。输出设备 906 和处理器 901 通信，可以以多种方式来显示信息。例如，输出设备 906 可以是液晶显示器（liquid crystal display, LCD）、发光二极管（light emitting diode, LED）显示设备、阴极射线管（cathode ray tube, CRT）显示设备或投影仪（projector）等。输入设备 907 和处理器 901 通信，可以以多种方式接收用户的输入。例如，输入设备 907 可以是

鼠标、键盘、触摸屏设备或传感设备等。

在一些实施例中，存储器 903 用于存储执行本申请方案的程序代码 910，处理器 901 可以执行存储器 903 中存储的程序代码 910。也即是，网络设备 900 可以通过处理器 901 以及存储器 903 中的程序代码 910，来实现方法实施例提供的方法 300、方法 400 或方法 500。

本申请实施例的网络设备 900 可对应于上述各个方法实施例中的路由管理设备或 AS 管理设备，并且，该网络设备 900 中的处理器 901、通信接口 904 等可以实现上述各个方法实施例中的设备所具有的功能和/或所实施的各种步骤和方法。为了简洁，在此不再赘述。

装置 600 中的接收单元 602、发送单元 603 可以相当于网络设备 900 中的通信接口 904；装置 600 的处理单元 501 可以相当于网络设备 900 中的处理器 901。

装置 800 中的接收单元 802、发送单元 803 可以相当于网络设备 900 中的通信接口 904；装置 800 中的处理单元 801 可以相当于网络设备 900 中的处理器 901。

参见图 10，图 10 示出了本申请一个示例性实施例提供的网络设备 1000 的结构示意图，该网络设备 1000 可以配置为路由管理设备或 AS 管理设备。网络设备 1000 包括：主控板 1010 和接口板 1030。

主控板 1010 也称为主处理单元（main processing unit，MPU）或路由处理卡（route processor card），主控板 1010 用于对网络设备 1000 中各个组件的控制和管理，包括路由计算、设备管理、设备维护、协议处理功能。主控板 1010 包括：中央处理器 1011 和存储器 1012。

接口板 1030 也称为线路接口单元卡（line processing unit，LPU）、线卡（line card）或业务板。接口板 1030 用于提供各种业务接口并实现数据包的转发。业务接口包括但不限于以太网接口、POS(Packet over SONET/SDH)接口等，以太网接口例如是灵活以太网业务接口(Flexible Ethernet Clients, FlexE Clients)。接口板 1030 包括：中央处理器 1031、网络处理器 1032、转发表项存储器 1034 和物理接口卡（physical interface card，PIC）1033。

接口板 1030 上的中央处理器 1031 用于对接口板 1030 进行控制管理并与主控板 1010 上的中央处理器 1011 进行通信。

网络处理器 1032 用于实现报文的转发处理。网络处理器 1032 的形态可以是转发芯片。具体而言，网络处理器 1032 用于基于转发表项存储器 1034 保存的转发表转发接收到的报文，如果报文的地址为网络设备 1000 的地址，则将该报文上送至 CPU（如中央处理器 1011）处理；如果报文的地址不是网络设备 1000 的地址，则根据该地址从转发表中查找到该地址对应的下一跳和出接口，将该报文转发到该地址对应的出接口。其中，上行报文的处理包括：报文入接口的处理，转发表查找；下行报文的处理：转发表查找等等。

物理接口卡 1033 用于实现物理层的对接功能，原始的流量由此进入接口板 1030，以及处理后的报文从该物理接口卡 1033 发出。物理接口卡 1033 也称为子卡，可安装在接口板 1030 上，负责将光电信号转换为报文并对报文进行合法性检查后转发给网络处理器 1032 处理。在一些实施例中，中央处理器也可执行网络处理器 1032 的功能，比如基于通用 CPU 实现软件转发，从而物理接口卡 1033 中不需要网络处理器 1032。

可选地，网络设备 1000 包括多个接口板，例如网络设备 1000 还包括接口板 1040，接口板 1040 包括：中央处理器 1041、网络处理器 1042、转发表项存储器 1044 和物理接口卡 1043。

可选地，网络设备 1000 还包括交换网板 1020。交换网板 1020 也可以称为交换网板单元 (switch fabric unit, SFU)。在网络设备有多个接口板 1030 的情况下，交换网板 1020 用于完成各接口板之间的数据交换。例如，接口板 1030 和接口板 1040 之间可以通过交换网板 1020 通信。

主控板 1010 和接口板 1030 耦合。例如。主控板 1010、接口板 1030 和接口板 1040，以及交换网板 1020 之间通过系统总线与系统背板相连实现互通。在一种可能的实现方式中，主控板 1010 和接口板 1030 之间建立进程间通信协议 (inter-process communication, IPC) 通道，主控板 1010 和接口板 1030 之间通过 IPC 通道进行通信。

在逻辑上，网络设备 1000 包括控制面和转发面，控制面包括主控板 1010 和中央处理器 1031，转发面包括执行转发的各个组件，比如转发表项存储器 1034、物理接口卡 1033 和网络处理器 1032。控制面执行路由器、生成转发表、处理信令和协议报文、配置与维护设备的状态等功能，控制面将生成的转发表下发给转发面，在转发面，网络处理器 1032 基于控制面下发的转发表对物理接口卡 1033 收到的报文查表转发。控制面下发的转发表可以保存在转发表项存储器 1034 中。在有些实施例中，控制面和转发面可以完全分离，不在同一设备上。

如果网络设备 1000 被配置为路由管理设备，物理接口卡 1033 接收携带第一 AS 标识和第二 AS 标识的消息，发送给网络处理器 1032，网络处理器 1032 根据该消息，获得对应关系等信息，在根据该对应关系对路由消息处理后，将路由消息从物理接口卡 1033 发送出去。

如果网络设备 1000 被配置为 AS 管理设备，物理接口卡 1033 接收第一 AS 标识和第二 AS 标识，发送给网络处理器 1032，网络处理器 1032 确定该第一 AS 标识和第二 AS 标识为兄弟 AS，并生成消息，并将该消息通过物理接口卡 1033 发送给路由管理设备。

装置 600 中的接收单元 602、发送单元 603 相当于网络设备 1000 中的物理接口卡 1033；网络设备 1000 中的处理单元 601 可以相当于网络处理器 1032 或中央处理器 1011。

装置 800 中的接收单元 802、发送单元 803 相当于网络设备 1000 中的物理接口卡 1033；装置 800 中的处理单元 602 可以相当于网络处理器 1032 或中央处理器 1011。

本申请实施例中接口板 1040 上的操作与接口板 1030 的操作一致，为了简洁，不再赘述。本实施例的网络设备 1000 可对应于上述各个方法实施例中的路由管理设备或 AS 管理设备，该网络设备 1000 中的主控板 1010、接口板 1030 和/或 1040 可以实现上述各个方法实施例中的路由管理设备或 AS 管理设备所具有的功能和/或所实施的各种步骤，为了简洁，在此不再赘述。

值得说明的是，主控板可能有一块或多块，有多块的时候可以包括主用主控板和备用主控板。接口板可能有一块或多块，网络设备的数据处理能力越强，提供的接口板越多。接口板上的物理接口卡也可以有一块或多块。交换网板可能没有，也可能有一块或多块，有多块的时候可以共同实现负荷分担冗余备份。在集中式转发架构下，网络设备可以不需

要交换网板，接口板承担整个系统的业务数据的处理功能。在分布式转发架构下，网络设备可以有至少一块交换网板，通过交换网板实现多块接口板之间的数据交换，提供大容量的数据交换和处理能力。所以，分布式架构的网络设备的数据接入和处理能力要大于集中式架构的设备。可选地，网络设备的形态也可以是只有一块板卡，即没有交换网板，接口板和主控板的功能集成在该一块板卡上，此时接口板上的中央处理器和主控板上的中央处理器在该一块板卡上可以合并为一个中央处理器，执行两者叠加后的功能，这种形态设备的数据交换和处理能力较低(例如，低端交换机或路由器等网络设备)。具体采用哪种架构，取决于具体的组网部署场景，此处不做任何限定。

在一些可能的实施例中，上述路由管理设备或 AS 管理设备可以实现为虚拟化设备。

例如，虚拟化设备可以是运行有用于发送报文功能的程序的虚拟机(英文：Virtual Machine, VM)，虚拟机部署在硬件设备上(例如，物理服务器)。虚拟机指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。可以将虚拟机配置为第一网络设备或第二网络设备。例如，可以基于通用的物理服务器结合网络功能虚拟化(Network Functions Virtualization, NFV)技术来实现路由管理设备或 AS 管理设备。路由管理设备或 AS 管理设备为虚拟主机、虚拟路由器或虚拟交换机。本领域技术人员通过阅读本申请即可结合 NFV 技术在通用物理服务器上虚拟出具有上述功能的路由管理设备或 AS 管理设备。此处不再赘述。

例如，虚拟化设备可以是容器，容器是一种用于提供隔离的虚拟化环境的实体，例如，容器可以是 docker 容器。可以将容器配置为路由管理设备或 AS 管理设备。例如，可以通过对应的镜像来创建出路由管理设备或 AS 管理设备，例如可以通过 proxy-container (提供代理服务的容器)的镜像，为 proxy-container 创建 2 个容器实例，分别是容器实例 proxy-container1、容器实例 proxy-container2，将容器实例 proxy-container1 提供为路由管理设备，将容器实例 proxy-container2 提供为 AS 管理设备。采用容器技术实现时，路由管理设备或 AS 管理设备可以利用物理机的内核运行，多个路由管理设备或 AS 管理设备可以共享物理机的操作系统。通过容器技术可以将不同的路由管理设备或 AS 管理设备隔离开来。容器化的路由管理设备或 AS 管理设备可以在虚拟化的环境中运行，例如可以在虚拟机中运行，容器化的路由管理设备或 AS 管理设备也可以直接在物理机中运行。

例如，虚拟化设备可以是 Pod，Pod 是 Kubernetes (Kubernetes 是谷歌开源的一种容器编排引擎，英文简称为 K8s) 为部署、管理、编排容器化应用的基本单位。Pod 可以包括一个或多个容器。同一个 Pod 中的每个容器通常部署在同一主机上，因此同一个 Pod 中的每个容器可以通过该主机进行通信，并且可以共享该主机的存储资源和网络资源。可以将 Pod 配置为路由管理设备或 AS 管理设备。例如，具体地，可以指令容器即服务(英文全称：container as a service，英文简称：CaaS，是一种基于容器的 PaaS 服务)来创建 Pod，将 Pod 提供为路由管理设备或 AS 管理设备。

当然，路由管理设备或 AS 管理设备还可以是其他虚拟化设备，在此不做一一列举。

在一些可能的实施例中，上述路由管理设备或 AS 管理设备也可以由通用处理器来实现。例如，该通用处理器的形态可以是一种芯片。具体地，实现路由管理设备或 AS 管理设备的通用处理器包括处理电路和与该处理电路内部连接通信的输入接口以及输出接口，该

处理电路用于通过输入接口执行上述各个方法实施例中的报文的生成步骤，该处理电路用于通过输入接口执行上述各个方法实施例中的接收步骤，该处理电路用于通过输出接口执行上述各个方法实施例中的发送步骤。可选地，该通用处理器还可以包括存储介质，该处理电路用于通过存储介质执行上述各个方法实施例中的存储步骤。存储介质可以存储处理电路执行的指令，该处理电路用于执行存储介质存储的指令以执行上述各个方法实施例。

参见图 11，本申请实施例提供了一种网络系统 1100，所述系统 1100 包括：路由管理设备 1101 和/或 AS 管理设备 1102。可选的，路由管理设备 1101 为如装置 600、装置 700、网络设备 900 或网络设备 1000，AS 管理设备 1102 为如装置 800、网络设备 900 或网络设备 1000。

本申请实施例提供了一种计算机程序产品，当该计算机程序产品在路由管理设备或 AS 管理设备上运行时，使得路由管理设备或 AS 管理设备执行上述方法实施例中的方法 300、方法 400 或方法 500。

上述各种产品形态的装置，分别具有上述方法实施例中路由管理设备或 AS 管理设备的任意功能，此处不再赘述。

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中描述的各方法步骤和单元，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各实施例的步骤及组成。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。本领域普通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申请的范围。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参见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，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，该单元的划分，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。另外，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，也可以是电的，机械的或其它的形式连接。

该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申请实施例方案的目的。

另外，在本申请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，也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

该集成的单元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存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分，或者该技术方案的全部或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）执行本申请各个实施例中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（read-only memory, ROM）、随机存取存储器（random access memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上描述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机程序指令。在计算机上加载和执行该计算机程序指令时，全部或部分地产生按照本申请实施例中的流程或功能。该计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。该计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，该计算机程序指令可以从一个网站站点、计算机、服务器或数据中心通过有线或无线方式向另一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质（例如软盘、硬盘、磁带）、光介质（例如，数字视频光盘（digital video disc, DVD）、或者半导体介质（例如固态硬盘）等。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，该程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上描述仅为本申请的可选实施例，并不用以限制本申请，凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权 利 要 求 书

1. 一种路由管理方法，其特征在于，包括：

获得对应关系，所述对应关系包括第一自治系统 AS 标识和第二 AS 标识，所述对应关系用于指示所述第一 AS 标识和所述第二 AS 标识为兄弟 AS；

根据所述对应关系进行路由管理。

2. 根据权利要求 1 所述的方法，其特征在于，所述根据所述对应关系进行路由管理，包括：

根据所述对应关系确定路由消息有效。

3. 根据权利要求 2 所述的方法，其特征在于，在根据所述对应关系确定路由消息有效之前，所述方法还包括：

根据路由起源授权 ROA 信息确定所述路由消息无效，所述路由消息无效包括：所述路由消息的路由被劫持；或

根据商业关系信息确定所述路由消息无效，所述路由消息无效包括：所述路由消息发生路由泄漏。

4. 根据权利要求 3 所述的方法，其特征在于，所述路由消息包括第一路由前缀和第三 AS 标识，所述路由消息指示所述第三 AS 为所述第一路由前缀的源 AS，

所述根据 ROA 信息确定所述路由消息无效，包括：

根据所述 ROA 信息确定所述第一路由前缀被所述第三 AS 劫持，所述 ROA 信息指示第二路由前缀的源 AS 为所述第二 AS，所述第一路由前缀与所述第二路由前缀对应；

所述根据对应关系确定路由消息有效，包括：

根据所述第三 AS 标识与所述第一 AS 标识相同，确定所述路由消息未被所述第三 AS 标识劫持。

5. 根据权利要求 3 所述的方法，其特征在于，所述路由消息包括第一路由前缀、第三 AS 标识和第四 AS 标识，所述第三 AS 标识与所述第四 AS 标识在所述路由消息的 AS 路径中相邻，

所述根据商业关系信息确定所述路由消息无效，包括：

校验所述第一路由前缀由所述第三 AS 泄漏给所述第四 AS；

所述根据对应关系确定路由消息有效，包括：

根据所述第四 AS 标识与所述第一 AS 标识相同以及满足第一条件确定所述路由消息未被所述第三 AS 泄漏，所述第一条件包括：所述第三 AS 标识与所述第二 AS 标识相同，或所述路由消息包括的源 AS 标识与所述第二 AS 标识相同。

6. 根据权利要求 2-5 任一项所述的方法，其特征在于，在确定所述路由消息有效之后，还包括：

将所述路由消息对应的校验状态更新为有效。

7. 根据权利要求 1-6 任一项所述的方法，其特征在于，所述获得对应关系，包括：

接收第一消息，所述第一消息包括所述对应关系。

8. 根据权利要求 7 所述的方法，其特征在于，所述第一消息由资源公钥基础设施 RPKI

服务器发送, 所述第一消息包括兄弟 AS 协议数据单元 PDU, 所述 PDU 包括所述第一 AS 标识和所述第二 AS 标识。

9. 根据权利要求 7 或 8 所述的方法, 其特征在于, 所述第一消息还包括组织标识 和/或兄弟 AS 数。

10. 根据权利要求 2-9 任一项所述的方法, 其特征在于, 所述路由消息为边界网关协议 BGP 消息。

11. 根据权利要求 1-10 任一项所述的方法, 其特征在于, 所述根据所述对应关系进行路由管理, 包括:

向接收设备发送消息, 所述消息包括所述对应关系, 所述消息用于使所述接收设备根据所述对应关系进行路由分析。

12. 根据权利要求 1-6 任一项所述的方法, 其特征在于, 所述获得对应关系, 包括:

获得所述第一 AS 标识和所述第二 AS 标识;

确定所述第一 AS 标识和所述第二 AS 标识为兄弟 AS;

生成所述对应关系。

13. 根据权利要求 1-12 任一项所述的方法, 其特征在于, 应用于资源公钥基础设施 RPKI 系统中。

14. 一种自治系统 AS 管理方法, 其特征在于, 包括:

获得第一自治系统 AS 标识和第二 AS 标识;

发送消息, 所述消息包括所述第一 AS 标识和所述第二 AS 标识, 所述消息用于指示所述第一 AS 标识和所述第二 AS 标识为兄弟 AS。

15. 根据权利要求 14 所述的方法, 其特征在于, 所述消息还包括组织标识和/或 AS 数量。

16. 根据权利要求 14-15 任一项所述的方法, 其特征在于, 所述第一 AS 标识和所述第二 AS 标识携带在所述消息的兄弟 AS 协议数据单元 PDU 中。

17. 一种路由管理装置, 其特征在于, 包括:

处理单元, 用于获得对应关系, 所述对应关系包括第一自治系统 AS 标识和第二 AS 标识, 所述对应关系用于指示所述第一 AS 标识和所述第二 AS 标识为兄弟 AS;

所述处理单元, 还用于根据所述对应关系进行路由管理。

18. 根据权利要求 17 所述的装置, 其特征在于, 所述处理单元, 用于根据所述对应关系确定路由消息有效。

19. 根据权利要求 18 所述的装置, 其特征在于, 在所述处理单元用于确定所述路由消息有效之前, 所述处理单元还用于:

根据路由起源授权 ROA 信息确定所述路由消息无效, 所述路由消息无效包括: 所述路由消息的路由被劫持; 或

根据商业关系信息确定所述路由消息无效, 所述路由消息无效包括: 所述路由消息发生路由泄漏。

20. 根据权利要求 19 所述的装置, 其特征在于, 所述路由消息包括第一路由前缀和第三 AS 标识, 所述路由消息指示所述第三 AS 为所述第一路由前缀的源 AS,

所述处理单元用于：

根据所述 ROA 信息确定所述第一路由前缀被所述第三 AS 劫持，所述 ROA 信息指示第二路由前缀的源 AS 为所述第二 AS，所述第一路由前缀与所述第二路由前缀对应；

所述处理单元还用于：

根据所述第三 AS 标识与所述第一 AS 标识相同，确定所述路由消息未被所述第三 AS 标识劫持。

21. 根据权利要求 19 所述的装置，其特征在于，所述路由消息包括第一路由前缀、第三 AS 标识和第四 AS 标识，所述第三 AS 标识与所述第四 AS 标识在所述路由消息的 AS 路径中相邻，

所述处理单元用于：

确定所述第一路由前缀由所述第三 AS 泄漏给所述第四 AS；

所述处理单元还用于：

根据所述第四 AS 标识与所述第一 AS 标识相同以及满足第一条件确定所述路由消息未被所述第三 AS 泄漏，所述第一条件包括：所述第三 AS 标识与所述第二 AS 标识相同，或所述路由消息包括的源 AS 标识与所述第二 AS 标识相同。

22. 根据权利要求 18-21 任一项所述的装置，其特征在于，所述处理单元，还用于：将所述路由消息对应的确定状态更新为有效。

23. 根据权利要求 17-22 任一项所述的方法，其特征在于，还包括：发送单元，用于：向接收设备发送消息，所述消息包括所述对应关系，所述消息用于使所述接收设备根据所述对应关系进行路由分析。

24. 根据权利要求 17-23 任一项所述的装置，其特征在于，还包括接收单元，用于接收第一消息，所述第一消息包括所述对应关系。

25. 根据权利要求 17-23 任一项所述的方法，其特征在于，所述处理单元，还用于：获得所述第一 AS 标识和所述第二 AS 标识；确定所述第一 AS 标识和所述第二 AS 标识为兄弟 AS；生成所述对应关系。

26. 一种自治系统 AS 管理装置，其特征在于，包括：

处理单元，用于获得第一自治系统 AS 标识和第二 AS 标识；

发送单元，用于发送消息，所述消息包括所述第一 AS 标识和所述第二 AS 标识，所述消息用于指示所述第一 AS 标识和所述第二 AS 标识为兄弟 AS。

27. 根据权利要求 26 所述的装置，其特征在于，所述消息还包括组织标识和/或 AS 数量。

28. 根据权利要求 26 或 27 所述的装置，其特征在于，所述第一 AS 标识和所述第二 AS 标识携带在所述消息的兄弟 AS 协议数据单元 PDU 中。

29. 一种路由管理系统，其特征在于，包括如权利要求 17-28 中任一所述的装置。

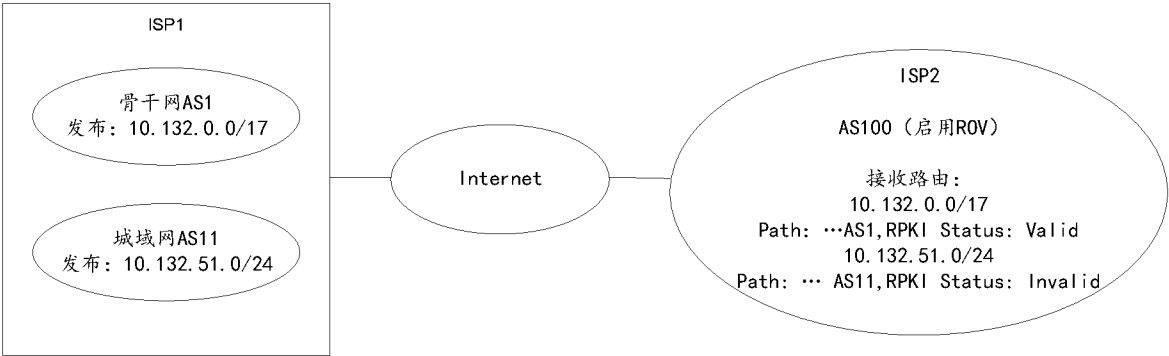


图 1

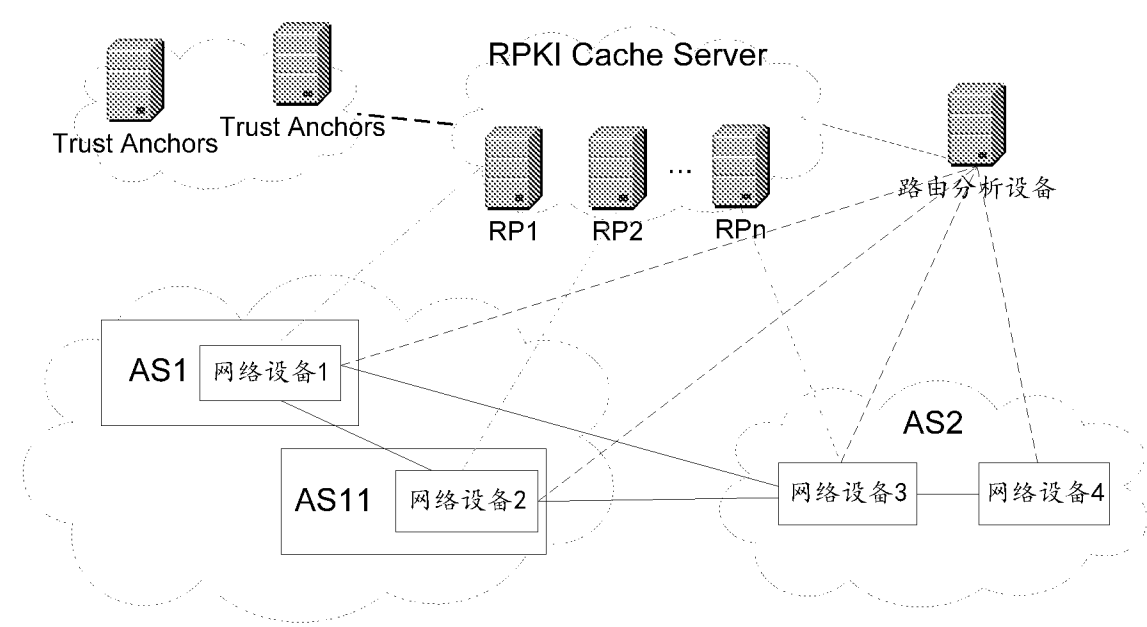


图 2

300

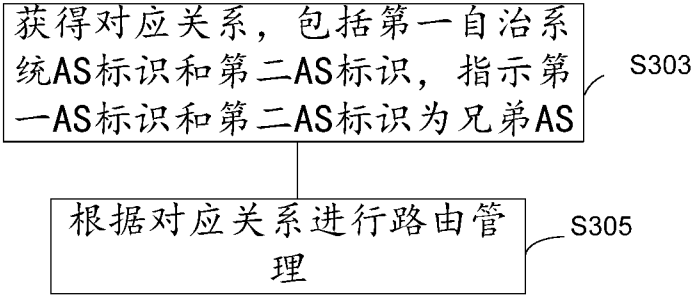


图 3a

400

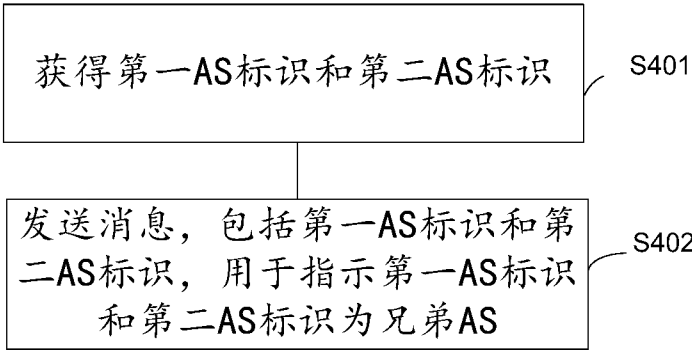


图 3b

0	8	16	24	31
Protocol Version 协议版本	PDU Type PUD 类型	Zero1 零区域1		
Length 长度				
Flags 标志	Zero2 零区域2	Sibling AS Count 兄弟AS数量		
Organization Identifier 组织标识				
Sibing AS Number(s) 兄弟AS号				

图 4

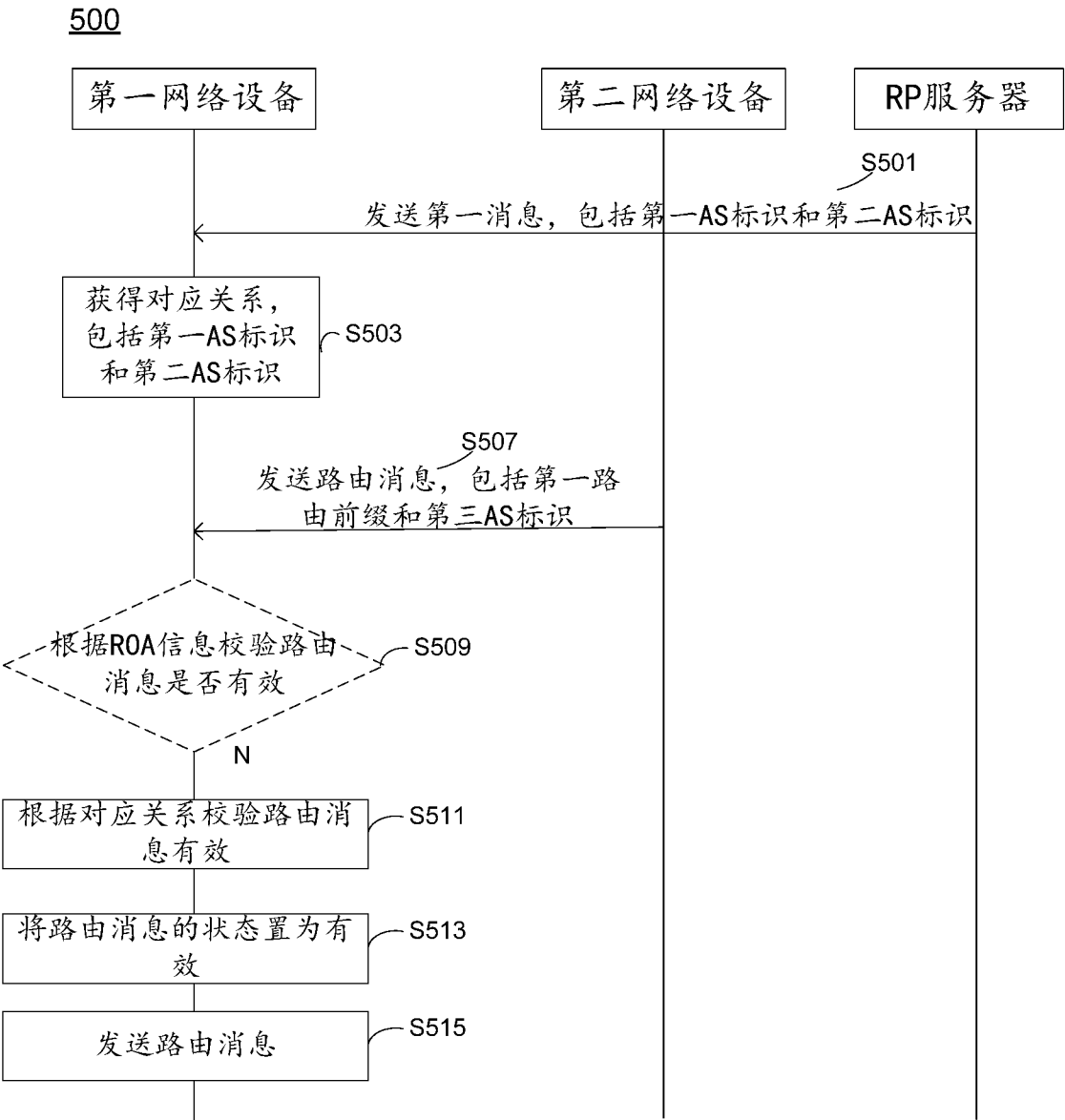


图 5

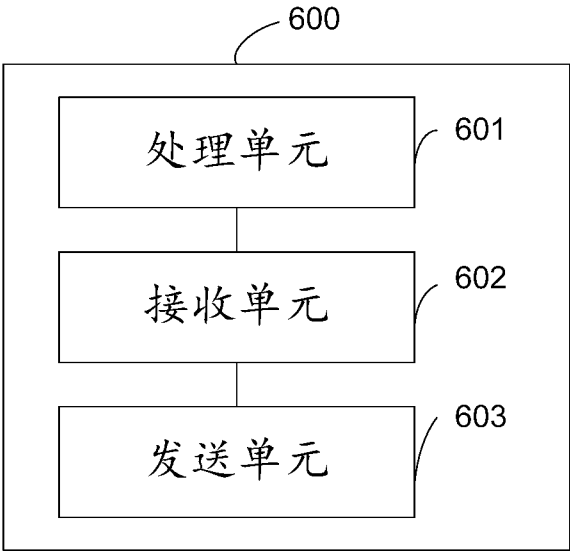


图 6

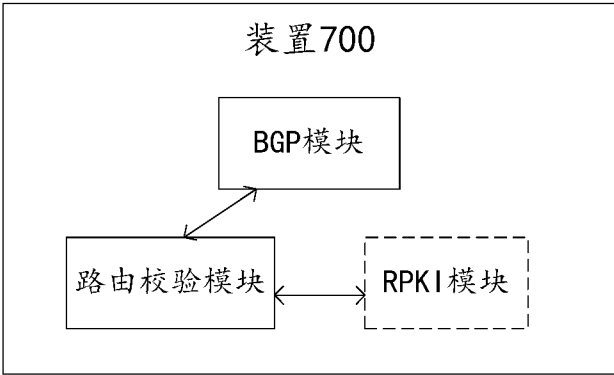


图 7

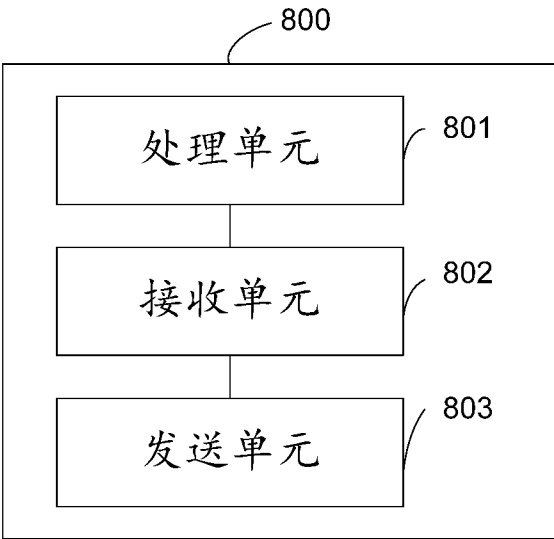


图 8

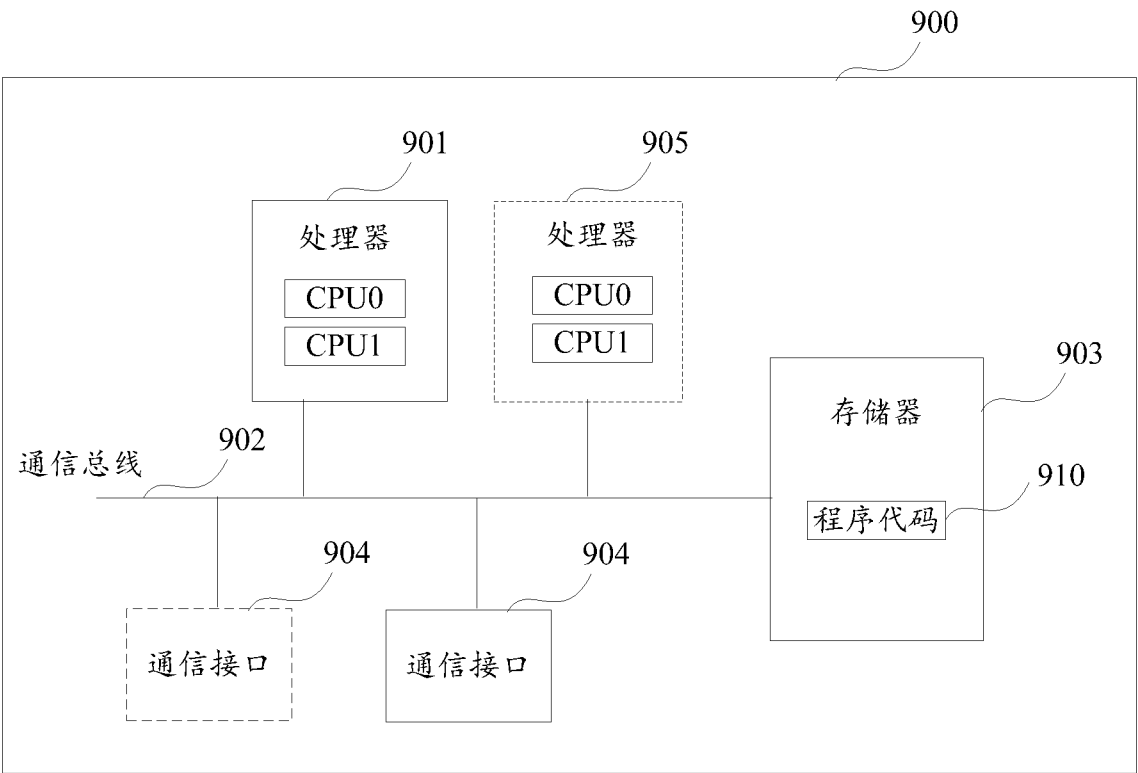


图 9

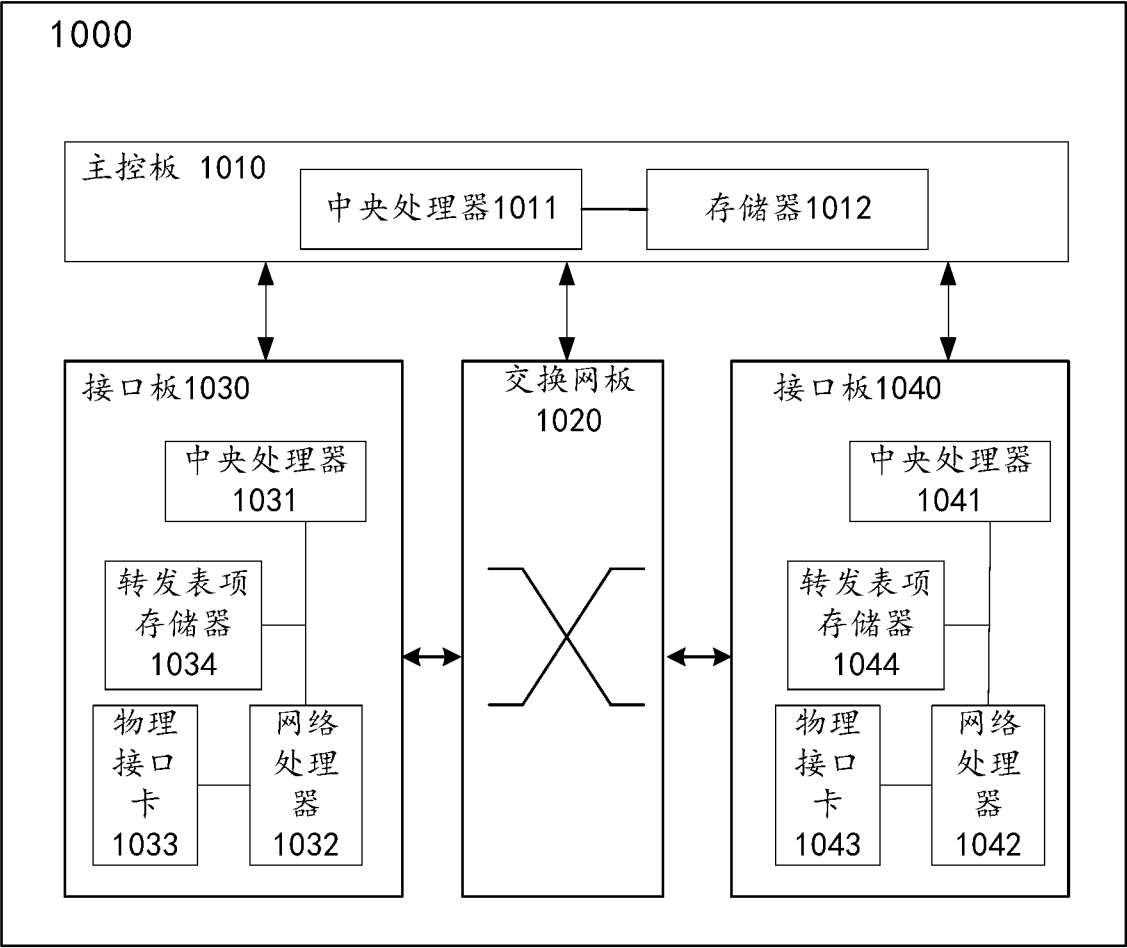


图 10

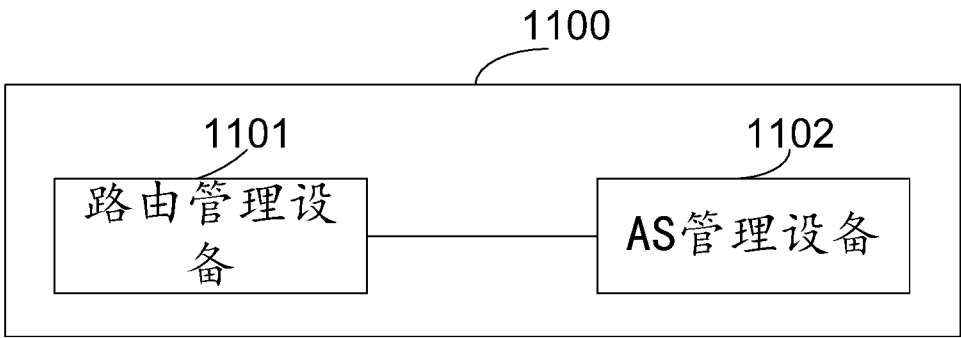


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/106689

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(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)

G06F; 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: 对应, 映射, 自治, 标识, 识别, 兄弟, 同胞, 路由, correspond+, map+, autonomous, identi+, sibling, rout+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101681341 A (MICROSOFT CORPORATION) 24 March 2010 (2010-03-24) description page 3 line 10 to page 9 line 8	1-3, 6-19, 22-29
X	梁海英 等 (LIANG, Haiying et al.). "地址检查BGP/MPLS VPN 中MP-BGP配置错误的方法 (Method of Inspecting MP-BGP Misconfiguration in BGP/MPLS VPN)" <i>计算机工程 (Computer Engineering)</i> , 31 March 2006 (2006-03-31), section 3.2	1-3, 6-19, 22-29
X	王洪君 等 (WANG, Hongjun et al.). "一种BGP无效路由检测方法 (An Approach to Detect BGP Invalid Routes)" <i>吉林师范大学学报(自然科学版) (Jilin Normal University Journal(Natural Science Edition))</i> , 31 August 2008 (2008-08-31), sections 2-4	1-3, 6-19, 22-29
X	邹秀斌 等 (ZOU, Xiubin et al.). "在因特网上推导自治系统 (AS) 相互关系的启发式算法 (The Heuristic Algorithms for Inferring Autonomous System Relationships on the Internet)" <i>计算机工程与应用 (Computer Engineering and Applications)</i> , 31 December 2003 (2003-12-31), sections 2-3	1-3, 6-19, 22-29
A	CN 103210669 A (CISCO TECHNOLOGY, INC.) 17 July 2013 (2013-07-17) entire document	1-29



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

13 September 2021

Date of mailing of the international search report

18 October 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/106689**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017041332 A1 (CISCO TECHNOLOGY, INC.) 09 February 2017 (2017-02-09) entire document	1-29
A	US 2009141637 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 04 June 2009 (2009-06-04) entire document	1-29

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/106689

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	101681341	A	24 March 2010	US	2008301214	A1	04 December 2008
				EP	2568686	A1	13 March 2013
				WO	2008150624	A1	11 December 2008
				EP	2171605	A1	07 April 2010
CN	103210669	A	17 July 2013	US	2012117268	A1	10 May 2012
				WO	2012064794	A1	18 May 2012
				EP	2638738	A1	18 September 2013
US	2017041332	A1	09 February 2017	None			
US	2009141637	A1	04 June 2009	None			

国际检索报告

国际申请号

PCT/CN2021/106689

A. 主题的分类 G06F 15/16 (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) G06F; 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, EPDOC, CNKI: 对应, 映射, 自治, 标识, 识别, 兄弟, 同胞, 路由, correspond+, map+, autonomous, identi+, sibling, rout+																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101681341 A (微软公司) 2010年 3月 24日 (2010 - 03 - 24) 说明书第3页第10行至第9页第8行</td> <td>1-3, 6-19, 22-29</td> </tr> <tr> <td>X</td> <td>梁海英等. "地址检查BGP/MPLS VPN 中MP-BGP配置错误的方法" 计算机工程, 2006年 3月 31日 (2006 - 03 - 31), 第3.2节</td> <td>1-3, 6-19, 22-29</td> </tr> <tr> <td>X</td> <td>王洪君等. "一种BGP无效路由检测方法" 吉林师范大学学报 (自然科学版), 2008年 8月 31日 (2008 - 08 - 31), 第2-4节</td> <td>1-3, 6-19, 22-29</td> </tr> <tr> <td>X</td> <td>邹秀斌等. "在因特网上推导自治系统 (AS) 相互关系的启发式算法" 计算机工程与应用, 2003年 12月 31日 (2003 - 12 - 31), 第2-3节</td> <td>1-3, 6-19, 22-29</td> </tr> <tr> <td>A</td> <td>CN 103210669 A (思科技术公司) 2013年 7月 17日 (2013 - 07 - 17) 全文</td> <td>1-29</td> </tr> <tr> <td>A</td> <td>US 2017041332 A1 (CISCO TECHNOLOGY, INC.) 2017年 2月 9日 (2017 - 02 - 09) 全文</td> <td>1-29</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 101681341 A (微软公司) 2010年 3月 24日 (2010 - 03 - 24) 说明书第3页第10行至第9页第8行	1-3, 6-19, 22-29	X	梁海英等. "地址检查BGP/MPLS VPN 中MP-BGP配置错误的方法" 计算机工程, 2006年 3月 31日 (2006 - 03 - 31), 第3.2节	1-3, 6-19, 22-29	X	王洪君等. "一种BGP无效路由检测方法" 吉林师范大学学报 (自然科学版), 2008年 8月 31日 (2008 - 08 - 31), 第2-4节	1-3, 6-19, 22-29	X	邹秀斌等. "在因特网上推导自治系统 (AS) 相互关系的启发式算法" 计算机工程与应用, 2003年 12月 31日 (2003 - 12 - 31), 第2-3节	1-3, 6-19, 22-29	A	CN 103210669 A (思科技术公司) 2013年 7月 17日 (2013 - 07 - 17) 全文	1-29	A	US 2017041332 A1 (CISCO TECHNOLOGY, INC.) 2017年 2月 9日 (2017 - 02 - 09) 全文	1-29
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
X	CN 101681341 A (微软公司) 2010年 3月 24日 (2010 - 03 - 24) 说明书第3页第10行至第9页第8行	1-3, 6-19, 22-29																					
X	梁海英等. "地址检查BGP/MPLS VPN 中MP-BGP配置错误的方法" 计算机工程, 2006年 3月 31日 (2006 - 03 - 31), 第3.2节	1-3, 6-19, 22-29																					
X	王洪君等. "一种BGP无效路由检测方法" 吉林师范大学学报 (自然科学版), 2008年 8月 31日 (2008 - 08 - 31), 第2-4节	1-3, 6-19, 22-29																					
X	邹秀斌等. "在因特网上推导自治系统 (AS) 相互关系的启发式算法" 计算机工程与应用, 2003年 12月 31日 (2003 - 12 - 31), 第2-3节	1-3, 6-19, 22-29																					
A	CN 103210669 A (思科技术公司) 2013年 7月 17日 (2013 - 07 - 17) 全文	1-29																					
A	US 2017041332 A1 (CISCO TECHNOLOGY, INC.) 2017年 2月 9日 (2017 - 02 - 09) 全文	1-29																					
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
<table border="0"> <tr> <td> * 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 </td> <td> "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 </td> </tr> </table>			* 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																			
* 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																					
2021年 9月 13日		2021年 10月 18日																					
ISA/CN的名称和邮寄地址		受权官员																					
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		李玉萍 电话号码 86-(10)-53961674																					

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	US 2009141637 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2009年 6月 4日 (2009 - 06 - 04) 全文	1-29

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/106689

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	101681341	A	2010年 3月 24日	US	2008301214	A1	2008年 12月 4日
				EP	2568686	A1	2013年 3月 13日
				WO	2008150624	A1	2008年 12月 11日
				EP	2171605	A1	2010年 4月 7日
CN	103210669	A	2013年 7月 17日	US	2012117268	A1	2012年 5月 10日
				WO	2012064794	A1	2012年 5月 18日
				EP	2638738	A1	2013年 9月 18日
US	2017041332	A1	2017年 2月 9日	无			
US	2009141637	A1	2009年 6月 4日	无			