(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 1 月 26 日 (26.01.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/012089 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2015/084772

(22) 国际申请日: 2015 年 7 月 22 日 (22.07.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(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: **杜宗鹏 (DU, Zongpeng)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **蒋胜 (JIANG, Sheng)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **刘冰 (LIU, Bing)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.)**; 中国北京市海淀区丹棱街 16 号海兴大厦 C 座 1108, Beijing 100080 (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, 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, KN, KP, KR, 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 DATA LINK LAYER

(54) **发明名称** : 一种基于数据链路层的通信方法、设备和系统

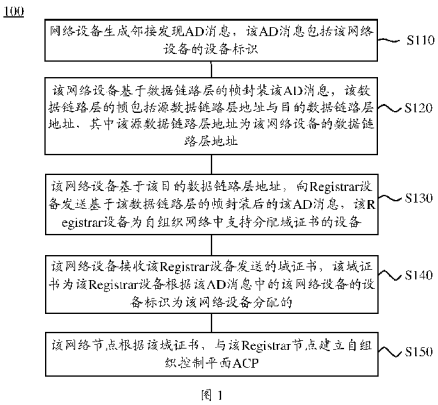

图 1

S110 A NETWORK DEVICE GENERATES AN ADJACENCY DISCOVERY (AD) MESSAGE, THE AD MESSAGE COMPRISING A DEVICE IDENTIFIER OF THE NETWORK DEVICE

S120 THE NETWORK DEVICE ENCAPSULATES THE AD MESSAGE ACCORDING TO A FRAME OF THE DATA LINK LAYER, THE FRAME OF THE DATA LINK LAYER COMPRISING A SOURCE DATA LINK LAYER ADDRESS AND A DESTINATION DATA LINK LAYER ADDRESS, AND THE SOURCE DATA LINK LAYER ADDRESS BEING A DATA LINK LAYER ADDRESS OF THE NETWORK DEVICE

S130 THE NETWORK DEVICE SENDS, TO A REGISTRAR DEVICE ACCORDING TO THE DESTINATION DATA LINK LAYER ADDRESS, THE AD MESSAGE ENCAPSULATED ACCORDING TO THE FRAME OF THE DATA LINK LAYER, AND THE REGISTRAR DEVICE BEING A DEVICE SUPPORTING ALLOCATION OF THE DOMAIN CERTIFICATE IN A SELF-ORGANIZING NETWORK

S140 THE NETWORK DEVICE RECEIVES A DOMAIN CERTIFICATE SENT BY THE REGISTRAR DEVICE, THE DOMAIN CERTIFICATE BEING ALLOCATED BY THE REGISTRAR DEVICE TO THE NETWORK DEVICE ACCORDING TO THE DEVICE IDENTIFIER OF THE NETWORK DEVICE IN THE AD MESSAGE

S150 THE NETWORK DEVICE ESTABLISHES AN AUTONOMIC CONTROL PLANE (ACP) WITH THE REGISTRAR NODE ACCORDING TO THE DOMAIN CERTIFICATE

(57) **Abstract**: Embodiments of the present invention provide a communication method, device and system based on a data link layer. The method comprises: a network device generates an adjacency discovery (AD) message, the AD message comprising a device identifier of the network device; the network device encapsulates the AD message according to a frame of the data link layer, the frame of the data link layer comprising a source data link layer address and a destination data link layer address; the network device sends, to a Registrar device according to the destination data link layer address, the AD message encapsulated according to the frame of the data link layer; the network device receives a domain certificate sent by the Registrar device, the domain certificate being allocated by the Registrar device to the network device according to the device identifier of the network device in the AD message; and the network device establishes an autonomic control plane (ACP) with the Registrar device according to the domain certificate. In the embodiments of the present invention, communication based on a self-organizing network may not sense an IP protocol, and compared the prior art, the present invention has good network compatibility, thereby effectively reducing obstacles of deployment of the self-organizing network.

(57) **摘要**:

[见续页]

WO 2017/012089 A1

本发明实施例提供一种基于数据链路层的通信方法、设备和系统，该方法包括：网络设备生成邻接发现 AD 消息，AD 消息包括该网络设备的设备标识；网络设备基于数据链路层的帧封装该 AD 消息，数据链路层的帧包括源数据链路层地址与目的数据链路层地址；该网络设备基于目的数据链路层地址，向 Registrar 设备发送基于该数据链路层的帧封装后的该 AD 消息；该网络设备接收该 Registrar 设备发送的域证书，该域证书为该 Registrar 设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的；网络设备根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。在本发明实施例中，基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，有效减小自组织网络的部署障碍。

一种基于数据链路层的通信方法、设备和系统

技术领域

本发明实施例涉及通信领域，并且更具体地，涉及一种基于数据链路层的通信方法、设备和系统。

背景技术

自组织网络（Autonomic Network，简称为“AN”）是一种能够支持自管理的网络，例如包括网络自配置、自保护、自愈和自优化，能够提升网络的自动化程度。自组织网络中的一个关键技术是自动控制平面（Autonomic Control Plane，简称为“ACP”）的建立，自组织控制平面 ACP 指的是自组织网络中的控制平面，上层的自组织功能实体可以使用该 ACP 平面传输控制信令。

当前技术中提出一种基于 IPv6（Internet Protocol Version 6）建立 ACP 的实现方式，但是当前技术中，需要网络设备支持 IPv6，才能实现 ACP 的建立，导致自组织网络兼容性不好。

发明内容

本发明实施例提供一种基于数据链路层的通信方法、设备和系统，基于数据链路层建立自组织网络，能够克服现有技术中实现自组织网络必须依赖于 IPv6 的问题，具有较好的网络兼容性。

第一方面，提供了一种基于数据链路层的通信方法，该方法包括:

网络设备生成邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识;

该网络设备基于数据链路层的帧封装该 AD 消息，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址;

该网络设备基于该目的数据链路层地址，向登记 Registrar 设备发送基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备;

该网络设备接收该 Registrar 设备发送的域证书，该域证书为该 Registrar

设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的;

该网络设备根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。

结合第一方面，在第一方面的第一种可能的实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

结合第一方面或一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

结合第一方面及其上述实现方式，在第一方面的第三种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第一方面及其上述实现方式，在第一方面的第四种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

结合第一方面及其上述实现方式，在第一方面的第五种实现方式中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

第二方面，提供了一种基于数据链路层的通信方法，该方法包括:

登记 Registrar 设备接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配;

当该 Registrar 设备确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书;

该 Registrar 设备根据该域证书，与该网络设备建立自组织控制平面 ACP。

结合第二方面，在第二方面的第一种实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

结合第二方面或第二方面的第一种实现方式，在第二方面的第二种实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

结合第二方面及其上述实现方式，在第二方面的第三种实现方式中，该网络设备为该 Registrar 设备的邻居设备，该方法还包括:

该 Registrar 设备根据该 AD 消息，建立该 Registrar 设备的邻居列表，该邻居列表包括该网络设备的设备标识以及该网络设备的数据链路层地址。

结合第二方面及其上述实现方式，在第二方面的第四种实现方式中，该网络设备的设备标识为该网络设备的唯一设备标识 UDI，

其中，当该 Registrar 设备确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书，包括:

当该 Registrar 设备确定白名单具有该网络设备的 UDI 的匹配项时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该 UDI 分配的该域证书，该白名单包括允许加入该自组织网络的设备的 UDI。

结合第二方面及其上述实现方式，在第二方面的第五种实现方式中，该网络设备的设备标识为该网络设备的安全的唯一设备标识 S-UDI，

其中，当该 Registrar 设备确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书，包括:

当该 Registrar 设备通过验证服务器确定该 S-UDI 对应的设备数字证书有效时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该设备数字证书分配的该域证书。

结合第二方面及其上述实现方式，在第二方面的第六种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第二方面及其上述实现方式，在第二方面的第七种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

第三方面，提供了一种基于数据链路层的通信方法，该通信方法应用于自组织网络，该方法包括:

第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，该第一网络设备为该自组织网络中的自组织设备;

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址;

该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，该第二网络设备也为该自组织网络中的自组织设备，且该第二网络设备为该第一网络设备的邻居设备。

结合第三方面，在第三方面的第一种实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

结合第三方面或在第三方面的第一种实现方式，在第三方面的第二种实现方式中，

该第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

该第一网络设备需要与该自组织网络中的目标设备通信时，当确定该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，该第一网络设备的邻居列表包括该第一网络设备的邻居设备的设备标识与数据链路层地址;

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，包括:

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，包括:

该第一网络设备根据该目标设备的数据链路层地址，向该目标设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第三方面或在第三方面的第一种实现方式，在第三方面的第三种实现方式中，该第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

该第一网络设备需要与该自组织网络中的目标设备通信时，当确定该邻居列表中不包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文;

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，包括:

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，包括:

该第一网络设备根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第三方面或在第三方面的第一种实现方式，在第三方面的第四种实现方式中，该第一网络设备生成 L2 ACP 报文，包括:

当该第一网络设备需要在该 ACP 内广播控制消息时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文;

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，包括:

该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，包括:

该第一网络设备根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第三方面的第三种或第四种实现方式，在第三方面的第五种实现方式中，该 L2 ACP 报文的报文头还包括用于唯一指示该 L2 ACP 报文的报文 ID。

结合第三方面第三种至第五种实现方式中的任一种实现方式，在第三方面的第六种实现方式中，该 L2 ACP 报文的报文头还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

结合第三方面及其上述实现方式，在第三方面的第七种实现方式中，该自组织网络中的每个设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，

其中，该第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

当该第一网络设备需要通过 IP 会话与该自组织网络内的目标设备通信时，生成该 L2 ACP 报文，该 L2 ACP 报文还包括目的 IP 地址，该目的 IP 地址为该目标设备的 IP 地址。

结合第三方面及其上述实现方式，在第三方面的第八种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第三方面及其上述实现方式，在第三方面的第九种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

结合第三方面及其上述实现方式，在第三方面的第十种实现方式中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

第四方面，提供了一种基于数据链路层的通信方法，该通信方法应用于自组织网络，该方法包括:

第二网络设备接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，该 L2 ACP 报文包括目的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配，该第二网络设备与该第一网络设备均为该自组织网络中的自组织设备;

该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文。

结合第四方面，在第四方面的第一种实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

结合第四方面及其上述实现方式，在第四方面的第二种实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

其中，该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

该第二网络设备确定该目的设备标识为该第二网络设备的设备标识，并解析该 L2 ACP 报文。

结合第四方面或第四方面的第一种实现方式，在第四方面的第三种实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

当该第二网络设备确定该第二网络设备的设备标识与该目的设备标识相匹配时，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文;

当该第二网络设备确定该第二网络设备的设备标识与该目的设备标识不匹配时，缓存该 L2 ACP 报文，并根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第四方面或第四方面的第一种实现方式，在第四方面的第四种实现方式中，该 L2 ACP 报文的报文头还包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

该第二网络设备确定该第二网络设备的设备标识与该目的设备标识相匹配，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文，以及根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第四方面的第三种或第四种实现方式，在第四方面的第五种实现方式中，该 L2 ACP 报文的报文头中还包括用于唯一标识该 L2 ACP 报文的报文 ID，

其中，该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

当该第二网络设备确定本地未缓存该报文 ID 时，通过判断该第二网络设备的设备标识是否与该目的设备标识相匹配，处理该 L2 ACP 报文。

结合第四方面的第三种至第五种实现方式中的任一种实现方式，在第四方面的第六种实现方式中，该 L2 ACP 报文的报文头中还包括定时信息，该

定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文，

该方法还包括:

当该第二网络设备确定缓存该 L2 ACP 报文的时间超过该定时信息所指示的预设时长时，清除该 L2 ACP 报文。

结合第四方面及其上述实现方式，在第四方面的第七种实现方式中，该自组织网络内的每个自组织设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，其中，该 L2 ACP 报文还包括目的 IP 地址，

该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

当该第二网络设备确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识不匹配时，根据该 L2 ACP 报文的目的数据链路层地址向该第二网络设备的邻居设备转发该 L2 ACP 报文;

当该第二网络设备确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识相匹配、且该第二网络设备的 IP 地址与该 L2 ACP 报文的该目的 IP 地址相匹配时，解析该 L2 ACP 报文。

结合第四方面及其上述实现方式，在第四方面的第八种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第四方面及其上述实现方式，在第四方面的第九种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

结合第四方面及其上述实现方式，在第四方面的第十种实现方式中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

第五方面，提供了一种网络设备，该网络设备应用于自组织网络，该网络设备包括:

生成模块，用于网络设备生成邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识;

封装模块，用于基于数据链路层的帧封装该生成模块生成的该 AD 消息，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址;

发送模块，用于基于该目的数据链路层地址，向登记 Registrar 设备发送

该封装模块确定的基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备;

接收模块，用于接收该 Registrar 设备发送的域证书，该域证书为该 Registrar 设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的;

建立模块，用于根据该接收模块接收的该域证书，与该 Registrar 设备建立自组织控制平面 ACP。

结合第五方面，在第五方面的第一种可能的实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

结合第五方面或一方面的第一种可能的实现方式，在第五方面的第二种可能的实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

结合第五方面及其上述实现方式，在第五方面的第三种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第五方面及其上述实现方式，在第五方面的第四种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

结合第五方面及其上述实现方式，在第五方面的第五种实现方式中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

第六方面，提供了一种登记 Registrar 设备，该 Registrar 设备应用于自组织网络，该 Registrar 设备为该自组织网络中支持分配域证书的设备，Registrar 设备包括:

接收模块，用于接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配;

发送模块，用于当确定该网络设备允许加入该自组织网络时，根据该接收模块接收的该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书;

ACP 建立模块，用于根据该发送模块发送的该域证书，与该网络设备建立自组织控制平面 ACP。

结合第六方面，在第六方面的第一种实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

结合第六方面或第六方面的第一种实现方式，在第六方面的第二种实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

结合第六方面及其上述实现方式，在第六方面的第三种实现方式中，该网络设备为该 Registrar 设备的邻居设备，该 Registrar 设备还包括:

邻居列表建立模块，用于根据该 AD 消息，建立该 Registrar 设备的邻居列表，该邻居列表包括该网络设备的设备标识以及该网络设备的数据链路层地址。

结合第六方面及其上述实现方式，在第六方面的第四种实现方式中，该网络设备的设备标识为该网络设备的唯一设备标识 UDI，

其中，该发送模块具体用于，当确定白名单具有该网络设备的 UDI 的匹配项时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该 UDI 分配的该域证书，该白名单包括允许加入该自组织网络的设备的 UDI。

结合第六方面及其上述实现方式，在第六方面的第五种实现方式中，该网络设备的设备标识为该网络设备的安全的唯一设备标识 S-UDI，

其中，该发送模块具体用于，当通过验证服务器确定该 S-UDI 对应的设备数字证书有效时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该设备数字证书分配的该域证书。

结合第六方面及其上述实现方式，在第六方面的第六种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第六方面及其上述实现方式，在第六方面的第七种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

第七方面，提供了一种网络设备，该网络设备用作第一网络设备，该第一网络设备应用于自组织网络，该第一网络设备包括:

生成模块，用于生成数据链路层自组织控制平面 L2 ACP 报文，该第一

网络设备为该自组织网络中的自组织设备;

封装模块，用于基于数据链路层的帧封装该生成模块生成的该 L2 ACP 报文，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址;

发送模块，用于根据该目的数据链路层地址，向第二网络设备发送该封装模块确定的基于该数据链路层的帧封装后的该 L2 ACP 报文，该第二网络设备也为该自组织网络中的自组织设备，且该第二网络设备为该第一网络设备的邻居设备。

结合第七方面，在第七方面的第一种实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

结合第七方面或在第七方面的第一种实现方式，在第七方面的第二种实现方式中，该生成模块具体用于，需要与该自组织网络中的目标设备通信时，当确定该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，该第一网络设备的邻居列表包括该第一网络设备的邻居设备的设备标识与数据链路层地址;

该封装模块具体用于，基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

该发送模块具体用于，根据该目标设备的数据链路层地址，向该目标设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第七方面或在第七方面的第一种实现方式，在第七方面的第三种实现方式中，该生成模块具体用于，需要与该自组织网络中的目标设备通信时，当确定该邻居列表中不包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文;

该封装模块具体用于，基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

该发送模块具体用于，根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第七方面或在第七方面的第一种实现方式，在第七方面的第四种实

现方式中，该生成模块具体用于，需要在该 ACP 内广播控制消息时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文；

该封装模块具体用于，基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

其中，该发送模块具体用于，根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第七方面的第三种或第四种实现方式，在第七方面的第五种实现方式中，该 L2 ACP 报文的报文头还包括用于唯一指示该 L2 ACP 报文的报文 ID。

结合第七方面第三种至第五种实现方式中的任一种实现方式，在第七方面的第六种实现方式中，该 L2 ACP 报文的报文头还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

结合第七方面及其上述实现方式，在第七方面的第七种实现方式中，该自组织网络中的每个设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，

其中，该生成模块具体用于，当需要通过 IP 会话与该自组织网络内的目标设备通信时，生成该 L2 ACP 报文，该 L2 ACP 报文还包括目的 IP 地址，该目的 IP 地址为该目标设备的 IP 地址。

结合第七方面及其上述实现方式，在第七方面的第八种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第七方面及其上述实现方式，在第七方面的第九种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

结合第七方面及其上述实现方式，在第七方面的第十种实现方式中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

第八方面，提供了一种网络设备，该网络设备用作第二网络设备，该第二网络设备应用于自组织网络，该第二网络设备包括：

接收模块，用于接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，该 L2 ACP 报文包括目的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第

一网络设备的数据链路层地址，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配，该第二网络设备与该第一网络设备均为该自组织网络中的自组织设备;

处理模块，用于通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该接收模块接收的该 L2 ACP 报文。

结合第八方面，在第八方面的第一种实现方式中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

结合第八方面及其上述实现方式，在第八方面的第二种实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

其中，该处理模块具体用于，确定该目的设备标识为该第二网络设备的设备标识，并解析该 L2 ACP 报文。

结合第八方面或第八方面的第一种实现方式，在第八方面的第三种实现方式中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该处理模块具体用于，当确定该第二网络设备的设备标识与该目的设备标识相匹配时，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文;

处理模块具体用于，当确定该第二网络设备的设备标识与该目的设备标识不匹配时，缓存该 L2 ACP 报文，并根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第八方面或第八方面的第一种实现方式，在第八方面的第四种实现方式中，该 L2 ACP 报文的报文头还包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该处理模块具体用于，确定该第二网络设备的设备标识与该目的设备标识相匹配，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文，以及根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转

发基于该数据链路层的帧封装后的该 L2 ACP 报文。

结合第八方面的第三种或第四种实现方式，在第八方面的第五种实现方式中，该 L2 ACP 报文的报文头中还包括用于唯一标识该 L2 ACP 报文的报文 ID，

其中，该处理模块具体用于，当确定本地未缓存该报文 ID 时，通过判断该第二网络设备的设备标识是否与该目的设备标识相匹配，处理该 L2 ACP 报文。

结合第八方面的第三种至第五种实现方式中的任一种实现方式，在第八方面的第六种实现方式中，该 L2 ACP 报文的报文头中还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文，

该第二网络设备还包括:

缓存清除模块，用于当确定缓存该 L2 ACP 报文的时间超过该定时信息所指示的预设时长时，清除该 L2 ACP 报文。

结合第八方面及其上述实现方式，在第八方面的第七种实现方式中，该自组织网络内的每个自组织设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，其中，该 L2 ACP 报文还包括目的 IP 地址，

该处理模块具体用于，当确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识不匹配时，根据该 L2 ACP 报文的目的数据链路层地址向该第二网络设备的邻居设备转发该 L2 ACP 报文;

当确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识相匹配、且该第二网络设备的 IP 地址与该 L2 ACP 报文的该目的 IP 地址相匹配时，解析该 L2 ACP 报文。

结合第八方面及其上述实现方式，在第八方面的第八种实现方式中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

结合第八方面及其上述实现方式，在第八方面的第九种实现方式中，该数据链路层地址为介质访问控制 MAC 地址。

结合第八方面及其上述实现方式，在第八方面的第十种实现方式中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

第九方面提供了一种基于数据链路层的系统，该系统包括上述第五方面

提供的网络设备和第六方面提供的登记 Registrar 设备。

第十方面提供了一种基于数据链路层的系统，该系统包括上述第七方面提供的网络设备和第八方面提供的网络设备。

基于上述技术方案，在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

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所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提供的基于数据链路层的通信方法的示意性流程图。

图 2 示出了本发明实施例提供的基于数据链路层的通信方法的示意图。

图 3 示出了本发明实施例提供的基于数据链路层的通信方法的另一示意性流程图。

图 4 示出了本发明实施例提供的基于数据链路层的通信方法的再一示意性流程图。

图 5 示出了本发明实施例提供的基于数据链路层的通信方法的再一示意性流程图。

图 6 示出了本发明实施例提供的网络设备的示意性框图。

图 7 示出了本发明实施例提供的 Registrar 设备的示意性框图。

图 8 示出了本发明实施例提供的另一网络设备的示意性框图。

图 9 示出了本发明实施例提供的再一网络设备的示意性框图。

图 10 示出了本发明实施例提供的基于数据链路层的系统的示意性框图。

图 11 示出了本发明另一实施例提供的基于数据链路层的系统的示意性

框图。

图 12 示出了本发明另一实施例提供的网络设备的示意性框图。

图 13 示出了本发明另一实施例提供的 Registrar 设备的示意性框图。

图 14 示出了本发明另一实施例提供的另一网络设备的示意性框图。

图 15 示出了本发明另一实施例提供的再一网络设备的示意性框图。

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。

应理解，本发明的技术方案可以应用于各种通信系统，例如固定网络通信系统，具体地例如接入网络系统、汇聚网络系统、骨干网络系统、专用网络系统等固定网络系统。本发明的技术方案可以应用于移动通信系统，具体地，例如为通用移动通信系统（Universal Mobile Telecommunication System，简称为“UMTS”）、全球移动通讯（Global System of Mobile communication，简称为“GSM”）系统、通用分组无线业务（General Packet Radio Service，简称为“GPRS”）、长期演进（Long Term Evolution，简称为“LTE”）系统等移动通信系统，本发明实施例对此不作限定。

还应理解，本发明实施例涉及到的设备可以为网络设备，具体地，例如路由器、交换机、或者用户设备，其中，该用户设备也可称之为终端、移动台（Mobile Station，简称为“MS”）、移动终端（Mobile Terminal）等，该用户设备可以经有线网络接入 Internet 或者企业网络；该用户设备也可以经无线接入网（Radio Access Network，简称为“RAN”）与一个或多个核心网进行通信，例如，该用户设备可以是移动电话（或称为“蜂窝”电话）、具有移动终端的计算机，还可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和/或数据。

应理解，现有的 ACP 技术方案中，要支持自组织特性，需要先支持 IPv6，就 ACP 的构建依赖于 IPv6 的实现，网络兼容性差，网络部署有困难，给管理工作带来麻烦。

应理解，现有技术是基于网络层（也可称之为 L3 层）建立 ACP。本发

明是基于数据链路层（也可称之为 L2 层）建立 ACP，相对于现有技术，实现了建立 ACP 可以不感知 IP 协议，也就是不依赖于网络设备是支持 IPv4 协议，还是支持 IPv6 协议，而且支持 IPv4 的网络设备和支持 IPv6 协议的网络设备可以共同组成自组织网络，提高了网络兼容性，降低了部署困难。

应理解，本发明实施例中涉及的设备均为自组织设备，即该设备支持自组织特性，该设备有自己的唯一设备标识（Unique Device Identification，简称为“UDI”），或者设备证书（IDevID Certificate）。其中，设备支持自组织特性，指的是设备具有自动建立 ACP 或者自动加入 ACP 的功能。

还应理解，本发明实施例中涉及的登记 Registrar 设备指的是能够为自组织域内的设备（包括该 Registrar 设备）分配域证书的设备，例如该 Registrar 设备与数字证书认证管理机构有连接，且可以通信，换句话说，该 Registrar 设备能够通过数字证书认证管理结构为自组织域内的所有设备分配域证书。具体地，例如 Registrar 设备根据设备的设备标识，判断该设备是否允许加入自组织域，如果确定允许，则根据该设备的设备标识为其分配域证书，反之亦然。具体地，设备的设备标识可以是唯一设备标识 UDI，也可以是设备证书，本发明实施例对此不作限定。应理解，Registrar 设备首先会给自己分配域证书。

图 1 示出了本发明实施例提供的基于数据链路层的通信方法 100 的示意性流程图，该方法例如可以由自组织网络中的网络设备来执行，该方法 100 包括:

S110，网络设备生成邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识;

S120，该网络设备基于数据链路层的帧封装该 AD 消息，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址;

应理解，该数据链路层的帧的目的数据链路层地址可以为广播数据链路层地址，或者为该网络设备的邻居设备的数据链路层地址。

S130，该网络设备基于该目的数据链路层地址，向 Registrar 设备发送基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备;

S140，该网络设备接收该 Registrar 设备发送的域证书，该域证书为该

Registrar 设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的;

S150，该网络设备根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

在本发明实施例中，可选地，该数据链路层地址为介质访问控制（Media Access Control，简称为“MAC”）地址。

下文的示例中均以数据链路层地址为 MAC 地址为例进行描述。

应理解，在本发明实施例中，基于数据链路层的帧封装邻接发现（Adjacency Discovery，简称为“AD”）消息。应理解，在本发明实施例中，生成 AD 消息后，直接基于数据链路层的帧封装该 AD 消息，并不基于 IP 的报文封装该 AD 消息。换句话说，在本发明实施例中，AD 消息直接封装在数据链路层的帧中，不再基于 IP 报文封装。因此，本发明实施例中的 AD 消息对 IP 协议或者 IP 地址可以不感知，从而，自组织控制平面 ACP 的实现可以不依赖于 IP 协议，例如 IPv6 或 IPv4。因此，在本发明实施例中，基于数据链路层实现 ACP，相比于现有技术具有较好的网络兼容性，也降低了自组织网络部署的难度。

还应理解，该数据链路层的帧的目的数据链路层地址为数据链路层广播地址或该网络设备的邻居设备的数据链路层地址，其中，该邻居设备可以为该 Registrar 设备或 Proxy 设备。该 Registrar 设备可以是该网络设备的邻居设备，也可以是非邻居设备，本发明实施例对此不作限定。

可选地，在本发明实施例中，该网络设备的邻居设备包括该 Registrar 设备;

其中，该数据链路层的帧的目的 MAC 地址为该 Registrar 设备的 MAC 地址或 MAC 广播地址;

S130 该网络设备基于该目的数据链路层地址，向 Registrar 设备发送基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备，包括:

该网络设备根据该目的 MAC 地址，直接向该 Registrar 设备发送基于数据链路层的帧封装后的该 AD 消息。

换句话说，该 AD 消息从网络设备到该 Registrar 设备，无需中间设备的转发。这种情形也可称之为，该 AD 消息以邻居单播的方式，从网络设备传输至 Registrar 设备。

可选地，在本发明实施例中，该 Registrar 设备不是该网络设备的邻居设备;

其中，该数据链路层的帧的目的 MAC 地址为 MAC 广播地址;

S130 该网络设备基于该目的数据链路层地址，向 Registrar 设备发送基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备，包括:

该网络设备基于该目的数据链路层地址，通过具备由 Registrar 设备分配的域证书的 Proxy 设备，向该自组织网络中支持分配域证书的 Registrar 设备发送基于数据链路层的帧封装后的该 AD 消息。

具体地，以图 2 为例进行说明，例如网络设备为图 2 中的设备 5，Registrar 设备为图 2 中的设备 1，这种情形下，设备 5 向中间设备 2 发送 AD 消息，中间设备 2 确定所述网络设备还不具备域证书时，向该 Registrar 设备申请该设备 5 的域证书，该中间设备 2 还接收该 Registrar 设备为该设备 5 分配的域证书，并将该设备 5 的域证书发送给该设备 5，其中，该中间设备 2 为已经具备由 Registrar 设备分配的域证书的网络设备，已经具备域证书的网络设备可以称之为 Proxy 设备。

在 S150 中，该网络设备与该 Registrar 设备建立自组织控制平面 ACP，具体地，该网络设备与该 Registrar 设备基于网络设备的域证书以及 Registrar 设备的域证书（Registrar 设备会首先给自己分配域证书），相互认证，在数据链路层建立安全连接，例如建立 MACsec 通路，这个过程可称之为在网络设备与 Registrar 设备之间建立自组织控制平面 ACP。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧

的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

具体地，本发明实施例中的 L2 ACP 报文用于指示基于数据链路层的在 ACP 上传输的报文。应理解，基于数据链路层的帧封装该 AD 消息，即该数据链路层的帧的数据载荷字段承载该 AD 消息，其中，该数据链路层的帧的 Type 字段指示该数据载荷字段承载的消息为 L2 ACP 报文，可以认为 L2 ACP 报文包括该 AD 消息。

具体地，例如该数据链路层的帧的类型 Type 字段的 Type 值为 0x88e7。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

具体地，该 AD 消息的报文头包括用于指示该 L2 ACP 报文为该 AD 消息的标志位字段。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

具体地，表 1 示出了根据本发明实施例提供的 AD 消息的格式:

表 1

报文头
报文内容

从表 1 可知，根据本发明实施例提供的 AD 消息包括报文头和报文内容，其中，报文内容中包括了网络设备的设备标识（例如 UDI）或域证书等信息，应理解，当网络设备分配了域证书后，其 AD 消息里可以携带其域证书。

AD 消息的报文头具体可以如表 2 所示:

表 2

版本	标志位	协议	数据包长度

如表 2 所示，该 AD 消息的报文头包括版本字段、标志位字段、协议字段和数据包长度字段，其中，版本字段的值指示的该 AD 消息对应的协议的版本，例如该版本字段共 4 位；该标志位字段为 4 位，例如该标志位字段的值为 0000，用于指示该 AD 消息为该 AD 消息；协议字段的值用于指示该数据链路层的帧的数据载荷字段携带的内容的协议，协议字段共 8 位，例如可以使用与 IP 协议对应的协议字段的取值；数据包长度字段指共 16 位，其值

用于指示整个数据包的长度。

基于数据链路层的帧封装之后的 AD 消息的格式如表 3 所示:

表 3

目的 MAC 地址	源 MAC 地址	类型 Type
报文头		
报文内容		

由表 3 可知，基于数据链路层的帧封装之后的 AD 消息的格式包括该数据链路层的帧的帧头、报文头和报文内容，其中，报文头与报文内容如上文结合表 1 和表 2 所示。该数据链路层的帧的帧头包括目的 MAC 地址、源 MAC 地址和类型 Type 字段，其中目的 MAC 地址可以为 MAC 广播地址或者是该网络设备的邻居设备的 MAC 地址；源 MAC 地址为该网络设备的 MAC 地址。类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文，具体地，该 Type 字段可申请赋值为 0x88e7。

应理解，表 1、表 2 和表 3 仅作为示例而非限定。

应理解，在本发明实施例中，AD 消息也可以称之为 L2 ACP 报文，数据链路层的设备均可识别该 AD 消息，即该 AD 消息可以在数据链路层有效传输、有效接收。例如，Registrar 设备接收到来自于网络设备的基于数据链路层封装的 AD 消息后，通过该数据链路层的帧进行解析获取到该 AD 消息，从而获取 AD 消息中携带的该网络设备的设备标识（例如 UDI）或 MAC 地址等信息。

在 S140 中，该网络设备接收该 Registrar 设备发送的域证书，该域证书为该 Registrar 设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的，具体地，该 Registrar 设备根据设备标识判断该网络设备是否允许加入自组织网络，确定允许的情况下，根据该设备标识分配域证书，并发送给该网络设备。

可选地，在本发明实施例中，该设备标识为唯一设备标识（Unique Device Identification，简称为“UDI”）或者安全的唯一设备标识（Safe Unique Device Identification，简称为“SUDI”）。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的唯

一设备标识 UDI;

该网络设备接收该 Registrar 设备根据该设备标识发送的域证书，包括:

该网络设备接收该 Registrar 设备根据该网络设备的 UDI 发送的域证书，该域证书是该 Registrar 设备在确定白名单具有该网络设备的 UDI 的匹配项的情况下为该网络设备配置的，该白名单包括允许加入自组织域的设备的 UDI。

具体地，例如，当该设备标识为 UDI 时，该 Registrar 设备通过白名单来判断该网络设备是否允许加入自组织域，该白名单记载了允许加入该自组织域的设备的 UDI，当 Registrar 设备在白名单内找到该网络设备的 UDI 的匹配项时，例如通过数字证书认证管理结构，基于该网络设备的 UDI，为该网络设备分配域证书; 如果 Registrar 网络设备在白名单内找不到该网络设备的 UDI 的匹配项，则确定该网络设备不允许加入自组织域。

应理解，给 Registrar 设备配置白名单，可以是人为配置的，也可以是通过其他的方式导入的，本发明实施例对此不作限定。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的安全的唯一设备标识 SUDI;

该网络设备接收该 Registrar 设备根据该设备标识发送的域证书，包括:

该网络设备接收该 Registrar 设备根据该 SUDI 发送的域证书，该域证书是该 Registrar 设备确定该 SUDI 对应的设备数字证书有效时，以及根据验证服务器的验证结果确定该网络设备被允许加入自组织域时，确定该网络设备允许加入自组织域，根据该设备标识为该网络设备分配的。

具体地，例如，当该设备标识为安全的唯一设备标识 SUDI 时，该网络设备向该 Registrar 设备发送与该 SUDI 相对应的设备数字证书;

该 Registrar 设备在验证该设备数字证书有效，以及根据验证服务器的验证结果确定该网络设备被允许加入自组织域时，根据 SUDI，为该网络设备分配域证书。

为了便于描述和理解，在下文示例中，以设备标识为 UDI 为例进行描述。

应理解，自组织网络中的设备的自组织特性使能之后，会持续周期性（例如每隔 10s）地发送 AD 消息，以确定自己的邻居设备，该 AD 消息包括该自组织设备的 UDI，可选地，在该自组织设备具备域证书的情况下，该 AD 消息中也可以携带其域证书。每个设备根据接收到 AD 消息，构建自己的邻

居列表。

应理解，当设备 A 接收到一个 AD 消息，当确定该 AD 消息中携带的目的 MAC 地址（例如 MAC 广播地址）与本设备的 MAC 地址匹配，则可知该 AD 消息的源发送设备为自己的邻居设备，将该 AD 消息中携带的 UDI 和源 MAC 地址更新到自己的邻居列表中。

可选地，在本发明实施例中，该方法 100 还包括:

S160，该网络设备接收来自于该网络设备的邻居设备的基于数据链路层的帧封装后的 AD 消息，该 AD 消息包括邻居节点的设备标识与 MAC 地址;

应理解，来自于该网络设备的邻居设备的该基于数据链路层的帧封装后的 AD 消息的格式也如上述表 3 所示。

S170，该网络设备根据该 AD 消息，建立该网络设备的邻居列表，该邻居列表包括该邻居设备的设备标识以及该邻居设备的数据链路层地址。

具体地，该邻居列表除了包括该邻居设备的设备标识以及该邻居设备的数据链路层地址（MAC 地址）之外，该邻居列表还可以包括邻居设备的安全认证信息，具体地，如表 4 所示:

表 4

UDI
MAC 地址
安全认证信息（Trust information）
安全认证验证信息（Validity of the trust）

如表 4 所示，一个设备的邻居列表包括邻居设备的 UDI、MAC 地址，以及安全信息和认证信息，其中，安全认证信息（Trust information）可以包括安全认证类型信息，认证时间等信息，例如，the certificate chain，if available; 安全认证验证信息（Validity of the trust）用于指示邻居设备是否通过 Registrar 设备的认证，即是否分配了域证书。

具体地，图 2 示出了自组织网络的示意图，示意性地给出了 11 个自组织设备，其中，假设设备 1 为 Registrar 设备，设备 2、3 和 4 为设备 1 的邻居设备，设备 5 和 6 为设备 2 的邻居设备，设备 7 和 8 为设备 6 的邻居设备，设备 7 也是设备 5 的邻居设备，设备 9 和 10 为设备 3 的邻居设备，设备 11 为设备 4 的邻居设备。例如，设备 2 向 Registrar 设备发送包括设备 2 的 UDI

的 AD 消息(对应于本发明实施例中网络设备为 Registrar 设备的邻居设备的情形)，Registrar 设备在白名单里找到设备 2 的 UDI 的匹配项，则为设备 2 分配域证书。然后 Registrar 设备与设备 2 基于各自的域证书，相互认证，创建安全的连接，即在设备 1 和设备 2 之间建立了 ACP。

上面例子中，Registrar 设备为设备 2 分配了域证书，并与之建立了安全连接，即设备 2 得到认证，这时，该设备 2 可以作为代理（Proxy）点或认证点，将自己邻居设备的 AD 消息转发给 Registrar 设备，以便于 Registrar 设备认证设备 2 的邻居设备。

具体地，例如设备 2 的邻居设备 5 还未得到域证书，当设备 2 接收到设备 5 发的 AD 消息后，设备 2 通过解析该 AD 消息，检测到设备 5 没有域证书，设备 2 基于此可以确定设备 5 还没有得到认证，就会触发将设备 5 的 AD 消息转发出去的流程,因为设备 2 已经与 Registrar 设备建立了安全连接，所以设备 2 是已知 Registrar 设备的 UDI 的，所以设备 2 可以基于 Registrar 设备的 UDI，将设备 5 的 AD 消息转发给 Registrar 设备，后续 Registrar 设备对设备 5 的认证以及分配域证书的过程与为设备 2 分配域证书的流程类似，这里不再赘述。应理解，Registrar 为设备 5 分配了域证书后，也是通过设备 2 转发给设备 5 的。

需要说明的是，在本实施例中，在设备 5 分配到域证书之前，设备 5 的 AD 消息中没有域证书，这时，设备 2 根据设备 5 的 AD 消息建立的邻居列表中，设备 5 对应的 Validity of the trust 条目是未通过认证的。后续当设备 5 获取域证书后发送的 AD 消息中会携带域证书。

应理解，对于任一个经过 Registrar 设备认证之后的代理（Proxy）点或认证点，当其确定自己的某个邻居设备的 Validity of the trust 条目是未通过认证的，就会将该邻居设备的 AD 消息转发至 Registrar 设备，以便于 Registrar 设备对该邻居设备进行认证。

还应理解，在图 2 所示的例子中，与设备 2 和设备 5 认证过程类似，图 2 所示的其他自组织设备的 AD 消息都会传输至 Registrar 设备进行认证，假设 Registrar 设备为图 2 所示的所有设备都分配了域证书，即图 2 所示的各个设备之间均建立起安全连接，即这 11 个设备之间建立了自组织控制平面 ACP。

应理解，上文为了便于理解和描述，以图 2 为例描述了设备之间建立

ACP 的过程，图 2 仅为示例而非限定。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

上文结合图 1 和图 2，从 AD 消息的发送端设备的角度描述了本发明实施例提供的基于数据链路层的通信方法，下文从 AD 消息的接收端设备的角度描述本发明实施例提供的基于数据链路层的通信方法。

图 3 示出了本发明实施例提供的基于数据链路层的通信方法 200 的示意性流程图，该方法例如可以由自组织网络中支持分配域证书的登记 Registrar 设备来执行，该方法 200 包括:

S210，Registrar 设备接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配;

应理解，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配指的是，该目的数据链路层地址就是为该 Registrar 设备的数据链路层地址，或者该目的数据链路层地址为广播数据链路层地址，应理解，可以认为广播数据链路层地址与任意固定的数据链路层地址相匹配。

S220，当该 Registrar 设备确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书;

S230，该 Registrar 设备根据该域证书，与该网络设备建立自组织控制平面 ACP。

具体地，该网络设备与该 Registrar 设备基于网络设备的域证书以及 Registrar 设备的域证书（Registrar 设备会首先给自己分配域证书），相互认证，在数据链路层建立安全连接，例如建立 MACsec 通路，这个过程可称之

为在网络设备与 Registrar 设备之间建立自组织控制平面 ACP。

在本发明实施例中，设备的邻接发现 AD 消息是基于数据链路层的帧封装的；该 AD 消息基于数据链路层地址，发送至自组织网络中分配域证书的 Registrar 设备；该 Registrar 设备根据该 AD 消息为该设备分配域证书；基于该域证书，该设备与 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

应理解，在本发明实施例中，基于数据链路层的帧封装邻接发现（Adjacency Discovery，简称为“AD”）消息。应理解，在本发明实施例中，生成 AD 消息后，直接基于数据链路层的帧封装该 AD 消息，并不基于 IP 的报文封装该 AD 消息。换句话说，在本发明实施例中，AD 消息直接封装在数据链路层的帧中，不再基于 IP 报文封装。因此，本发明实施例中的 AD 消息对 IP 协议或者 IP 地址可以不感知，从而，自组织控制平面 ACP 的实现可以不依赖于 IP 协议，例如 IPv6 或 IPv4。因此，在本发明实施例中，基于数据链路层实现 ACP，相比于现有技术具有较好的网络兼容性，也降低了自组织网络部署的难度。

在本发明实施例中，可选地，该数据链路层地址为介质访问控制（Media Access Control，简称为“MAC”）地址。

下文的示例中均以数据链路层地址为 MAC 地址为例进行描述。

还应理解，该数据链路层的帧的目的数据链路层地址为数据链路层广播地址或该网络设备的邻居设备的数据链路层地址，该 Registrar 设备可以是该网络设备的邻居设备，也可以是非邻居设备，本发明实施例对此不作限定。

可选地，在本发明实施例中，该网络设备的邻居设备包括该 Registrar 设备；

其中，该数据链路层的帧的目的 MAC 地址为该 Registrar 设备的 MAC 地址或 MAC 广播地址。

具体地，该网络设备根据该目的 MAC 地址，直接向该 Registrar 设备发送基于数据链路层的帧封装后的该 AD 消息，换句话说，该 AD 消息是从网络设备一跳发送到该 Registrar 设备的，无需中间设备的转发。这种情形也可称之为，该 AD 消息以邻居单播的方式，从网络设备传输至 Registrar 设备。

可选地，在本发明实施例中，该 Registrar 设备不是该网络设备的邻居设备；

其中，该数据链路层的帧的目的 MAC 地址为 MAC 广播地址；

S210，Registrar 设备来自于网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，包括：

Registrar 设备通过具备由该 Registrar 设备分配的域证书的 Proxy 设备，接收该网络设备的邻接发现 AD 消息。

具体地，如图 2 所示的自组织网络的示意图，其中，假设设备 1 为 Registrar 设备，设备 2、3 和 4 为设备 1 的邻居设备，设备 5 和 6 为设备 2 的邻居设备，设备 7 和 8 为设备 6 的邻居设备，设备 7 也是设备 5 的邻居设备，设备 9 和 10 为设备 3 的邻居设备，设备 11 为设备 4 的邻居设备。例如，设备 2 向 Registrar 设备发送包括设备 2 的 UDI 的 AD 消息（对应于本发明实施例中网络设备为 Registrar 设备的邻居设备的情形），Registrar 设备在白名单里找到设备 2 的 UDI 的匹配项，则为设备 2 分配域证书。然后 Registrar 设备与设备 2 基于各自的域证书，相互认证，创建安全的连接，即在设备 1 和设备 2 之间建立了 ACP。

上面例子中，Registrar 设备为设备 2 分配了域证书，并与之建立了安全连接，即设备 2 得到认证，这时，该设备 2 可以作为代理（Proxy）点或认证点，将自己邻居设备的 AD 消息转发给 Registrar 设备，以便于 Registrar 设备认证设备 2 的邻居设备。

具体地，例如设备 2 的邻居设备 5 还未得到域证书，当设备 2 接收到设备 5 发的 AD 消息后，设备 2 通过解析该 AD 消息，检测到设备 5 没有域证书，设备 2 基于此可以确定设备 5 还没有得到认证，就会触发将设备 5 的 AD 消息转发出去的流程，因为设备 2 已经与 Registrar 设备建立了安全连接，所以设备 2 是已知 Registrar 设备的 UDI 的，所以设备 2 可以基于 Registrar 设备的 UDI，将设备 5 的 AD 消息转发给 Registrar 设备，后续 Registrar 设备对设备 5 的认证以及分配域证书的过程与为设备 2 分配域证书的流程类似，这里不再赘述。应理解，Registrar 为设备 5 分配了域证书后，也是通过设备 2 转发给设备 5 的。

需要说明的是，在本实施例中，在设备 5 分配到域证书之前，设备 5 的 AD 消息中没有域证书，这时，设备 2 根据设备 5 的 AD 消息建立的邻居列

表中，设备 5 对应的 Validity of the trust 条目是未通过认证的。后续当设备 5 获取域证书后发送的 AD 消息中会携带域证书。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

具体地，本发明实施例中的 L2 ACP 报文用于指示基于数据链路层的在 ACP 上传输的报文。应理解，基于数据链路层的帧封装该 AD 消息，即该数据链路层的帧的数据载荷字段承载该 AD 消息，其中，该数据链路层的帧的 Type 字段指示该数据载荷字段承载的消息为 L2 ACP 报文，可以认为 L2 ACP 报文包括该 AD 消息。

具体地，例如该数据链路层的帧的类型 Type 字段的 Type 值为 0x88e7。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

具体地，该 AD 消息的报文头包括用于指示该 L2 ACP 报文为该 AD 消息的标志位字段。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

基于数据链路层的帧封装之后的 AD 消息的格式如表 3 所示，具体描述见上文描述，为了简洁这里不再赘述。

可选地，在本发明实施例中，该网络设备为该 Registrar 设备的邻居设备，该方法 200 还包括:

S240，该 Registrar 设备根据该 AD 消息，建立该 Registrar 设备的邻居列表，该邻居列表包括该网络设备的设备标识以及该网络设备的数据链路层地址。

具体地，该 Registrar 设备根据该 AD 消息建立的邻居列表如表 4 所示，详述见上文。

在 S220 中，该 Registrar 设备当确定该邻居设备允许加入自组织域时，根据该设备标识为该邻居设备分配域证书，并发送给该网络设备。

可选地，在本发明实施例中，该设备标识为唯一设备标识（Unique Device Identification，简称为“UDI”）或者安全的唯一设备标识（Safe Unique Device Identification，简称为“SUDI”）。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的唯一设备标识 UDI，

其中，S220 当该 Registrar 设备确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书，包括：

S221，当该 Registrar 设备确定白名单具有该网络设备的 UDI 的匹配项时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该 UDI 分配的该域证书，该白名单包括允许加入该自组织网络的设备的 UDI。

具体地，例如，当该设备标识为 UDI 时，该 Registrar 设备通过白名单来判断该网络设备是否允许加入自组织域，该白名单记载了允许加入该自组织域的设备的 UDI，当 Registrar 设备在白名单内找到该网络设备的 UDI 的匹配项时，例如通过数字证书认证管理结构，基于该网络设备的 UDI，为该网络设备分配域证书；如果 Registrar 网络设备在白名单内找不到该网络设备的 UDI 的匹配项，则确定该网络设备不允许加入自组织域。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的安全的唯一设备标识 S-UDI，

其中，S220 当该 Registrar 设备确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书，包括：

S222，当该 Registrar 设备通过验证服务器确定该 S-UDI 对应的设备数字证书有效时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该设备数字证书分配的该域证书。

具体地，例如，当该设备标识为安全的唯一设备标识 SUDI 时，该网络设备向该 Registrar 设备发送与该 SUDI 相对应的设备数字证书；

该 Registrar 设备在验证该设备数字证书有效，以及根据验证服务器的验证结果确定该网络设备被允许加入自组织域时，根据 SUDI，为该网络设备分配域证书。

在本发明实施例中，设备的邻接发现 AD 消息是基于数据链路层的帧封装的；该 AD 消息基于数据链路层地址，发送至自组织网络中分配域证书的 Registrar 设备；该 Registrar 设备根据该 AD 消息为该设备分配域证书；基于该域证书，该设备与 Registrar 设备建立自组织控制平面 ACP。因此，在本

发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

应理解，自组织设备之间建立了 ACP 之后，上层的自组织功能实体可以使用该 ACP 平面传输控制消息，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

图 4 示出了本发明实施例提供的基于数据链路层的通信方法 300 的示意性流程图，该通信方法应用于自组织网络，该自组织网络的自组织控制平面 ACP 基于数据链路层建立，该方法 300 包括:

S310，第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，该第一网络设备为该自组织网络中的自组织设备;

具体地，第一网络设备从上层的自组织功能实体接收通信任务，例如该通信任务指示从第一网络设备向 ACP 内的目标设备发送控制消息，或者，指示该第一网络设备在 ACP 内广播控制消息等，第一网络设备根据该通信任务，生成该 L2 ACP 报文，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

S320，该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址;

应理解，该数据链路层的帧的目的数据链路层地址为该第一网络设备的邻居设备的数据链路层地址，或者为广播数据链路层地址。

S330，该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，该第二网络设备也为该自组织网络中的自组织设备，且该第二网络设备为该第一网络设备的邻居设备。

在本发明实施例中，基于数据链路层的帧封装该 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，网络设备可以无需像现有技术中一样维护路由表。

应理解，本发明实施例中的自组织控制平面 ACP 是基于数据链路层建立的，具体建立过程，详见上文方法 100 和方法 200 的描述，这里不再赘述。

还应理解，在本发明实施例中，L2 ACP 报文基于 L2 的帧封装，不再基于网络层的 IP 报文封装。换句话说，在本发明实施例中，可以利用数据链路层上的转发表资源（例如 MAC 转发表）来实现 L2 ACP 报文的传输，而无需依赖于网络层的 IP 协议或者 IP 路由表。

还应理解，在本发明实施例中，该 L2 的 MAC 转发表资源可以为每个设备所具有的邻居列表，例如，设备 A 的邻居列表中包括该设备 A 的邻居设备的设备标识与 MAC 地址，所以，当设备 A 需要发送 L2 ACP 报文时，基于邻居列表中包括的邻居设备(一个或多个)的 MAC 地址，确定该 L2 ACP 报文的目的 MAC 地址，从而将该 L2 ACP 报文发送到对应的邻居设备。或者是，将该 L2 ACP 报文的目的 MAC 地址设置为 MAC 广播地址，然后通过设备 A 与邻居设备的接口将该 MAC 报文发送出去。应理解，MAC 广播地址与任意的 MAC 地址都认为是相匹配的，所以设备 A 的邻居设备都能接收到该 L2 ACP 报文。

综上所述，在本发明实施例中，在 ACP 上传输信令，无需像现有技术中依赖于 IP 协议或者 IP 路由表来实现，可以不感知 IP 协议或 IP 地址，相比于现有技术，具有较好的网络兼容性。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制（Media Access Control，简称为“MAC”）地址。

下文的示例中均以数据链路层地址为 MAC 地址为例进行描述。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

具体地，例如该数据链路层的帧的类型 Type 字段的 Type 值为 0x88e7。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

具体地，表 5 示意性地给出了根据本发明实施例提供的 L2 ACP 报文的格式:

表 5

报文头
报文内容

从表 5 可知，该 L2 ACP 报文包括报文头和报文内容。其中，L2 ACP 报文的报文内容，例如，包括上层自组织功能实体下发的通信任务中指示的控制消息，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。L2 ACP 报文的报文头具体可以如表 6 所示：

表 6

版本	标志位	协议	数据包长度
源 UDI			
目的 UDI			

具体地，该 L2 ACP 报文的报文头包括版本字段、标志位字段、协议字段和数据包长度字段，以及源 UDI 和目的 UDI，其中源 UDI 为该第一网络设备的 UDI，目的 UDI 为目标设备的 UDI 或者广播 UDI。应理解，当 L2 ACP 报文为广播报文时，该 L2 ACP 报文中的目的 UDI 可以为空。版本字段的值指示的该 L2 ACP 报文对应的协议的版本，例如该版本字段共 4 位；该标志位字段为 4 位，用于指示该 L2 ACP 报文为邻居单播报文或非邻居单播报文或者广播报文，例如该标志位字段的值为 0001；协议字段的值用于指示该数据链路层的帧的数据载荷字段携带的内容的协议，协议字段共 8 位，例如可以使用与 IP 协议对应的协议字段的取值；数据包长度字段指共 16 位，其值用于指示整个数据包的长度。

基于数据链路层的帧封装之后的 L2 ACP 报文的格式如表 7 所示：

表 7

目的 MAC 地址	源 MAC 地址	类型 Type
报文头		
报文内容		

由表 7 可知，该数据链路层的帧的帧头包括目的 MAC 地址、源 MAC 地址和类型 Type 字段，其中目的 MAC 地址可以为 MAC 广播地址或者是为

目标设备的 MAC 地址；源 MAC 地址为第一网络设备的 MAC 地址。类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文，具体地，该 Type 字段可申请赋值为 0x88e7。

应理解，数据链路层上的设备接收到基于该数据链路层的封装的 L2 ACP 报文，通过其 Type 值能够识别出该 L2 ACP 报文为用于在 ACP 传输的报文。

应理解，表 5、表 6 和表 7 仅作为 L2 ACP 报文的示例而非限定。

应理解，在本发明实施例中，数据链路层的设备均可识别该 L2 ACP 报文，即 L2 ACP 报文可以在数据链路层有效传输、有效接收。例如，设备 2 接收到设备 5 发送的基于数据链路层的帧封装的 L2 ACP 报文后，基于数据链路层的帧进行解码获得该 L2 ACP 报文，进一步处理该 L2 ACP 报文，例如解析 L2 ACP 报文中的控制消息，或者不处理转发出去等，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

可选地，在本发明实施例中，S310 该第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

S311，该第一网络设备需要与该自组织网络中的目标设备通信时，当确定该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，该第一网络设备的邻居列表包括该第一网络设备的邻居设备的设备标识与数据链路层地址;

具体地，例如第一网络设备从上层的自组织功能实体接收到的通信任务，该通信任务指示该第一网络设备向 ACP 内的目标设备发送控制消息，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。应理解，第一网络设备可以从上层自组织功能实体获取到该目标设备的设备标识与 MAC 地址。

应理解，该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项指的是，该第一网络设备的邻居列表包括与该目标设备的设备标识相同的设备标识。还应理解，当该目标设备的设备标识为广播设备标识时，也可认为该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项。如果该第一网络设备的邻居列表不包括与该目标设备的设备标识相同的设备

标识、且该目标设备的设备标识也不是广播设备标识时，则认为该第一网络设备的邻居列表不包括该目标设备的设备标识的匹配项。

S320 该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，包括:

S321，该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

S330 该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，包括:

S331，该第一网络设备根据该目标设备的数据链路层地址，向该目标设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

具体地，该第一网络设备确定邻居列表中包括该目标设备的 UDI 的匹配项，则确定该 L2 ACP 报文的目的设备为自己的邻居设备，则生成该 L2 ACP 报文，该 L2 ACP 报文的报文头中包括用于指示邻居单播的标志位字段。

具体地，还以图 2 所示为例，例如上层自组织网络功能实体下发的传输任务一为从设备 5 向设备 2（设备 5 的邻居设备）传输目标信令，该传输任务一中携带设备 5 的 UDI。设备 5 根据传输任务一，确定 L2 ACP 报文，该 L2 ACP 报文包括该目标信令和目的 UDI，该目的 UDI 为该设备 2 的 UDI，并基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的 MAC 地址为该设备 2 的 MAC 地址，且该 L2 ACP 报文的报文头中的标志位字段用于指示邻居单播。

具体地，在本发明实施例中，L2 ACP 报文的格式如表 5 所示；L2 ACP 报文的报文头如表 6 所示，其中目的 UDI 为该目标设备的 UDI，其中标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，即用于指示该 L2 ACP 报文的接收设备不再向其他设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文，该标志位字段的值例如为 0001。基于数据链路层的帧封装后的该 L2 ACP 报文的格式如表 7 所示，其中目的 MAC 地址为该目标设备的 MAC 地址。

在本发明实施例中，当确定目标设备为第一网络设备的邻居设备时，生成 L2 ACP 报文，且该 L2 ACP 报文包括用于指示该 L2 ACP 报文为邻居单播报文的标志位，然后基于数据链路层的帧封装该 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协

议，相比于现有技术，具有较好的网络兼容性。此外，本发明实施例提供的方案也可以应用于部分设备配置为 IPv6，部分设备配置为 IPv4 的网络中。

此外，在本发明实施例中，网络设备无需维护路由表，就能实现 L2 ACP 报文的传输。

可选地，在本发明实施例中，S310 该第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

S312，该第一网络设备需要与该自组织网络中的目标设备通信时，当确定该邻居列表中不包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文;

S320，该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，包括:

S322，该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

S330，该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，包括:

S332，该第一网络设备根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

具体地，L2 ACP 报文的格式如表 5 所示；L2 ACP 报文的报文头如表 6 所示，其中目的 UDI 为该目标设备的 UDI，其中标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，即用于指示当该 L2 ACP 报文的接收设备的设备标识与该目的设备标识不匹配时，继续向该接收设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文；当该 L2 ACP 报文的接收设备的设备标识与该目的设备标相匹配时，解析该 L2 ACP 报文，不再转发。该标志位字段的值例如为 0002。基于数据链路层的帧封装之后的 L2 ACP 报文的格式如表 7 所示，其中，数据链路层的帧的目的 MAC 地址为 MAC 广播地址。

具体地，以图 2 为例，例如上层网络功能实体下发的传输任务为从设备 7 向设备 2（不是设备 7 的邻居设备）传输信令。则设备 7 向邻居设备 5 和 6 分别发送。基于数据链路层的帧封装之后 L2 ACP 报文。基于数据链路层的帧封装之后 L2 ACP 报文如表 7 所示，其中，报文内容中包括实际要传输的信令内容，源 UDI 即为设备 7 的 UDI，目的 UDI 为设备 2 的 UDI，标志位

是用于指示该报文为非邻居单播消息的标识。

对应地，设备 5 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2；类似的，设备 6 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2 和 8；当设备 2 接收到该 L2 ACP 报文后，通过解析，确定该报文为非邻居单播消息，然后检测目的 UDI 与自己的 UDI 匹配，则解析该 L2 ACP 报文的内容。

本发明实施例中描述的当上层的传输需求中指明的目的 UDI 不在设备的邻居列表中时，在设备之间传输信令的方法也可称之为采用泛洪的方式发送。

在本发明实施例中，当确定目标设备不是第一网络设备的邻居设备时，生成 L2 ACP 报文，且该 L2 ACP 报文包括用于指示该 L2 ACP 报文为非邻居单播报文的标志位，然后基于数据链路层的帧封装该 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。此外，本发明实施例提供的方案也可以应用于部分设备配置为 IPv6，部分设备配置为 IPv4 的网络中。

此外，在本发明实施例中，网络设备无需维护路由表，就能实现 L2 ACP 报文的传输。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括用于唯一指示该 L2 ACP 报文的报文 ID。

具体地，该 L2 ACP 报文的报文头如表 8 所示：

表 8

版本	标志位	协议	数据包长度
报文 ID			定时信息
源 UDI			
目的 UDI			

具体地，报文 ID 是该 L2 ACP 报文的生成设备上的唯一的字符串。报文 ID 是用于接收设备检测自己是否已经接收过相同的报文。具体，例如上

述例子中，设备 6 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2 和 8，则设备 2 会从自己的邻居设备 5 和 6 重复收到源自设备 7 的 L2 ACP 报文，L2 ACP 报文中包括报文 ID 就可以避免设备 2 重复处理相同的 L2 ACP 报文，例如当设备 2 首先接收到邻居设备 5 发送的 L2 ACP 报文，设备 2 在解析该 L2 ACP 报文后，缓存该 L2 ACP 报文，自然也保存了该 L2 ACP 报文的报文 ID。当设备 2 接收到设备 6 发送的源自设备 7 的 L2 ACP 报文时，解析该 L2 ACP 报文，检测到自己已经接收过该 L2 ACP 报文，就可以对该 L2 ACP 报文作丢弃操作。

在本发明实施例中，在 L2 ACP 报文包括报文 ID，能够避免重复的信令转发。

应理解，表 8 中的版本字段、标志位字段、协议字段、数据包长度字段、源 UDI 与目的 UDI 的描述与上文结合表 6 的描述一致，这里不再赘述。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

具体地，该 L2 ACP 报文的报文头如表 8 所示，有一个定时信息的字段，其值用于指示预设时间，用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

具体地，该定时信息例如为一个定时器，具体的时间值可以根据业务需求或者具体情况预配置，例如设备 5 接收到来自设备 7 的 L2 ACP 报文，并缓存该 L2 ACP 报文，缓存的时常超过阈值之后，可以认为该 L2 ACP 报文已经传输到目的 UDI 对应的设备了，即该 L2 ACP 报文的传输结束了，就可以删除该 L2 ACP 报文了。可选的，该定时信息也可以是一个时间戳。

在本发明实施例中，在 L2 ACP 报文包括定时信息，能够实现设备及时地清除已经传输完毕的 L2 ACP 报文，能够避免设备长时间缓存无用 L2 ACP 报文。

可选地，在本发明实施例中，S310 该第一网络设备生成 L2 ACP 报文，包括:

S313，当该第一网络设备需要在该 ACP 内广播控制消息时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用

于指示该 L2 ACP 报文为广播报文;

S320，该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，包括:

S323，该第一网络设备基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，S330 该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，包括:

S333，该第一网络设备根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

具体地，L2 ACP 报文的格式如表 5 所示，L2 ACP 报文的报文头如表 6 所示，其中标志位字段的值用于指示该 L2 ACP 报文为广播报文，即用于指示该 L2 ACP 报文的接收设备解析该 L2 ACP 报文，并向该接收设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文，例如，该标志位字段的值例如为 0003。

具体地，例如第一网络设备从上层的自组织功能实体接收到的通信任务，该通信任务指示该第一网络设备在 ACP 内广播控制消息，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。还以图 2 为例，例如上层网络功能实体下发的任务是从设备 6 广播 L2 ACP 报文。设备 6 生成的 L2 ACP 报文如表 5 和表 6 所示，该 L2 ACP 报文的报文头的标志位字段的值用于指示广播报文；基于数据链路层的帧封装该 L2 ACP 报文，其中，数据链路层的帧的目的 MAC 地址为 MAC 广播地址。设备 6 的邻居设备接收到该 L2 ACP 报文，通过解析确定该 L2 ACP 报文为广播报文，继续转发给自己的邻居设备 2、7 和 8 和 7，类似的，设备 2、7 和 8 继续向自己的邻居设备转发该 L2 ACP 报文。

应理解，当 L2 ACP 报文为广播报文时，其报文头中的目的 UDI 可以为广播 UDI，或者该目的 UDI 为空。

在本发明实施例中，当需要广播控制消息时，生成 L2 ACP 报文，且该 L2 ACP 报文包括用于指示该 L2 ACP 报文为广播报文的标志位，然后基于数据链路层的帧封装该 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。此外，本发明实施例提供的方案也可以应用于部分设备

配置为 IPv6，部分设备配置为 IPv4 的网络中。

此外，在本发明实施例中，网络设备无需维护路由表，就能实现 L2 ACP 报文的传输。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括用于唯一指示该 L2 ACP 报文的报文 ID。

具体地，该 L2 ACP 报文的报文头如表 8 所示。

具体地，报文 ID 是该 L2 ACP 报文的生成设备上的唯一的字符串。报文 ID 是用于接收设备检测自己是否已经接收过相同的报文。具体，例如上述例子中，设备 6 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2 和 8，则设备 2 会从自己的邻居设备 5 和 6 重复收到源自设备 7 的 L2 ACP 报文，L2 ACP 报文中包括报文 ID 就可以避免设备 2 重复处理相同的 L2 ACP 报文，例如当设备 2 首先接收到邻居设备 5 发送的 L2 ACP 报文，设备 2 在解析该 L2 ACP 报文后，缓存该 L2 ACP 报文，自然也保存了该 L2 ACP 报文的报文 ID。当设备 2 接收到设备 6 发送的源自设备 7 的 L2 ACP 报文时，解析该 L2 ACP 报文，检测到自己已经接收过该 L2 ACP 报文，就可以对该 L2 ACP 报文作丢弃操作。

在本发明实施例中，在 L2 ACP 报文包括报文 ID，能够避免重复的信令转发。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

具体地，该 L2 ACP 报文的报文头如表 8 所示，有一个定时信息的字段，其值用于指示预设时间，用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

具体地，该定时信息例如为一个定时器，具体的时间值可以根据业务需求或者具体情况预配置，例如设备 5 接收到来自设备 7 的 L2 ACP 报文，并缓存该 L2 ACP 报文，缓存的时常超过阈值之后，可以认为该 L2 ACP 报文已经传输到目的 UDI 对应的设备了，即该 L2 ACP 报文的传输结束了，就可以删除该 L2 ACP 报文了。可选的，该定时信息也可以是一个时间戳。

在本发明实施例中，在 L2 ACP 报文包括定时信息，能够实现设备及时

地清除已经传输完毕的 L2 ACP 报文，能够避免设备长时间缓存无用 L2 ACP 报文。

应理解，在本发明实施例中，数据链路层的设备均可识别该 L2 ACP 报文，即 L2 ACP 报文可以在数据链路层有效传输、有效接收。例如，设备 2 接收到设备 5 发送的基于数据链路层的帧封装后的 L2 ACP 报文后，基于数据链路层的帧进行解码获取到该 L2 ACP 报文，匹配该 L2 ACP 报文中的目的 UDI 与设备 2 的 UDI，匹配成功后，解析获取该 L2 ACP 报文中目标信令。

应理解，本发明实施例中 L2 ACP 报文的报文格式、以及封装该 L2 ACP 报文的数据链路层的帧的帧格式均是数据链路层的收发端设备都公知的，即数据链路层的设备都能够识别 L2 ACP 报文。

在本发明实施例中，基于数据链路层的帧封装 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

进一步地，在本发明实施例中，基于目标设备的设备标识（例如 UDI）和网络设备的邻居列表，在网络设备之间传输 L2 ACP 报文，而非依赖于 loopback 地址，从而避免了网络设备需要维护路由表。每个网络设备都具有自己的 UDI 和邻居列表，直接利用现成的资源去实现信令传输，能够降低维护成本。

此外，本发明实施例中的自组织网络以及自组织网络中的报文传输均可以不感知 IP 协议，因此并不苛求网络设备统一支持 IPv6 或者 IPv4，从而相对于现有技术，具有更好的网络兼容性，而且也降低了自组织网络部署的难度。

可选地，在本发明实施例中，自组织网络中的每个网络设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，

其中，S310 该第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

S314，当该第一网络设备需要通过 IP 会话与该 ACP 内的目标设备通信时，生成该 L2 ACP 报文，该 L2 ACP 报文还包括目的 IP 地址，该目的 IP 地址为该目标设备的 IP 地址。

具体地，该 L2 ACP 报文的格式如表 5 和表 6 所示，其中 L2 ACP 报文的报文头中的协议字段的值可以采用 IP 报文中的协议字段的值。

具体地，例如，某些上层业务，例如远端用户拨入验证服务（Remote Authentication Dial In User Service，简称为“RADIUS”），严格要求基于 IP，或者 TCP/UDP 来传输信令。

在本发明实施例中，ACP 内的每个自组织设备支持无重复的自配置的环回（Loopback）地址；且 ACP 内的每个自组织设备支持 UDI 和 IP 的映射（包括自己的和对端设备的）。

具体地，例如，上层的自组织代理（Agent）的传输需求中指明需要建立 IP 会话，则相关的服务设备（如 AAA）需要向客户设备发送自己的服务器 IP 地址和自己的 UDI，此阶段被称为服务自发现，或者 service advertisement。

客户设备接收到服务设备发送的消息后，绑定该 IP 地址，UDI，以及相关服务，并且通过一个自配置的 IPv6 ULA loopback 地址，或者 IPv4 loopback 地址，向服务器发起 IP 会话。

服务器的 UDI 层收到相关报文后，绑定该客户设备的 IP 和 UDI。

后续，在服务器和客户端的 ACP 通信中，服务端/客户端封装了 IP 包后，查找 IP 和 UDI 映射表，在 ACP 平面内基于 UDI 进行转发。

在本发明实施例涉及的场景下，虽然在上层设备应用看来它们之间在 ACP 平面内发起了一次 IP 会话，但是 ACP 平面仍然不提供基于 IP 的转发，网络设备无需维护相关的路由表。

因此，本发明实施例提供的 ACP 能够提供基于 IP 的通信能力，从而能够为上层应用提供更好的兼容性，让它们尽量无感知的使用基于 L2 层的 ACP。

在本发明实施例中，基于数据链路层的帧封装 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

进一步地，在本发明实施例中，基于目标设备的设备标识（例如 UDI）和网络设备的邻居列表，在网络设备之间传输 L2 ACP 报文，而非依赖于 loopback 地址，从而避免了网络设备需要维护路由表。每个网络设备都具有

自己的 UDI 和邻居列表，直接利用现成的资源去实现信令传输，能够降低维护成本。

此外，本发明实施例中的自组织网络以及自组织网络中的报文传输均可以不感知 IP 协议，因此并不苛求网络设备统一支持 IPv6 或者 IPv4，从而相对于现有技术，具有更好的网络兼容性，而且也降低了自组织网络部署的难度。

图 5 示出了本发明实施例提供的基于数据链路层的通信方法 400 的示意性流程图，该自组织网络的自组织控制平面 ACP 基于数据链路层建立，该自组织网络内的每个自组织设备均具有邻居列表，该邻居列表包括该每个自组织设备的邻居设备的设备标识与数据链路层地址，该方法 400 包括:

S410，第二网络设备接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，该 L2 ACP 报文包括目的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配，该第二网络设备与该第一网络设备均为该自组织网络中的自组织设备;

应理解，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配指的是，该目的数据链路层地址直接为该第二网络设备的数据链路层地址，或者，该目的数据链路层地址为广播数据链路层地址，应理解，广播数据链路层地址可以为认为任意固定的数据链路层地址相匹配。

S420，该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文。

应理解，当该目的设备标识直接就是该第二网络设备的设备标识时，或者该目的设备标识为广播设备标识时，则可认为该目的设备标识与该第二网络设备的设备标识相匹配，否则不匹配。

本发明实施例中的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该 L2 ACP 报文的目的数据链路层地址在 ACP 内传输该 L2 ACP 报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。此外，在本发明实施例中，网络设备可以无需像现有技术中一样维护路由表。

应理解，本发明实施例中的自组织控制平面 ACP 是基于数据链路层建

立的，具体建立过程，详见上文方法 100 和方法 200 的描述，这里不再赘述。

还应理解，在本发明实施例中，L2 ACP 报文基于 L2 的帧封装，不再基于网络层的 IP 报文封装。换句话说，在本发明实施例中，可以利用数据链路层上的转发表资源（例如 MAC 转发表）来实现 L2 ACP 报文的传输，而无需依赖于网络层的 IP 协议或者 IP 路由表。

还应理解，在本发明实施例中，该 L2 的 MAC 转发表资源可以为每个设备所具有的邻居列表，例如，设备 A 的邻居列表中包括该设备 A 的邻居设备的设备标识与 MAC 地址，所以，当设备 A 需要发送 L2 ACP 报文时，基于邻居列表中包括的邻居设备(一个或多个)的 MAC 地址，确定该 L2 ACP 报文的目的 MAC 地址，从而将该 L2 ACP 报文发送到对应的邻居设备。或者是，将该 L2 ACP 报文的目的 MAC 地址设置为 MAC 广播地址，然后通过设备 A 与邻居设备的接口将该 MAC 报文发送出去。应理解，MAC 广播地址与任意的 MAC 地址都认为是相匹配的，所以设备 A 的邻居设备都能接收到该 L2 ACP 报文。

综上所述，在本发明实施例中，在 ACP 上传输信令，无需像现有技术中依赖于 IP 协议或者 IP 路由表来实现，可以不感知 IP 协议或 IP 地址，相比于现有技术，具有较好的网络兼容性。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制（Media Access Control，简称为“MAC”）地址。

下文的示例中均以数据链路层地址为 MAC 地址为例进行描述。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

具体地，例如该数据链路层的帧的类型 Type 字段的 Type 值为 0x88e7。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

具体地，该 L2 ACP 报文如表 5 所示，该 L2 ACP 报文的报文头如表 6 所示，基于数据链路层的帧封装后的该 L2 ACP 报文如表 7 所示。具体描述见上文相关内容，这里不再赘述。

应理解，在本发明实施例中，数据链路层的设备均可识别该 L2 ACP 报文，即 L2 ACP 报文可以在数据链路层有效传输、有效接收。例如，设备 2 接收到设备 5 发送的基于数据链路层的帧封装的 L2 ACP 报文后，基于数据链路层的帧进行解码获得该 L2 ACP 报文，进一步处理该 L2 ACP 报文，例如解析 L2 ACP 报文中的控制消息，具体地，该控制消息可以为实现控制和/或管理功能的控制信令，或者不处理转发出去等。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址；

其中，S420 该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括：

S421，该第二网络设备确定该目的设备标识为该第二网络设备的设备标识，并解析该 L2 ACP 报文。

具体地，通过解析该 L2 ACP 报文，获取该 L2 ACP 报文中的报文内容，例如控制消息等，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。应理解，在本发明实施例中，该 L2 ACP 报文的接收设备不再向其邻居设备转发该 L2 ACP 报文。

具体地，在本发明实施例中，L2 ACP 报文的格式如表 5 所示；L2 ACP 报文的报文头如表 6 所示，其中目的 UDI 为该目标设备的 UDI，其中标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，即用于指示该 L2 ACP 报文的接收设备不再向其他设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文，该标志位字段的值例如为 0001。基于数据链路层的帧封装后的该 L2 ACP 报文的格式如表 7 所示，其中目的 MAC 地址为该目标设备的 MAC 地址。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

其中，S420 该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括：

S422，当该第二网络设备确定该第二网络设备的设备标识与该目的设备标识相匹配时，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文；

具体地，通过解析该 L2 ACP 报文，获取该 L2 ACP 报文中的报文内容，例如控制消息等，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

S423，当该第二网络设备确定该第二网络设备的设备标识与该目的设备标识不匹配时，缓存该 L2 ACP 报文，并根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

具体地，L2 ACP 报文的格式如表 5 所示；L2 ACP 报文的报文头如表 6 所示，其中目的 UDI 为该目标设备的 UDI，其中标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，即用于指示当该 L2 ACP 报文的接收设备的设备标识与该目的设备标识不匹配时，继续向该接收设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文；当该 L2 ACP 报文的接收设备的设备标识与该目的设备标相匹配时，解析该 L2 ACP 报文，不再转发。该标志位字段的值例如为 0002。基于数据链路层的帧封装之后的 L2 ACP 报文的格式如表 7 所示，其中，数据链路层的帧的目的 MAC 地址为 MAC 广播地址。

具体地，以图 2 为例，例如上层网络功能实体下发的传输任务为从设备 7 向设备 2（不是设备 7 的邻居设备）传输信令。则设备 7 向邻居设备 5 和 6 分别发送。基于数据链路层的帧封装之后 L2 ACP 报文。基于数据链路层的帧封装之后 L2 ACP 报文如表 7 所示，其中，报文内容中包括实际要传输的信令内容，源 UDI 即为设备 7 的 UDI，目的 UDI 为设备 2 的 UDI，标志位是用于指示该报文为非邻居单播消息的标识。

对应地，设备 5 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2；类似的，设备 6 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2 和 8；当设备 2 接收到该 L2 ACP 报文后，通过解析，确定该报文为非邻居单播消息，然后检测目的 UDI 与自己的 UDI 匹配，则解析该 L2 ACP 报文的内容。

本发明实施例中描述的当上层的传输需求中指明的目的 UDI 不在设备的邻居列表中时，在设备之间传输信令的方法也可称之为采用泛洪的方式发

送。

在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。此外，本发明实施例提供的方案也可以应用于部分设备配置为 IPv6，部分设备配置为 IPv4 的网络中。

此外，在本发明实施例中，网络设备无需维护路由表，就能实现 L2 ACP 报文的传输。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括用于唯一标识该 L2 ACP 报文的报文 ID，

其中，S420 该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

S425，当该第二网络设备确定本地未缓存该报文 ID 时，通过判断该第二网络设备的设备标识是否与该目的设备标识相匹配，处理该 L2 ACP 报文。

具体地，该 L2 ACP 报文的报文头如表 8 所示。

具体地，报文 ID 是源设备上的唯一的字符串。报文 ID 是用于接收设备检测自己是否已经接收过相同的报文。具体地，例如一个设备接收到 L2 ACP 报文，确定本地没有缓存该 L2 ACP 报文的报文 ID，即是第一次接收到该 L2 ACP 报文，则解析报文内容，并且缓存该报文 ID，然后向邻居设备转发该 L2 ACP 报文；如果一个设备接收到 L2 ACP 报文，确定本地已经缓存了该 L2 ACP 报文的报文 ID，则认为不是第一次收到该 L2 ACP 报文，则可以丢弃该报文。与第二种情况类似，当一个设备接收到 L2 ACP 报文之后，超过时间戳指示的时间后，可以删除这个 L2 ACP 报文。具体地，例如上述例子中，设备 6 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2 和 8，则设备 2 会从自己的邻居设备 5 和 6 重复收到源自设备 7 的 L2 ACP 报文，L2 ACP 报文中包括报文 ID 就可以避免设备 2 重复处理相同的 L2 ACP 报文，例如当设备 2 首先接收到邻居设备 5 发送的 L2 ACP 报文，设备 2 在解析该 L2 ACP 报文后，缓存该 L2 ACP 报文，自然也保存了该 L2 ACP 报文的报文 ID。当设备 2 接收到设备 6 发送的源自设备 7 的 L2 ACP 报文时，解析该 L2 ACP 报文，检测到自己已经接收过该 L2 ACP 报文，就可以对该 L2 ACP 报文作丢弃操作。

因此，在本发明实施例中，在验证 L2 ACP 报文中的设备标识是否与第

二网络设备的设备标识匹配之前，首先根据该报文 ID，验证第二网络设备是否已经收到过该 L2 ACP 报文（即检测本地是否已经缓存了该报文 ID），如果确定之前没有接收过该 L2 ACP 报文，则进行后续设备标识的判断，否则，可以丢弃该 L2 ACP 报文。

在 L2 ACP 报文包括报文 ID，能够避免重复的信令转发。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文，

该方法 400 还包括:

S430，当该第二网络设备确定缓存该 L2 ACP 报文的时间超过该定时信息所指示的预设时长时，清除该 L2 ACP 报文。

具体地，该定时信息例如为一个定时器，具体的时间值可以根据业务需求或者具体情况预配置，例如设备 5 接收到源自设备 7 的 L2 ACP 报文之后，根据该时间戳开始计时，计时超过阈值之后，可以认为该 L2 ACP 报文已经传输到目的 UDI 对应的设备了，即该 L2 ACP 报文的传输结束了，就可以删除该 L2 ACP 报文了。该定时信息也可以具体地为时间戳。

在本发明实施例中，在 L2 ACP 报文包括定时信息，能够实现设备及时地清除已经传输完毕的 L2 ACP 报文，能够避免设备长时间缓存无用 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，S420 该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

S424，该第二网络设备确定该第二网络设备的设备标识与该目的设备标识相匹配，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文，以及根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

具体地，L2 ACP 报文的格式如表 5 所示，L2 ACP 报文的报文头如表 6 所示，其中标志位字段的值用于指示该 L2 ACP 报文为广播报文，即用于指示该 L2 ACP 报文的接收设备解析该 L2 ACP 报文，并向该接收设备的邻居

设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文，例如，该标志位字段的值例如为 0003。

应理解，在本发明实施例中，该 L2 ACP 报文为广播报文，该 L2 ACP 报文中的目的设备标识可以为广播设备标识，则自组织网络中的任意网络设备接收到该 L2 ACP 报文，都会确定自己的设备标识与该目的设备标识相匹配。

还应理解，当该 L2 ACP 报文为广播报文的情况下，该 L2 ACP 报文中也可以不包括目的设备标识，网络设备根据该 L2 ACP 报文的标志位确定该 L2 ACP 报文为广播报文，则解析该 L2 ACP 报文，并转发，无需判断设备标识是否匹配。

具体地，还以图 2 为例，例如上层网络功能实体下发的任务是从设备 6 广播 L2 ACP 报文。设备 6 生成的 L2 ACP 报文如表 5 和表 6 所示，该 L2 ACP 报文的报文头的标志位字段的值用于指示广播报文；基于数据链路层的帧封装该 L2 ACP 报文，其中，数据链路层的帧的目的 MAC 地址为 MAC 广播地址。设备 6 的邻居设备接收到该 L2 ACP 报文，通过解析确定该 L2 ACP 报文为广播报文，继续转发给自己的邻居设备 2、7 和 8 和 7，类似的，设备 2、7 和 8 继续向自己的邻居设备转发该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括用于唯一标识该 L2 ACP 报文的报文 ID，

其中，S420 该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括：

S425，当该第二网络设备确定本地未缓存该报文 ID 时，通过判断该第二网络设备的设备标识是否与该目的设备标识相匹配，处理该 L2 ACP 报文。

具体地，该 L2 ACP 报文的报文头如表 8 所示。

具体地，报文 ID 是源设备上的唯一的字符串。报文 ID 是用于接收设备检测自己是否已经接收过相同的报文。具体地，例如一个设备接收到 L2 ACP 报文，确定本地没有缓存该 L2 ACP 报文的报文 ID，即是第一次接收到该 L2 ACP 报文，则解析报文内容，并且缓存该报文 ID，然后向邻居设备转发该 L2 ACP 报文；如果一个设备接收到 L2 ACP 报文，确定本地已经缓存了该 L2 ACP 报文的报文 ID，则认为不是第一次收到该 L2 ACP 报文，则可以丢弃该报文。与第二种情况类似，当一个设备接收到 L2 ACP 报文之后，超

过时间戳指示的时间后，可以删除这个 L2 ACP 报文。具体地，例如上述例子中，设备 6 接收到设备 7 发送的 L2 ACP 报文后，解析该 L2 ACP 报文为非邻居单播消息，检测目的 UDI 与自己的 UDI 不匹配，则将该 L2 ACP 报文转发给自己的邻居设备 2 和 8，则设备 2 会从自己的邻居设备 5 和 6 重复收到源自设备 7 的 L2 ACP 报文，L2 ACP 报文中包括报文 ID 就可以避免设备 2 重复处理相同的 L2 ACP 报文，例如当设备 2 首先接收到邻居设备 5 发送的 L2 ACP 报文，设备 2 在解析该 L2 ACP 报文后，缓存该 L2 ACP 报文，自然也保存了该 L2 ACP 报文的报文 ID。当设备 2 接收到设备 6 发送的源自设备 7 的 L2 ACP 报文时，解析该 L2 ACP 报文，检测到自己已经接收过该 L2 ACP 报文，就可以对该 L2 ACP 报文作丢弃操作。

因此，在本发明实施例中，在第二网络设备验证 L2 ACP 报文中的设备标识是否与该第二网络设备的设备标识匹配之前，首先根据该报文 ID，验证该第二网络设备是否已经收到过该 L2 ACP 报文（即检测本地是否已经缓存了该报文 ID），如果确定之前没有接收过该 L2 ACP 报文，则进行后续设备标识的判断，否则，可以丢弃该 L2 ACP 报文。

在 L2 ACP 报文包括报文 ID，能够避免重复的信令转发。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文，

该方法 400 还包括:

S430，当该第二网络设备确定缓存该 L2 ACP 报文的时间超过该定时信息所指示的预设时长时，清除该 L2 ACP 报文。

具体地，该 L2 ACP 报文的报文头如表 8 所示:

具体地，该定时信息例如为一个定时器，具体的时间值可以根据业务需求或者具体情况预配置，例如设备 5 接收到源自设备 7 的 L2 ACP 报文之后，根据该时间戳开始计时，计时超过阈值之后，可以认为该 L2 ACP 报文已经传输到目的 UDI 对应的设备了，即该 L2 ACP 报文的传输结束了，就可以删除该 L2 ACP 报文了。该定时信息也可以具体地为时间戳。

在本发明实施例中，在 L2 ACP 报文包括定时信息，能够实现设备及时地清除已经传输完毕的 L2 ACP 报文，能够避免设备长时间缓存无用 L2 ACP 报文。

在本发明实施例中，基于数据链路层的帧封装 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

进一步地，在本发明实施例中，基于目标设备的设备标识（例如 UDI）和网络设备的邻居列表，在网络设备之间传输 L2 ACP 报文，而非依赖于 loopback 地址，从而避免了网络设备需要维护路由表。每个网络设备都具有自己的 UDI 和邻居列表，直接利用现成的资源去实现信令传输，能够降低维护成本。

此外，本发明实施例中的自组织网络以及自组织网络中的报文传输均可以不感知 IP 协议，因此并不苛求网络设备统一支持 IPv6 或者 IPv4，从而相对于现有技术，具有更好的网络兼容性，而且也降低了自组织网络部署的难度。

可选地，在本发明实施例中，自组织网络中的每个网络设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，其中，该 L2 ACP 报文还包括目的 IP 地址，

其中，S420 该第二网络设备通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文，包括:

S426，当该第二网络设备确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识不匹配时，根据该 L2 ACP 报文的目的数据链路层地址向该第二网络设备的邻居设备转发该 L2 ACP 报文;

S427，当该第二网络设备确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识相匹配、且该第二网络设备的 IP 地址与该 L2 ACP 报文的该目的 IP 地址相匹配时，解析该 L2 ACP 报文。

具体地，该 L2 ACP 报文的格式如表 5 和表 6 所示，其中 L2 ACP 报文的报文头中的协议字段的值可以采用 IP 报文中的协议字段的值。

具体地，例如，某些上层业务，例如远端用户拨入验证服务（Remote Authentication Dial In User Service，简称为“RADIUS”），严格要求基于 IP，或者 TCP/UDP 来传输信令。

在本发明实施例中，ACP 内的每个自组织设备支持无重复的自配置的环回（Loopback）地址; 且 ACP 内的每个自组织设备支持 UDI 和 IP 的映射（包

括自己的和对端设备的）。

具体地，例如，上层的自组织代理（Agent）的传输需求中指明需要建立 IP 会话，则相关的服务设备（如 AAA）需要向客户设备发送自己的服务器 IP 地址和自己的 UDI，此阶段被称为服务自发现，或者 service advertisement。

客户设备接收到服务设备发送的消息后，绑定该 IP 地址，UDI，以及相关服务，并且通过一个自配置的 IPv6 ULA loopback 地址，或者 IPv4 loopback 地址，向服务器发起 IP 会话。

服务器的 UDI 层收到相关报文后，绑定该客户设备的 IP 和 UDI。

后续，在服务器和客户端的 ACP 通信中，服务端/客户端封装了 IP 包后，查找 IP 和 UDI 映射表，在 ACP 平面内基于 UDI 进行转发。

在本发明实施例涉及的场景下，虽然在上层设备应用看来它们之间在 ACP 平面内发起了一次 IP 会话，但是 ACP 平面仍然不提供基于 IP 的转发，网络设备无需维护相关的路由表。

因此，本发明实施例提供的 ACP 能够提供基于 IP 的通信能力，从而能够为上层应用提供更好的兼容性，让它们尽量无感知的使用基于 L2 层的 ACP。

应理解，本发明实施例中 L2 ACP 报文的报文格式是数据链路层的收发端设备都公知的，即数据链路层的设备都能够识别 L2 ACP 报文。

在本发明实施例中，利用 UDI 和设备的邻居列表，在 ACP 内传输信令，而非依赖于 loopback 地址，从而避免了每个设备需要维护路由表，每个设备都具有自己的 UDI 和邻居列表，直接利用现成的资源去实现信令传输，能够降低维护成本。

此外，本发明实施例中的 ACP 可以不感知 IP 协议，并不要求网络设备统一支持 IPv6 或者 IPv4 的情况才可以实现建立统一的 ACP，从而相对于现有技术，具有更好的网络兼容性，而且也降低了自组织网络部署的难度。

因此，在本发明实施例中，在 ACP 内，是基于设备的 UDI 来传输信令的，避免了现有技术中设备需要额外维护路由表的问题，能够节省部署成本。此外，在本发明实施例中，在 ACP 上传输信令，可以不感知 IP 协议，例如整个网络即使不支持 IPv6，也可以实现在 ACP 上传输信令，相比于现有技术，具有较好的网络兼容性，也能够减少网络部署的困难。此外，本发明实

施例提供的方案也可以应用于部分设备配置为 IPv6，部分设备配置为 IPv4 的网络中。

可选地，在本发明实施例中，方法 100 与方法 200 中涉及的 AD 消息（记为报文一）与方法 300 和方法 400 中涉及的 L2 ACP 报文（记为报文二）可以基于相同的数据链路层的帧格式封装，例如封装报文一的数据链路层的帧与封装报文二的数据链路层的帧的类型 Type 字段的取值可以采用同一个值。应理解，封装报文一的数据链路层的帧与封装报文二的数据链路层的帧的类型 Type 字段的取值也可以采用不同的值。

例如，当封装报文一与报文二的帧的类型 Type 采用同一个赋值时，利用报文头中的标志位的不同赋值来区分报文一和报文二。例如报文一与报文二的帧类型 Type 均为 88e7，但是报文一的报文头中的标志位为 0000，用于指示数据链路层的帧承载是邻接发现 AD 消息，报文二的报文头中的标志位为 0001，用于指示该数据链路层的帧承载的是 ACP 报文（即在 ACP 上传输信令的报文）。再具体地，例如该报文二分为邻居单播报文、非邻居单播报文和广播报文，可以通过对这三种不同传输类型的报文二的标志位赋不同的值，来区分不同传输类型的报文二，例如，当报文二的报文头中的标志位为 0001，指示数据链路层的帧承载的为邻居单播报文，当报文二的报文头中的标志位为 0002，指示数据链路层的帧承载的为非邻居单播报文，当报文二的报文头中的标志位为 0003，指示数据链路层的帧承载的为广播报文

例如，当报文一与报文二的帧类型 Type 采用不同赋值时，该帧类型 Type 可以用于区分报文一和报文二，例如封装报文一的数据链路层的帧类型 Type 赋值为 88e7，封装报文二的数据链路层的帧类型 Type 赋值为 88e8。再具体地，例如报文二分为邻居单播报文、非邻居单播报文和广播报文，则这三种传输类型的报文二的帧类型 Type 赋值也可以不同，以此来区分不同传输类型的报文二，例如，封装邻居单播报文的数据链路层的帧类型 Type 赋值为 88e8，封装非邻居单播报文的数据链路层的帧类型 Type 赋值为 88e9，封装广播报文的数据链路层的帧类型 Type 赋值为 88e6。应理解，还可以是，这三种传输类型的报文二的帧类型 Type 采用同一赋值，利用标志位来区分这三种传输类型的报文二，本发明实施例对此不作限定。

图 6 示出了本发明实施例提供的一种网络设备 500，该网络设备应用于自组织网络，该网络设备 500 包括:

生成模块 510，用于网络设备生成邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识；

封装模块 520，用于基于数据链路层的帧封装该生成模块生成的该 AD 消息，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址；

应理解，该数据链路层的帧的目的数据链路层地址可以为广播数据链路层地址，或者为该网络设备的邻居设备的数据链路层地址。

发送模块 530，用于基于该目的数据链路层地址，向登记 Registrar 设备发送该封装模块确定的基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备；

接收模块 540，用于接收该 Registrar 设备发送的域证书，该域证书为该 Registrar 设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的；

建立模块 550，用于根据该接收模块接收的该域证书，与该 Registrar 设备建立自组织控制平面 ACP。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

应理解，根据本发明实施例的网络设备 500 可对应于本发明实施例的基于数据链路层的通信方法中的网络设备，并且网络设备 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。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

图 7 示出了本发明实施例提供的一种登记 Registrar 设备 600，该 Registrar 设备 600 应用于自组织网络，该 Registrar 设备 600 为该自组织网络中支持分配域证书的设备，该 Registrar 设备 600 包括：

接收模块 610，用于接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配；

应理解，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配指的是，该目的数据链路层地址就是为该 Registrar 设备的数据链路层地址，或者该目的数据链路层地址为广播数据链路层地址，应理解，可以认为广播数据链路层地址与任意固定的数据链路层地址相匹配。

发送模块 620，用于当确定该网络设备允许加入该自组织网络时，根据该接收模块接收的该 AD 消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书；

ACP 建立模块 630，用于根据该发送模块发送的该域证书，与该网络设备建立自组织控制平面 ACP。

在本发明实施例中，设备的邻接发现 AD 消息是基于数据链路层的帧封

装的；该 AD 消息基于数据链路层地址，发送至自组织网络中分配域证书的 Registrar 设备；该 Registrar 设备根据该 AD 消息为该设备分配域证书；基于该域证书，该设备与 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

可选地，在本发明实施例中，该网络设备为该 Registrar 设备的邻居设备，该 Registrar 设备还包括：

邻居列表建立模块 640，用于根据该 AD 消息，建立该 Registrar 设备的邻居列表，该邻居列表包括该网络设备的设备标识以及该网络设备的数据链路层地址。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的唯一设备标识 UDI，

其中，该发送模块 620 具体用于，当确定白名单具有该网络设备的 UDI 的匹配项时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该 UDI 分配的该域证书，该白名单包括允许加入该自组织网络的设备的 UDI。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的安全的唯一设备标识 S-UDI，

其中，该发送模块 620 具体用于，当通过验证服务器确定该 S-UDI 对应的设备数字证书有效时，确定该网络设备允许加入该自组织网络，向该网络设备发送根据该设备数字证书分配的该域证书。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

应理解，根据本发明实施例的 Registrar 设备 600 可对应于本发明实施例的基于数据链路层的通信方法中的 Registrar 设备，并且 Registrar 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。

在本发明实施例中，设备的邻接发现 AD 消息是基于数据链路层的帧封装的；该 AD 消息基于数据链路层地址，发送至自组织网络中分配域证书的 Registrar 设备；该 Registrar 设备根据该 AD 消息为该设备分配域证书；基于该域证书，该设备与 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

图 8 示出了本发明实施例提供的网络设备 700，该网络设备用作第一网络设备，该第一网络设备应用于自组织网络，该网络设备 700 包括：

生成模块 710，用于生成数据链路层自组织控制平面 L2 ACP 报文，该第一网络设备为该自组织网络中的自组织设备；

封装模块 720，用于基于数据链路层的帧封装该生成模块生成的该 L2 ACP 报文，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址；

应理解，该数据链路层的帧的目的数据链路层地址为该第一网络设备的邻居设备的数据链路层地址，或者为广播数据链路层地址。

发送模块 730，用于根据该目的数据链路层地址，向第二网络设备发送该封装模块确定的基于该数据链路层的帧封装后的该 L2 ACP 报文，该第二网络设备也为该自组织网络中的自组织设备，且该第二网络设备为该第一网络设备的邻居设备。

在本发明实施例中，基于数据链路层的帧封装该 L2 ACP 报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文，在本发明实施例中，在 ACP 上传输报文可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，网络设备可以无需像现有技术中一样维护路由表。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义

的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

可选地，在本发明实施例中，该生成模块 710 具体用于，需要与该自组织网络中的目标设备通信时，当确定该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，该第一网络设备的邻居列表包括该第一网络设备的邻居设备的设备标识与数据链路层地址;

应理解，该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项指的是，该第一网络设备的邻居列表包括与该目标设备的设备标识相同的设备标识。还应理解，当该目标设备的设备标识为广播设备标识时，也可认为该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项。如果该第一网络设备的邻居列表不包括与该目标设备的设备标识相同的设备标识、且该目标设备的设备标识也不是广播设备标识时，则认为该第一网络设备的邻居列表不包括该目标设备的设备标识的匹配项。

该封装模块 720 具体用于，基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

该发送模块 730 具体用于，根据该目标设备的数据链路层地址，向该目标设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，该生成模块 710 具体用于，需要与该自组织网络中的目标设备通信时，当确定该邻居列表中不包括该目标设备的设备标识的匹配项时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文;

该封装模块 720 具体用于，基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

该发送模块 730 具体用于，根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，该生成模块 710 具体用于，需要在该 ACP 内广播控制消息时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文;

具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

该封装模块 720 具体用于，基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该发送模块 730 具体用于，根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括用于唯一指示该 L2 ACP 报文的报文 ID。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

可选地，在本发明实施例中，该自组织网络内的每个自组织设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，

该生成模块 710 具体用于，当需要通过 IP 会话与该 ACP 内的目标设备通信时，生成该 L2 ACP 报文，该 L2 ACP 报文还包括目的 IP 地址，该目的 IP 地址为该目标设备的 IP 地址。

应理解，根据本发明实施例的网络设备 700 可对应于本发明实施例的基于数据链路层的通信方法中的第一网络设备，并且网络设备 700 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。

本发明实施例中发送的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该 L2 ACP 报文的目的数据链路层地址在 ACP 内传输该 L2 ACP 报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，无需设备像现有技术中一样维护路由表，也能够实现基于 ACP 的通信。

图 9 示出了本发明实施例提供的一种网络设备 800，该网络设备 800 用作第二网络设备，该网络设备 800 应用于自组织网络，该网络设备 800 包括：

接收模块 810，用于接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，该 L2 ACP 报文包括目的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配，该第二网络设备与该第一网络设备均为该自组织网络中的自组织设备；

应理解，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配指的是，该目的数据链路层地址直接为该第二网络设备的数据链路层地址，或者，该目的数据链路层地址为广播数据链路层地址，应理解，广播数据链路层地址可以为认为任意固定的数据链路层地址相匹配。

处理模块 820，用于通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该接收模块接收的该 L2 ACP 报文。

应理解，当该目的设备标识直接解释该第二网络设备的设备标识时，或者该目的设备标识为广播设备标识时，则可认为该目的设备标识与该第二网络设备的设备标识相匹配，否则不匹配。

应理解，在本发明实施例中，该自组织网络的自组织控制平面 ACP 是基于数据链路层建立的，具体方法见上文方法 100 和 200 该，这里不再赘述。

本发明实施例中的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该 L2 ACP 报文的目的数据链路层地址在 ACP 内传输该 L2 ACP 报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，设备也无需像现有技术中一样维护路由表，也能够实现基于 ACP 的通信。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址；

其中，该处理模块 820 具体用于，确定该目的设备标识为该第二网络设备的设备标识，并解析该 L2 ACP 报文。

具体地，处理模块 820 具体用于具体地，通过解析该 L2 ACP 报文，获取该 L2 ACP 报文中的报文内容，例如控制消息等，具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该处理模块 820 具体用于，当确定该第二网络设备的设备标识与该目的设备标识相匹配时，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文;

具体地，通过解析该 L2 ACP 报文，获取该 L2 ACP 报文中的报文内容，例如控制消息等。

处理模块 820 具体用于，当确定该第二网络设备的设备标识与该目的设备标识不匹配时，缓存该 L2 ACP 报文，并根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，该处理模块 820 具体用于，确定该第二网络设备的设备标识与该目的设备标识相匹配，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文，以及根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

应理解，在本发明实施例中，该 L2 ACP 报文为广播报文，该 L2 ACP 报文中的目的设备标识可以为广播设备标识，则自组织网络中的任意网络设备接收到该 L2 ACP 报文，都会确定自己的设备标识与该目的设备标识相匹配。

还应理解，当该 L2 ACP 报文为广播报文的情况下，该 L2 ACP 报文中也可以不包括目的设备标识，网络设备根据该 L2 ACP 报文的标志位确定该 L2 ACP 报文为广播报文，则解析该 L2 ACP 报文，并转发，无需判断设备标识是否匹配。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括用于唯一标识该 L2 ACP 报文的报文 ID，

其中，该处理模块 820 具体用于，当确定本地未缓存该报文 ID 时，通过判断该第二网络设备的设备标识是否与该目的设备标识相匹配，处理该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文，

该网络设备 800 还包括:

缓存清除模块 830，用于当确定缓存该 L2 ACP 报文的时间超过该定时信息所指示的预设时长时，清除该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

可选地，在本发明实施例中，该自组织网络内的每个自组织设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，其中，该 L2 ACP 报文还包括目的 IP 地址，

该处理模块 820 具体用于，当该第二网络设备确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识不匹配时，根据该 L2 ACP 报文的目的数据链路层地址向该第二网络设备的邻居设备转发该 L2 ACP 报文;

该处理模块 820 具体用于，当该第二网络设备确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识相匹配、且该第二网络设备的 IP 地址与该 L2 ACP 报文的该目的 IP 地址相匹配时，解析该 L2 ACP 报文。

应理解，根据本发明实施例的网络设备 800 可对应于本发明实施例的基于数据链路层的通信方法中的第二网络设备，并且网络设备 800 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。

本发明实施例中发送的 L2 ACP 报文是基于数据链路层的帧封装的，可

以基于该L2 ACP报文的目的数据链路层地址在ACP内传输该L2 ACP报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，设备也无需像现有技术中一样维护路由表，也能够实现基于 ACP 的通信。

图 10 示出了本发明实施例提供的基于自组织网络的系统 900 的示意性框图，该系统 900 包括本发明实施例提供的网络设备 500 与 Registrar 设备 600。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

图 11 示出了本发明实施例提供的基于自组织网络的系统 1000 的示意性框图，该系统 1000 包括本发明实施例提供的网络设备 700 与网络设备 800。

本发明实施例中发送的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该L2 ACP报文的目的数据链路层地址在ACP内传输该L2 ACP报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，设备也无需像现有技术中一样维护路由表，也能够实现基于 ACP 的通信。

图 12 示出了本发明实施例提供的网络设备 1100 的示意性框图，该网络设备 1100 包括：处理器 1110、存储器 1120、总线系统 1130、接收器 1140 和发送器 1150。其中，处理器 1110、存储器 1120、接收器 1140 和发送器 1150 通过总线系统 1130 相连，该存储器 1120 用于存储指令，其中，处理器 1110 用于，生成邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识；基于数据链路层的帧封装该 AD 消息，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址；发送器 1150 用于，基于该目的数据链路层地址，向登记 Registrar

设备发送基于该数据链路层的帧封装后的该 AD 消息，该 Registrar 设备为自组织网络中支持分配域证书的设备；接收器 1140 用于，接收该 Registrar 设备发送的域证书，该域证书为该 Registrar 设备根据该 AD 消息中的该网络设备的设备标识为该网络设备分配的；处理器 1110 还用于，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

应理解，根据本发明实施例的网络设备 1100 可对应于本发明实施例的基于数据链路层的通信方法中的网络设备，以及可以对应于根据本发明实施例的网络设备 500，并且网络设备 1100 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。

在本发明实施例中，基于数据链路层的帧封装 AD 消息，基于该数据链路层的帧的目的数据链路层地址，向 Registrar 设备发送该基于数据链路层的帧封装后的该 AD 消息，接收该 Registrar 设备发送的域证书，根据该域证书，

与该 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

图 13 示出了本发明实施例提供的登记 Registrar 设备 1200 的示意性框图该 Registrar 设备 1200 应用于自组织网络中，该 Registrar 设备 1200 包括：处理器 1210、存储器 1220、总线系统 1230、接收器 1240 和发送器 1250。其中，处理器 1210、存储器 1220、接收器 1240 和发送器 1250 通过总线系统 1230 相连，该存储器 1220 用于存储指令，其中，

接收器 1240 用于，接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，该 AD 消息包括该网络设备的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址，该目的数据链路层地址与该 Registrar 设备的数据链路层地址相匹配；处理器 1210 用于，确定该网络设备允许加入该自组织网络时，根据该 AD 消息包括的该设备标识为该网络设备分配域证书；发送器 1250 用于，向该网络设备发送该域证书；处理器 1210 还用于，根据该域证书，与该网络设备建立自组织控制平面 ACP。

在本发明实施例中，设备的邻接发现 AD 消息是基于数据链路层的帧封装的；该 AD 消息基于数据链路层地址，发送至自组织网络中分配域证书的 Registrar 设备；该 Registrar 设备根据该 AD 消息为该设备分配域证书；基于该域证书，该设备与 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值指示该 L2 ACP 报文为该 AD 消息。

可选地，在本发明实施例中，该网络设备为该第二网络设备的邻居设备，处理器 1210 还用于，根据该 AD 消息，建立该第二网络设备的邻居列表，

该邻居列表包括该网络设备的设备标识以及该网络设备的数据链路层地址。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的唯一设备标识 UDI，

处理器 1210 还用于，当确定白名单具有该网络设备的 UDI 的匹配项时，确定该网络设备允许加入该自组织网络，根据该 UDI 分配该域证书，该白名单包括允许加入该自组织网络的设备的 UDI。

可选地，在本发明实施例中，该网络设备的设备标识为该网络设备的安全的唯一设备标识 S-UDI，

处理器 1210 还用于，当通过验证服务器确定该 S-UDI 对应的设备数字证书有效时，确定该网络设备允许加入该自组织网络，根据该设备数字证书分配该域证书。

可选地，在本发明实施例中，该 AD 消息的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

应理解，根据本发明实施例的 Registrar 设备 1200 可对应于本发明实施例的基于数据链路层的通信方法中的 Registrar 设备，以及可以对应于根据本发明实施例的 Registrar 设备 600，并且 Registrar 设备 1200 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。

在本发明实施例中，设备的邻接发现 AD 消息是基于数据链路层的帧封装的；该 AD 消息基于数据链路层地址，发送至自组织网络中分配域证书的 Registrar 设备；该 Registrar 设备根据该 AD 消息为该设备分配域证书；基于该域证书，该设备与 Registrar 设备建立自组织控制平面 ACP。因此，在本发明实施例中，建立 ACP 可以不依赖于 IP 协议，即实现基于自组织网络的通信可以对 IP 协议不感知，相对于现有技术，具有较好的网络兼容性，能够有效减小自组织网络的部署障碍。

图 14 示出了本发明实施例提供的网络设备 1300 的示意性框图，该网络设备 1300 应用于自组织网络，该网络设备 1300 用作第一网络设备，该网络设备 1300 包括：处理器 1310、存储器 1330、总线系统 1330、接收器 1340 和发送器 1350。其中，处理器 1310、存储器 1330、接收器 1340 和发送器

1350通过总线系统1330相连，该存储器1330用于存储指令，其中，处理器1310用于，生成数据链路层自组织控制平面L2 ACP报文，该第一网络设备为该自组织网络中的自组织设备；基于数据链路层的帧封装该L2 ACP报文，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址；发送器1350用于，根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该L2 ACP报文，该第二网络设备也为该自组织网络中的自组织设备，且该第二网络设备为该第一网络设备的邻居设备。

在本发明实施例中，基于数据链路层的帧封装该L2 ACP报文，并根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该L2 ACP报文，在本发明实施例中，在ACP上传输报文可以不依赖于IP协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，网络设备可以无需像现有技术中一样维护路由表。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型Type字段的Type值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面L2 ACP报文。

可选地，在本发明实施例中，处理器1310具体用于，需要与该自组织网络中的目标设备通信时，当确定该第一网络设备的邻居列表中包括该目标设备的设备标识的匹配项时，生成该L2 ACP报文，该L2 ACP报文的报文头包括标志位字段，该标志位字段的值用于指示该L2 ACP报文为邻居单播报文，该第一网络设备的邻居列表包括该第一网络设备的邻居设备的设备标识与数据链路层地址；基于数据链路层的帧封装该L2 ACP报文，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址；发送器1350具体用于，根据该目标设备的数据链路层地址，向该目标设备发送基于该数据链路层的帧封装后的该L2 ACP报文。

可选地，在本发明实施例中，处理器1310具体用于，需要与该自组织网络中的目标设备通信时，当确定该邻居列表中不包括该目标设备的设备标识的匹配项时，生成该L2 ACP报文，该L2 ACP报文的报文头包括标志位字段，该标志位字段的值用于指示该L2 ACP报文为非邻居单播报文；基于数据链路层的帧封装该L2 ACP报文，该数据链路层的帧的目的数据链路层

地址为广播数据链路层地址；发送器 1350 具体用于，根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，处理器 1310 具体用于，需要在该 ACP 内广播控制消息时，生成该 L2 ACP 报文，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文；基于数据链路层的帧封装该 L2 ACP 报文，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址；发送器 1350 具体用于，根据该广播数据链路层地址，向该第二网络设备发送基于该数据链路层的帧封装后的该 L2 ACP 报文。

具体地，该控制消息可以为实现控制和/或管理功能的控制信令。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括用于唯一指示该 L2 ACP 报文的报文 ID。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文。

可选地，在本发明实施例中，该自组织网络内的每个自组织设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，

处理器 1310 具体用于，当需要通过 IP 会话与该 ACP 内的目标设备通信时，生成该 L2 ACP 报文，该 L2 ACP 报文还包括目的 IP 地址，该目的 IP 地址为该目标设备的 IP 地址。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

应理解，根据本发明实施例的网络设备 1300 可对应于本发明实施例的基于数据链路层的通信方法中的第一网络设备，以及可以对应于根据本发明实施例的网络设备 700，并且网络设备 1300 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。

本发明实施例中发送的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该 L2 ACP报文的目的数据链路层地址在 ACP 内传输该 L2 ACP报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，无需设备像现有技术中一样维护路由表，也能够实现基于 ACP 的通信。

图 15 示出了本发明实施例提供的网络设备 1400 的示意性框图，该网络设备 1400 应用于自组织网络，该网络设备 1400 用作为第二网络设备，该网络设备 1400 包括: 处理器 1410、存储器 1420、总线系统 1440、接收器 1440 和发送器 1450。其中，处理器 1410、存储器 1420、接收器 1440 和发送器 1450 通过总线系统 1440 相连，该存储器 1420 用于存储指令，其中，接收器 1440 用于，接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，该 L2 ACP 报文包括目的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配，该第二网络设备与该第一网络设备均为该自组织网络中的自组织设备; 处理器 1410 用于，通过判断该第二网络设备的设备标识是否与该 L2 ACP 报文的该目的设备标识相匹配，处理该 L2 ACP 报文。

本发明实施例中发送的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该 L2 ACP报文的目的数据链路层地址在 ACP 内传输该 L2 ACP报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，网络设备可以无需像现有技术中一样维护路由表。

可选地，在本发明实施例中，该数据链路层的帧为符合以太网协议定义的帧，该数据链路层的帧的类型 Type 字段的 Type 值指示该数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为该目标设备的数据链路层地址;

处理器 1410 具体用于，确定该目的设备标识为该第二网络设备的设备标识，并解析该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为非邻居单播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

处理器 1410 具体用于，当确定该第二网络设备的设备标识与该目的设备标识相匹配时，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文；当确定该第二网络设备的设备标识与该目的设备标识不匹配时，缓存该 L2 ACP 报文，并根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括标志位字段，该标志位字段的值用于指示该 L2 ACP 报文为广播报文，其中，该数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

处理器 1410 具体用于，确定该第二网络设备的设备标识与该目的设备标识相匹配，解析该 L2 ACP 报文，并缓存该 L2 ACP 报文，以及根据该数据链路层的帧的目的数据链路层地址向该第二网络设备的邻居设备转发基于该数据链路层的帧封装后的该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括用于唯一标识该 L2 ACP 报文的报文 ID，

处理器 1410 具体用于，当确定本地未缓存该报文 ID 时，通过判断该第二网络设备的设备标识是否与该目的设备标识相匹配，处理该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头中还包括定时信息，该定时信息用于指示该 L2 ACP 报文的接收设备在缓存该 L2 ACP 报文的时间超过预设时长时，清除该 L2 ACP 报文，

处理器 1410 还用于，当确定缓存该 L2 ACP 报文的时间超过该定时信息所指示的预设时长时，清除该 L2 ACP 报文。

可选地，在本发明实施例中，该自组织网络内的每个自组织设备均具有 IP 地址，且该每个自组织设备具有该每个自组织设备的设备标识与该每个自组织设备的 IP 地址之间的映射，其中，该 L2 ACP 报文还包括目的 IP 地址，

处理器 1410 具体用于，当确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识不匹配时，根据该 L2 ACP 报文的目的数据链路层地

址向该第二网络设备的邻居设备转发该 L2 ACP 报文；当确定该第二网络设备的设备标识与该 L2 ACP 报文的该目的设备标识相匹配、且该第二网络设备的 IP 地址与该 L2 ACP 报文的该目的 IP 地址相匹配时，解析该 L2 ACP 报文。

可选地，在本发明实施例中，该 L2 ACP 报文的报文头还包括版本字段、协议字段和数据包长度字段。

可选地，在本发明实施例中，该数据链路层地址为介质访问控制 MAC 地址。

可选地，在本发明实施例中，该设备标识为唯一设备标识 UDI 或者安全的唯一设备标识 SUDI。

应理解，根据本发明实施例的网络设备 1400 可对应于本发明实施例的基于数据链路层的通信方法中的第二网络设备，以及可以对应于根据本发明实施例的网络设备 800，并且网络设备 1400 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。

本发明实施例中发送的 L2 ACP 报文是基于数据链路层的帧封装的，可以基于该 L2 ACP 报文的目的数据链路层地址在 ACP 内传输该 L2 ACP 报文，即在本发明实施例中，基于 ACP 的通信，可以不依赖于 IP 协议，相比于现有技术，具有较好的网络兼容性。

此外，在本发明实施例中，设备也无需像现有技术中一样维护路由表，也能够实现基于 ACP 的通信。

还应理解，本文中涉及的第一、第二、第三、第四、第五、第六、第七、第八以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，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

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，而不应对本发明实施例的实施过程构成任何限定。

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。

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时，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。

5

权利要求

1、一种基于数据链路层的通信方法，所述通信方法应用于自组织网络，其特征在于，包括:

网络设备生成邻接发现 AD 消息，所述 AD 消息包括所述网络设备的设备标识;

所述网络设备基于数据链路层的帧封装所述 AD 消息，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中所述源数据链路层地址为所述网络设备的数据链路层地址;

所述网络设备基于所述目的数据链路层地址，向登记 Registrar 设备发送基于所述数据链路层的帧封装后的所述 AD 消息，所述 Registrar 设备为自组织网络中支持分配域证书的设备;

所述网络设备接收所述 Registrar 设备发送的域证书，所述域证书为所述 Registrar 设备根据所述 AD 消息中的所述网络设备的设备标识为所述网络设备分配的;

所述网络设备根据所述域证书，与所述 Registrar 设备建立自组织控制平面 ACP。

2、根据权利要求 1 所述的方法，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

3、根据权利要求 2 所述的方法，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值指示所述 L2 ACP 报文为所述 AD 消息。

4、一种基于数据链路层的通信方法，所述通信方法应用于自组织网络，其特征在于，包括:

登记 Registrar 设备接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，所述 AD 消息包括所述网络设备的设备标识，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中所述源数据链路层地址为所述网络设备的数据链路层地址，所述目的数据链路层地址与所述 Registrar 设备的数据链路层地址相匹配;

当所述 Registrar 设备确定所述网络设备允许加入所述自组织网络时，根

据所述 AD 消息包括的所述设备标识为所述网络设备分配域证书，并向所述网络设备发送所述域证书;

所述 Registrar 设备根据所述域证书，与所述网络设备建立自组织控制平面 ACP。

5、根据权利要求 4 所述的方法，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

6、根据权利要求 4 或 5 所述的方法，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值指示所述 L2 ACP 报文为所述 AD 消息。

7、一种基于数据链路层的通信方法，所述通信方法应用于自组织网络，其特征在于，所述方法包括:

第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，所述第一网络设备为所述自组织网络中的自组织设备;

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，所述源数据链路层地址为所述第一网络设备的数据链路层地址;

所述第一网络设备根据所述目的数据链路层地址，向第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文，所述第二网络设备也为所述自组织网络中的自组织设备，且所述第二网络设备为所述第一网络设备的邻居设备。

8、根据权利要求 7 所述的方法，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是所述 L2 ACP 报文。

9、根据权利要求 7 或 8 所述的方法，其特征在于，所述第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

所述第一网络设备需要与所述自组织网络中的目标设备通信时，当确定所述第一网络设备的邻居列表中包括所述目标设备的设备标识的匹配项时，生成所述 L2 ACP 报文，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为邻居单播报文，所述第一网络

设备的邻居列表包括所述第一网络设备的邻居设备的设备标识与数据链路层地址;

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，包括:

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧的目的数据链路层地址为所述目标设备的数据链路层地址;

所述第一网络设备根据所述目的数据链路层地址，向第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文，包括:

所述第一网络设备根据所述目标设备的数据链路层地址，向所述目标设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

10、根据权利要求 7 或 8 所述的方法，其特征在于，所述第一网络设备生成数据链路层自组织控制平面 L2 ACP 报文，包括:

所述第一网络设备需要与所述自组织网络中的目标设备通信时，当确定所述邻居列表中不包括所述目标设备的设备标识的匹配项时，生成所述 L2 ACP 报文，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为非邻居单播报文;

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，包括:

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

所述第一网络设备根据所述目的数据链路层地址，向第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文，包括:

所述第一网络设备根据所述广播数据链路层地址，向所述第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

11、根据权利要求 7 或 8 所述的方法，其特征在于，所述第一网络设备生成 L2 ACP 报文，包括:

当所述第一网络设备需要在所述 ACP 内广播控制消息时，生成所述 L2 ACP 报文，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为广播报文;

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，包括:

所述第一网络设备基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，所述第一网络设备根据所述目的数据链路层地址，向第二网络设

备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文，包括:

所述第一网络设备根据所述广播数据链路层地址，向所述第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

12、根据权利要求 10 或 11 所述的方法，其特征在于，所述 L2 ACP 报文的报文头还包括用于唯一指示所述 L2 ACP 报文的报文 ID。

13、根据权利要求 10 至 12 中任一项所述的方法，其特征在于，所述 L2 ACP 报文的报文头还包括定时信息，所述定时信息用于指示所述 L2 ACP 报文的接收设备在缓存所述 L2 ACP 报文的时间超过预设时长时，清除所述 L2 ACP 报文。

14、一种基于数据链路层的通信方法，所述通信方法应用于自组织网络，其特征在于，所述方法包括:

第二网络设备接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，所述 L2 ACP 报文包括目的设备标识，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，所述源数据链路层地址为所述第一网络设备的数据链路层地址，所述目的数据链路层地址与所述第二网络设备的数据链路层地址相匹配，所述第二网络设备与所述第一网络设备均为所述自组织网络中的自组织设备;

所述第二网络设备通过判断所述第二网络设备的设备标识是否与所述 L2 ACP 报文的所述目的设备标识相匹配，处理所述 L2 ACP 报文。

15、根据权利要求 14 所述的方法，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是所述 L2 ACP 报文。

16、根据权利要求 14 或 15 所述的方法，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为邻居单播报文，其中，所述数据链路层的帧的目的数据链路层地址为所述目标设备的数据链路层地址;

其中，所述第二网络设备通过判断所述第二网络设备的设备标识是否与所述 L2 ACP 报文的所述目的设备标识相匹配，处理所述 L2 ACP 报文，包括:

所述第二网络设备确定所述目的设备标识为所述第二网络设备的设备标识，并解析所述 L2 ACP 报文。

17、根据权利要求 14 或 15 所述的方法，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为非邻居单播报文，其中，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

其中，所述第二网络设备通过判断所述第二网络设备的设备标识是否与所述 L2 ACP 报文的所述目的设备标识相匹配，处理所述 L2 ACP 报文，包括：

当所述第二网络设备确定所述第二网络设备的设备标识与所述目的设备标识相匹配时，解析所述 L2 ACP 报文，并缓存所述 L2 ACP 报文；

当所述第二网络设备确定所述第二网络设备的设备标识与所述目的设备标识不匹配时，缓存所述 L2 ACP 报文，并根据所述数据链路层的帧的目的数据链路层地址向所述第二网络设备的邻居设备转发基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

18、根据权利要求 14 或 15 所述的方法，其特征在于，所述 L2 ACP 报文的报文头还包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为广播报文，其中，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

其中，所述第二网络设备通过判断所述第二网络设备的设备标识是否与所述 L2 ACP 报文的所述目的设备标识相匹配，处理所述 L2 ACP 报文，包括：

所述第二网络设备确定所述第二网络设备的设备标识与所述目的设备标识相匹配，解析所述 L2 ACP 报文，并缓存所述 L2 ACP 报文，以及根据所述数据链路层的帧的目的数据链路层地址向所述第二网络设备的邻居设备转发基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

19、根据权利要求 17 或 18 所述的方法，其特征在于，所述 L2 ACP 报文的报文头中还包括用于唯一标识所述 L2 ACP 报文的报文 ID，

其中，所述第二网络设备通过判断所述第二网络设备的设备标识是否与所述 L2 ACP 报文的所述目的设备标识相匹配，处理所述 L2 ACP 报文，包括：

当所述第二网络设备确定本地未缓存所述报文 ID 时，通过判断所述第二网络设备的设备标识是否与所述目的设备标识相匹配，处理所述 L2 ACP

报文。

20、根据权利要求 17 至 19 中任一项所述的方法，其特征在于，所述 L2 ACP 报文的报文头中还包括定时信息，所述定时信息用于指示所述 L2 ACP 报文的接收设备在缓存所述 L2 ACP 报文的时间超过预设时长时，清除所述 L2 ACP 报文，

所述方法还包括:

当所述第二网络设备确定缓存所述 L2 ACP 报文的时间超过所述定时信息所指示的预设时长时，清除所述 L2 ACP 报文。

21、一种网络设备，所述网络设备应用于自组织网络，其特征在于，包括:

生成模块，用于网络设备生成邻接发现 AD 消息，所述 AD 消息包括所述网络设备的设备标识;

封装模块，用于基于数据链路层的帧封装所述生成模块生成的所述 AD 消息，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中所述源数据链路层地址为所述网络设备的数据链路层地址;

发送模块，用于基于所述目的数据链路层地址，向 Registrar 设备发送所述封装模块确定的基于所述数据链路层的帧封装后的所述 AD 消息，所述 Registrar 设备为自组织网络中支持分配域证书的设备;

接收模块，用于接收所述 Registrar 设备发送的域证书，所述域证书为所述 Registrar 设备根据所述 AD 消息中的所述网络设备的设备标识为所述网络设备分配的;

建立模块，用于根据所述接收模块接收的所述域证书，与所述 Registrar 设备建立自组织控制平面 ACP。

22、根据权利要求 21 所述的网络设备，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

23、根据权利要求 22 所述的网络设备，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值指示所述 L2 ACP 报文为所述 AD 消息。

24、一种登记 Registrar 设备，所述 Registrar 设备应用于自组织网络，

所述 Registrar 设备为所述自组织网络中支持分配域证书的设备，其特征在于，包括:

接收模块，用于接收来自网络设备的基于数据链路层的帧封装后的邻接发现 AD 消息，所述 AD 消息包括所述网络设备的设备标识，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中所述源数据链路层地址为所述网络设备的数据链路层地址，所述目的数据链路层地址与所述 Registrar 设备的数据链路层地址相匹配;

发送模块，用于当确定所述网络设备允许加入所述自组织网络时，根据所述接收模块接收的所述 AD 消息包括的所述设备标识为所述网络设备分配域证书，并向所述网络设备发送所述域证书;

ACP 建立模块，用于根据所述发送模块发送的所述域证书，与所述网络设备建立自组织控制平面 ACP。

25、根据权利要求 24 所述的 Registrar 设备，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是数据链路层自组织控制平面 L2 ACP 报文。

26、根据权利要求 24 或 25 所述的 Registrar 设备，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值指示所述 L2 ACP 报文为所述 AD 消息。

27、一种网络设备，所述网络设备用作第一网络设备，所述第一网络设备应用于自组织网络，其特征在于，包括:

生成模块，用于生成数据链路层自组织控制平面 L2 ACP 报文，所述第一网络设备为所述自组织网络中的自组织设备;

封装模块，用于基于数据链路层的帧封装所述生成模块生成的所述 L2 ACP 报文，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，所述源数据链路层地址为所述第一网络设备的数据链路层地址;

发送模块，用于根据所述目的数据链路层地址，向第二网络设备发送所述封装模块确定的基于所述数据链路层的帧封装后的所述 L2 ACP 报文，所述第二网络设备也为所述自组织网络中的自组织设备，且所述第二网络设备为所述第一网络设备的邻居设备。

28、根据权利要求 27 所述的第一网络设备，其特征在于，所述数据链

路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是所述 L2 ACP 报文。

29、根据权利要求 27 或 28 所述的第一网络设备，其特征在于，所述生成模块具体用于，需要与所述自组织网络中的目标设备通信时，当确定所述第一网络设备的邻居列表中包括所述目标设备的设备标识的匹配项时，生成所述 L2 ACP 报文，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为邻居单播报文，所述第一网络设备的邻居列表包括所述第一网络设备的邻居设备的设备标识与数据链路层地址；

所述封装模块具体用于，基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧的目的数据链路层地址为所述目标设备的数据链路层地址；

所述发送模块具体用于，根据所述目标设备的数据链路层地址，向所述目标设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

30、根据权利要求 27 或 28 所述的第一网络设备，其特征在于，所述生成模块具体用于，需要与所述自组织网络中的目标设备通信时，当确定所述邻居列表中不包括所述目标设备的设备标识的匹配项时，生成所述 L2 ACP 报文，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为非邻居单播报文；

所述封装模块具体用于，基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

所述发送模块具体用于，根据所述广播数据链路层地址，向所述第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

31、根据权利要求 27 或 28 所述的第一网络设备，其特征在于，所述生成模块具体用于，需要在所述 ACP 内广播控制消息时，生成所述 L2 ACP 报文，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为广播报文；

所述封装模块具体用于，基于数据链路层的帧封装所述 L2 ACP 报文，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址；

其中，所述发送模块具体用于，根据所述广播数据链路层地址，向所述

第二网络设备发送基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

32、根据权利要求 30 或 31 所述的第一网络设备，其特征在于，所述 L2 ACP 报文的报文头还包括用于唯一指示所述 L2 ACP 报文的报文 ID。

33、根据权利要求 30 至 32 中任一项所述的第一网络设备，其特征在于，所述 L2 ACP 报文的报文头还包括定时信息，所述定时信息用于指示所述 L2 ACP 报文的接收设备在缓存所述 L2 ACP 报文的时间超过预设时长时，清除所述 L2 ACP 报文。

34、一种网络设备，所述网络设备用作第二网络设备，所述第二网络设备应用于自组织网络，其特征在于，所述第二网络设备包括:

接收模块，用于接收第一网络设备发送的基于数据链路层的帧封装后的 L2 ACP 报文，所述 L2 ACP 报文包括目的设备标识，所述数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，所述源数据链路层地址为所述第一网络设备的数据链路层地址，所述目的数据链路层地址与所述第二网络设备的数据链路层地址相匹配，所述第二网络设备与所述第一网络设备均为所述自组织网络中的自组织设备;

处理模块，用于通过判断所述第二网络设备的设备标识是否与所述 L2 ACP 报文的所述目的设备标识相匹配，处理所述接收模块接收的所述 L2 ACP 报文。

35、根据权利要求 34 所述的第二网络设备，其特征在于，所述数据链路层的帧为符合以太网协议定义的帧，所述数据链路层的帧的类型 Type 字段的 Type 值指示所述数据链路层的帧的数据载荷字段承载的是所述 L2 ACP 报文。

36、根据权利要求 34 或 35 所述的第二网络设备，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为邻居单播报文，其中，所述数据链路层的帧的目的数据链路层地址为所述目标设备的数据链路层地址;

其中，所述处理模块具体用于，确定所述目的设备标识为所述第二网络设备的设备标识，并解析所述 L2 ACP 报文。

37、根据权利要求 34 或 35 所述的第二网络设备，其特征在于，所述 L2 ACP 报文的报文头包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为非邻居单播报文，其中，所述数据链路层的帧的目的数据链

路层地址为广播数据链路层地址;

其中，所述处理模块具体用于，当确定所述第二网络设备的设备标识与所述目的设备标识相匹配时，解析所述 L2 ACP 报文，并缓存所述 L2 ACP 报文;

处理模块具体用于，当确定所述第二网络设备的设备标识与所述目的设备标识不匹配时，缓存所述 L2 ACP 报文，并根据所述数据链路层的帧的目的数据链路层地址向所述第二网络设备的邻居设备转发基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

38、根据权利要求 34 或 35 所述的第二网络设备，其特征在于，所述 L2 ACP 报文的报文头还包括标志位字段，所述标志位字段的值用于指示所述 L2 ACP 报文为广播报文，其中，所述数据链路层的帧的目的数据链路层地址为广播数据链路层地址;

其中，所述处理模块具体用于，确定所述第二网络设备的设备标识与所述目的设备标识相匹配，解析所述 L2 ACP 报文，并缓存所述 L2 ACP 报文，以及根据所述数据链路层的帧的目的数据链路层地址向所述第二网络设备的邻居设备转发基于所述数据链路层的帧封装后的所述 L2 ACP 报文。

39、根据权利要求 37 或 38 所述的第二网络设备，其特征在于，所述 L2 ACP 报文的报文头中还包括用于唯一标识所述 L2 ACP 报文的报文 ID，

其中，所述处理模块具体用于，当确定本地未缓存所述报文 ID 时，通过判断所述第二网络设备的设备标识是否与所述目的设备标识相匹配，处理所述 L2 ACP 报文。

40、根据权利要求 37 至 39 中任一项所述的第二网络设备，其特征在于，所述 L2 ACP 报文的报文头中还包括定时信息，所述定时信息用于指示所述 L2 ACP 报文的接收设备在缓存所述 L2 ACP 报文的时间超过预设时长时，清除所述 L2 ACP 报文，

所述第二网络设备还包括:

缓存清除模块，用于当确定缓存所述 L2 ACP 报文的时间超过所述定时信息所指示的预设时长时，清除所述 L2 ACP 报文。

41、一种基于自组织网络的系统，其特征在于，包括如上述权利要求 21 至 23 中任一项所述的网络设备与上述权利要求 24 至 26 中任一项所述的 Registrar 设备。

42、一种基于自组织网络的系统，其特征在于，包括如上述权利要求 27 至 33 中任一项所述的网络设备与上述权利要求 34 至 40 中任一项所述的网络设备。

5


100
网络设备生成邻接发现AD消息，该AD消息包括该网络设备的设备标识
S110
该网络设备基于数据链路层的帧封装该AD消息，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址
S120
该网络设备基于该目的数据链路层地址，向Registrar设备发送基于该数据链路层的帧封装后的该AD消息，该Registrar设备为自组织网络中支持分配域证书的设备
S130
该网络设备接收该Registrar设备发送的域证书，该域证书为该Registrar设备根据该AD消息中的该网络设备的设备标识为该网络设备分配的
S140
该网络节点根据该域证书，与该Registrar节点建立自组织控制平面ACP
S150

图 1

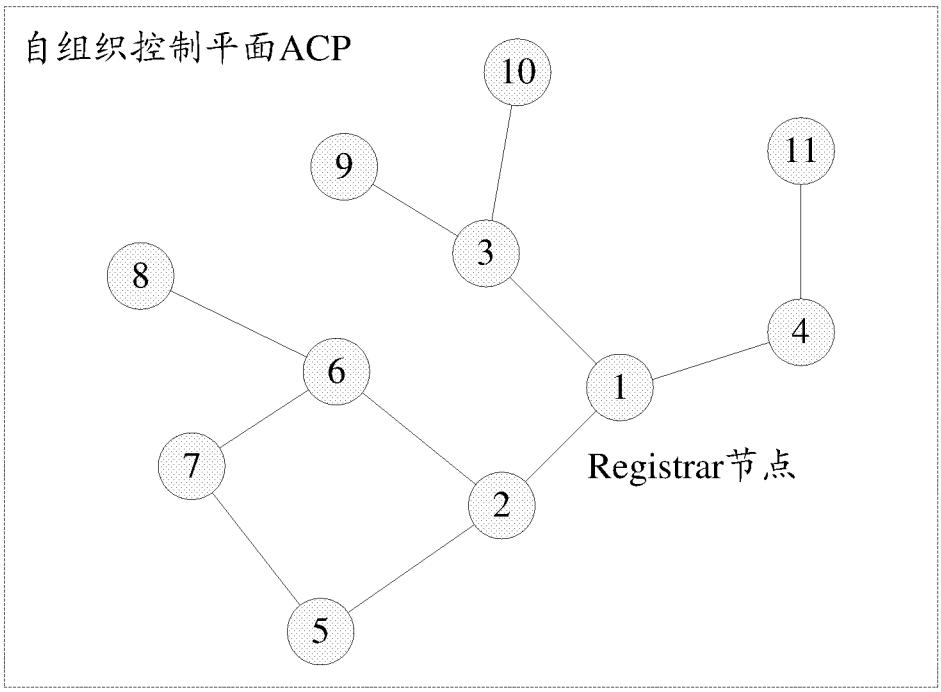
自组织控制平面ACP
10
9
11
3
8
4
6
1
7
Registrar节点
2
5

图 2

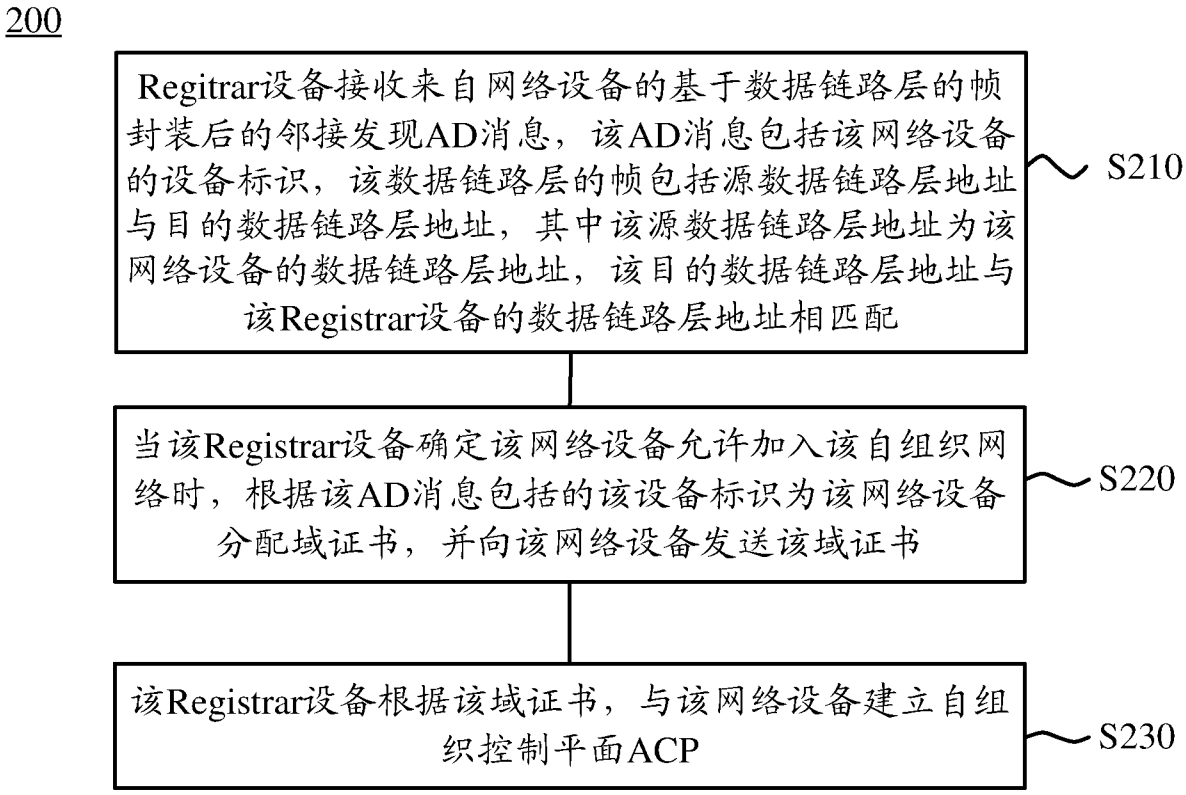
200
Regitrar设备接收来自网络设备的基于数据链路层的帧封装后的邻接发现AD消息，该AD消息包括该网络设备的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中该源数据链路层地址为该网络设备的数据链路层地址，该目的数据链路层地址与该Registrar设备的数据链路层地址相匹配
S210
当该Registrar设备确定该网络设备允许加入该自组织网络时，根据该AD消息包括的该设备标识为该网络设备分配域证书，并向该网络设备发送该域证书
S220
该Registrar设备根据该域证书，与该网络设备建立自组织控制平面ACP
S230

图 3

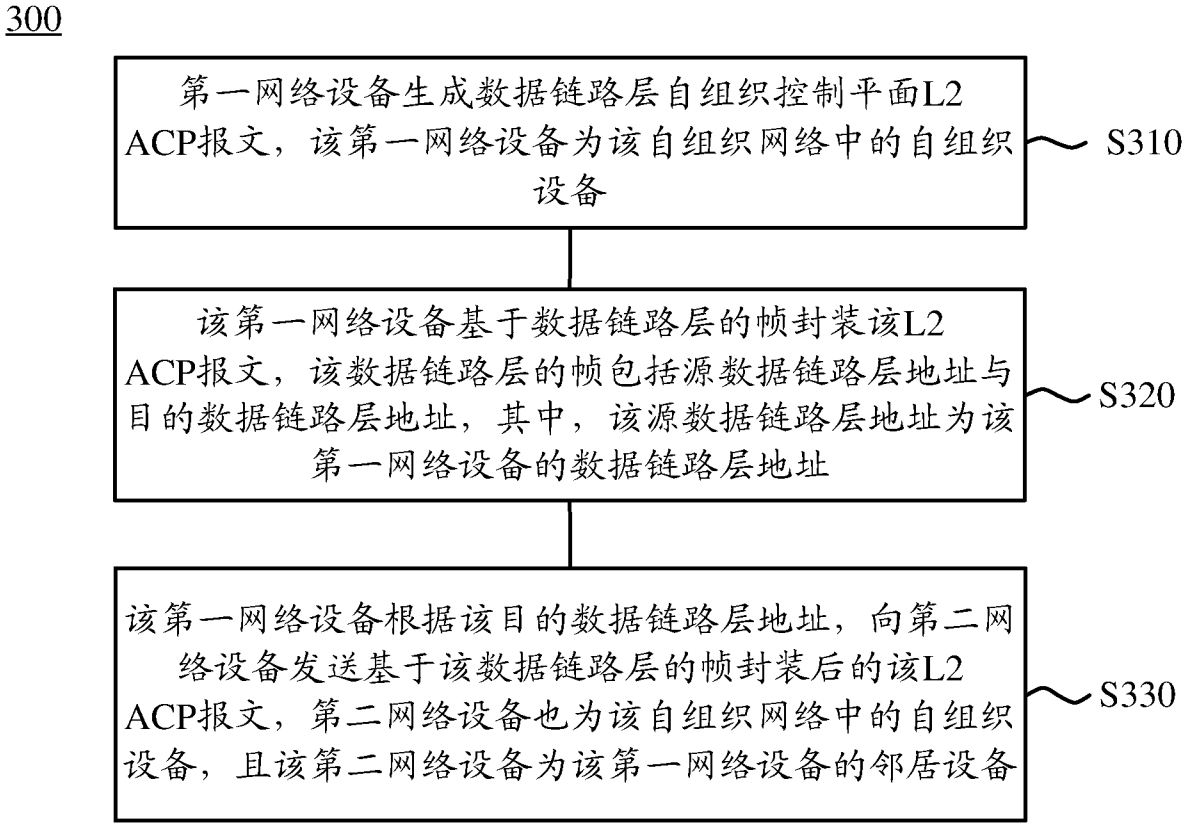
300
第一网络设备生成数据链路层自组织控制平面L2 ACP报文，该第一网络设备为该自组织网络中的自组织设备
S310
该第一网络设备基于数据链路层的帧封装该L2 ACP报文，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址
S320
该第一网络设备根据该目的数据链路层地址，向第二网络设备发送基于该数据链路层的帧封装后的该L2 ACP报文，第二网络设备也为该自组织网络中的自组织设备，且该第二网络设备为该第一网络设备的邻居设备
S330

图 4

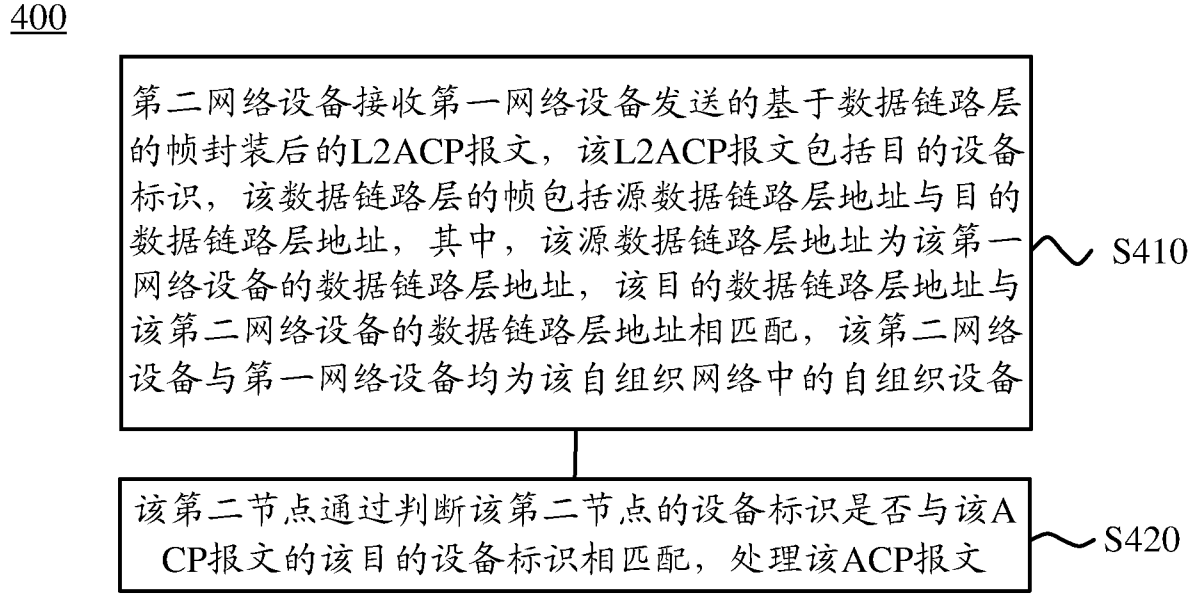
400
第二网络设备接收第一网络设备发送的基于数据链路层的帧封装后的L2ACP报文，该L2ACP报文包括目的设备标识，该数据链路层的帧包括源数据链路层地址与目的数据链路层地址，其中，该源数据链路层地址为该第一网络设备的数据链路层地址，该目的数据链路层地址与该第二网络设备的数据链路层地址相匹配，该第二网络设备与第一网络设备均为该自组织网络中的自组织设备
S410
该第二节点通过判断该第二节点的设备标识是否与该ACP报文的该目的设备标识相匹配，处理该ACP报文
S420

图 5

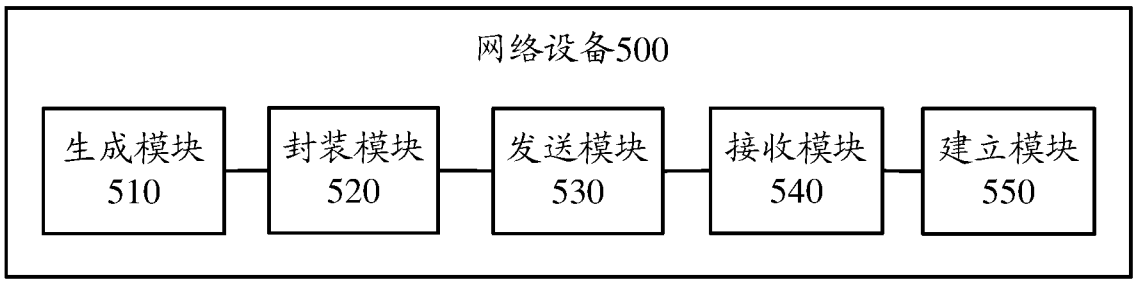
网络设备500
生成模块510
封装模块520
发送模块530
接收模块540
建立模块550

图 6

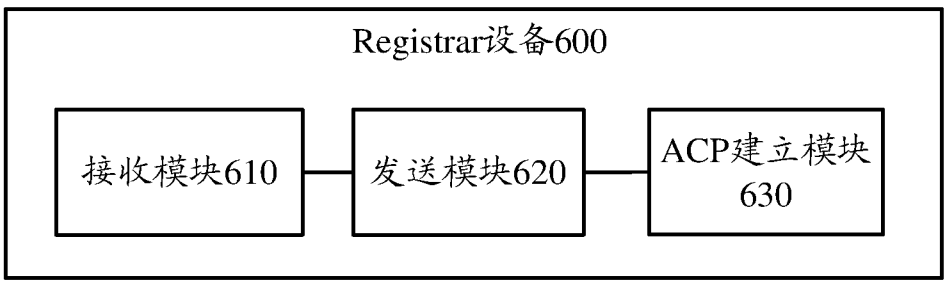
Registrar设备600
接收模块610
发送模块620
ACP建立模块630

图 7

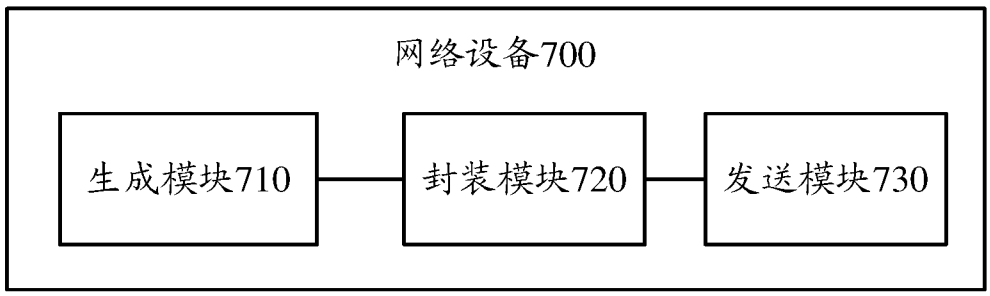
网络设备700
生成模块710
封装模块720
发送模块730

图 8

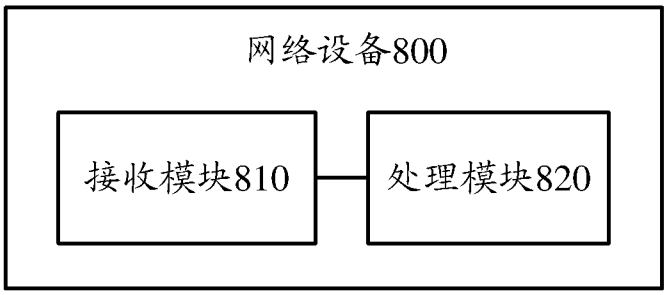

图 9

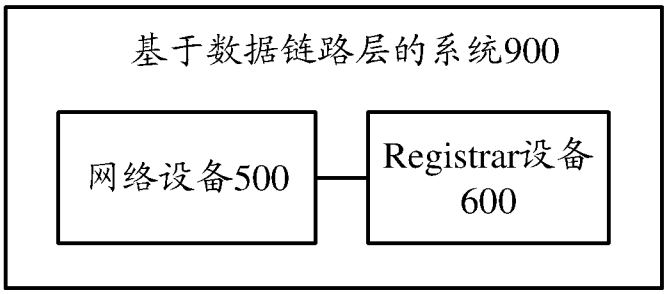

图 10

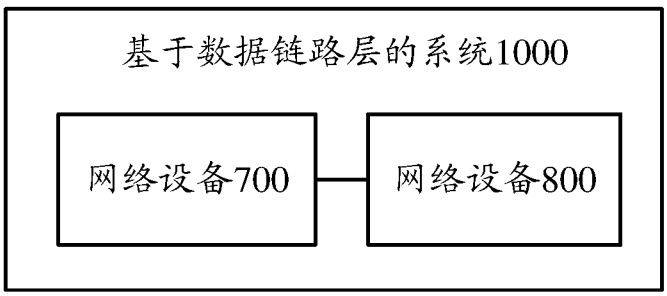

图 11

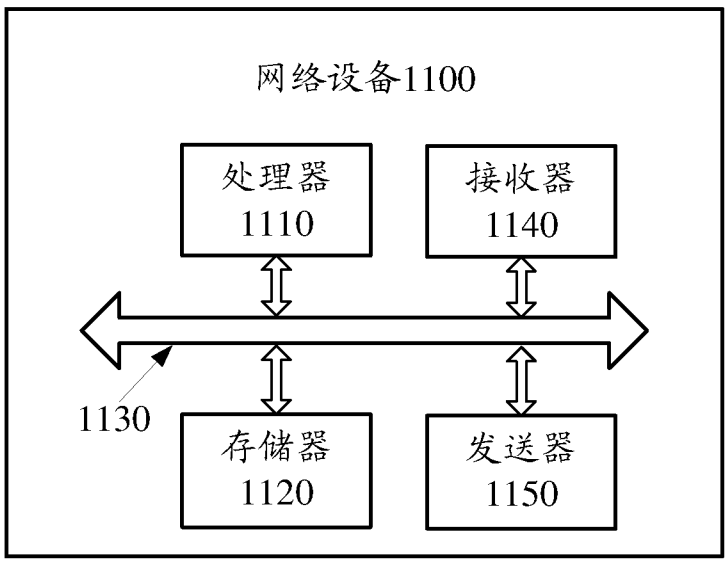

图 12

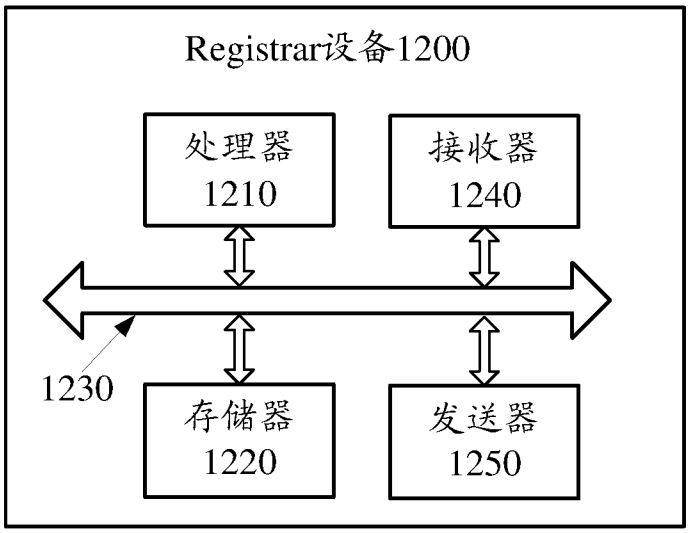
Registrar设备1200
处理器
1210
接收器
1240
1230
存储器
1220
发送器
1250

图 13

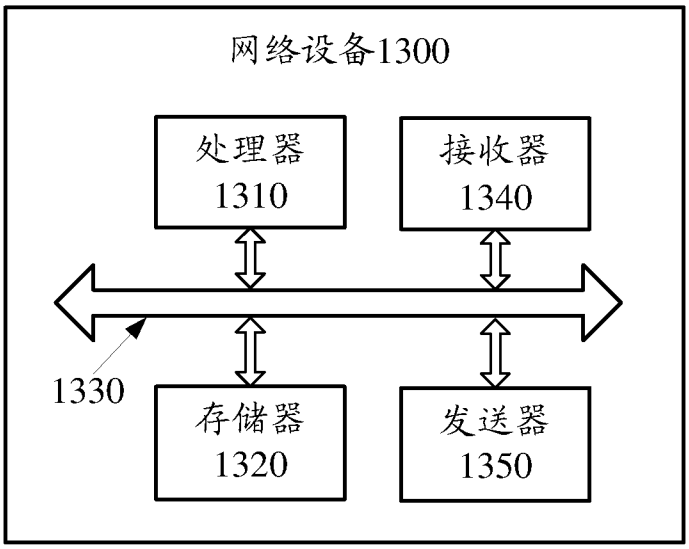
网络设备1300
处理器
1310
接收器
1340
1330
存储器
1320
发送器
1350

图 14

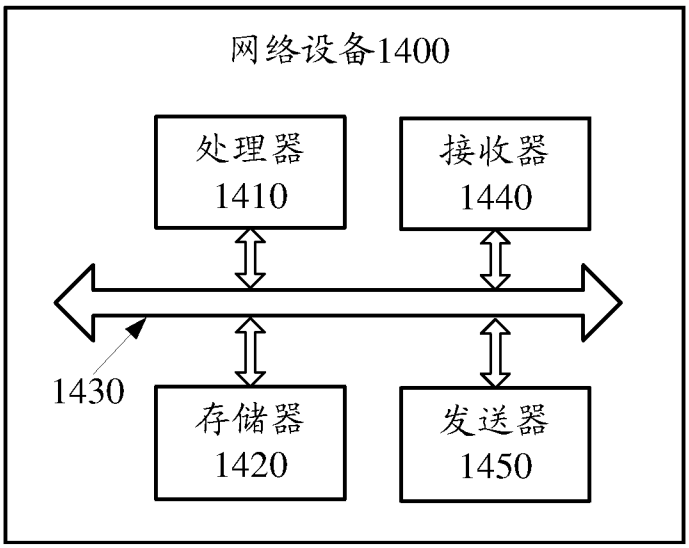
网络设备1400
处理器
1410
接收器
1440
1430
存储器
1420
发送器
1450

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/084772

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (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)

CNPAT, CNKI, EPODOC, WPI, IEEE: self-organization, new node, adjacent information, link layer, AN, new, join, certificate, domain, cluster, group, link, encapsulat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2013177069 A1 (CISCO TECHNOLOGY, INC.), 28 November 2013 (28.11.2013), description, paragraphs [0062]-[0067] and [0087]-[0090], and figure 4	1-42
A	CN 1897518 A (HUAWEI TECHNOLOGIES CO., LTD. et al.), 17 January 2007 (17.01.2007), the whole document	1-42
A	CN 101192928 A (HUAWEI TECHNOLOGIES CO., LTD. et al.), 04 June 2008 (04.06.2008), the whole document	1-42
A	CN 102148756 A (WUHAN RESEARCH INSTITUTE OF POSTS AND TELECOMMUNICATIONS), 10 August 2011 (10.08.2011), the whole document	1-42

☐ 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
18 March 2016 (18.03.2016)	**31 March 2016 (31.03.2016)**
Name and mailing address of the ISA/CN: 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 **ZHANG, Cuiling** Telephone No.: (86-10) **62413373**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/084772

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2013177069 A1	28 November 2013	US 2015280916 A1	01 October 2015
		US 2013318343 A1	28 November 2013
CN 1897518 A	17 January 2007	None	
CN 101192928 A	04 June 2008	None	
CN 102148756 A	10 August 2011	None	

国际检索报告

国际申请号
PCT/CN2015/084772

A. 主题的分类

H04L 12/24(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）)

CNPAT, CNKI, EPODOC, WPI, IEEE: 自组织, 新节点, 加入, 邻接消息, 证书, 域, 簇, 组, 链路层, 封装, AN, new, join, certificate, domain, cluster, group, link, encapsulat+

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	WO 2013177069 A1 (CISCO TECHNOLOGY, INC.) 2013年 11月 28日 (2013-11-28) 说明书第[0062]-[0067]，[0087]-[0090]段，附图4	1-42
A	CN 1897518 A (华为技术有限公司 等) 2007年 1月 17日 (2007-01-17) 全文	1-42
A	CN 101192928 A (华为技术有限公司 等) 2008年 6月 4日 (2008-06-04) 全文	1-42
A	CN 102148756 A (武汉邮电科学研究院) 2011年 8月 10日 (2011-08-10) 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	国际检索报告邮寄日期
2016年 3月 18日	2016年 3月 31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 张翠玲 电话号码 (86-10)62413373

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/084772

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)
WO 2013177069 A1	2013年 11月 28日	US 2015280916 A1	2015年 10月 1日
		US 2013318343 A1	2013年 11月 28日
CN 1897518 A	2007年 1月 17日	无	
CN 101192928 A	2008年 6月 4日	无	
CN 102148756 A	2011年 8月 10日	无	