

# (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)



(10) 国际公布号  
WO 2017/011948 A1

- (51) 国际专利分类号:  
H04L 12/70 (2013.01) H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2015/084384
- (22) 国际申请日: 2015 年 7 月 17 日 (17.07.2015)
- (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)。

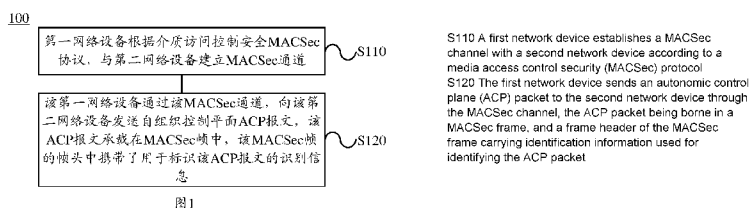
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, 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: PACKET TRANSMISSION METHOD, APPARATUS AND SYSTEM

(54) 发明名称: 报文传输的方法、装置和系统



(57) Abstract: Embodiments of the present invention relate to a packet transmission method, apparatus and system. The method comprises: a first network device establishes a MACSec channel with a second network device according to a MACSec protocol; and the first network device sends an ACP packet to the second network device through the MACSec channel, the ACP packet being borne in a MACSec frame, and a frame header of the MACSec frame carrying identification information used for identifying the ACP packet. In the packet transmission method, apparatus and system in the embodiments of the present invention, a MACSec channel is established between adjacent nodes in a self-organizing network according to a MACSec protocol, and an ACP packet is transmitted and processed between the adjacent nodes through the MACSec channel, so that a routable interface address and a local address used for establishing an IPsec link do not need to be configured on an interface at the same time, and a MACSec security mechanism provided for an ACP does not need to use an L3 tunnel, thereby improving the efficiency.

(57) 摘要: 本发明实施例涉及报文传输的方法、装置和系统。该方法包括第一网络设备根据 MACSec 协议, 与第二网络设备建立 MACSec 通道; 该第一网络设备通过该 MACSec 通道, 向该第二网络设备发送 ACP 报文, 该 ACP 报文承载在 MACSec 帧中, 该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息。本发明实施例的报文传输的方法、装置和系统, 根据 MACSec 协议, 自组织网络中的相邻节点之间建立 MACSec 通道, 通过该 MACSec 通道, 相邻节点之间传输并处理 ACP 报文, 从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址, 为 ACP 提供的 MACSec 安全机制, 不需要使用 L3 隧道, 进而提高了效率。

WO 2017/011948 A1

## 报文传输的方法、装置和系统

## 技术领域

本发明涉及信息技术领域，尤其涉及报文传输的方法、装置和系统。

5

## 背景技术

自组织网络支持自我管理，可以减少管理员的干预，提升网络的自动化程度，从而减轻网络管理的工作，方便新业务的部署，减少配置失误概率，降低运营费用（Operating Expense，简称“OPEX”）。

10

自组织网络的一个重要的方面是设备可以“即插即用”，支持自举，自配置，其中的一个关键技术是自动控制平面（Autonomic Control Plane，简称“ACP”）的建立，它的特点是无需管理员参与，这个控制平面自动产生，自动生长（新设备自动加入）；端到端的连接建立完全“零接触（zero-touch）”，而且 ACP 不受管理员的错误配置的影响，实现信息安全交互。

15

现有方案中 ACP 的建立依赖于 IPv6，而现网中大部分设备支持 IPv4，开发基于 IPv4 的 ACP 将拥有更好的现网兼容性，可以减少部署障碍。如果考虑采用类似于 IPv6 的链路本地地址（link-local-IP）（169.254.0.0/16）来建立安全隧道，基于 IPv4 建立具有 IPSec 通道的 ACP 时，需要使用 IPv4 链路本地地址，但是与 IPv6 不同的是，请求注解 RFC（Request For Comments）3927 建议仅在没有可路由的 IPv4 接口地址时才使用 IPv4 链路本地地址，因此通常此时没有对应于 IPv6 中的 link-local-IP 的三层隧道可用，无法建立基于 IPv4 的具有 IPSec 通道的 ACP。

20

## 发明内容

25

本发明提供了一种报文传输的方法、装置和系统，能够提高效率。

第一方面，提供了一种报文传输的方法，应用在自组织网络中，该方法包括：第一网络设备根据介质访问控制安全 MACSec 协议，与第二网络设备建立 MACSec 通道；该第一网络设备通过该 MACSec 通道，向该第二网络设备发送自组织控制平面 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息。

30

结合第一方面，在第一方面的一种实现方式中，该识别信息携带在该

MACSec 帧的帧头中的以太网类型字段中, 该以太网类型字段用于指示该 MACSec 帧用于承载该 ACP 报文。

结合第一方面及其上述实现方式, 在第一方面的另一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的标志位字段中, 该标识位字段为新增字段或版本字段。

结合第一方面及其上述实现方式, 在第一方面的另一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的 MAC 地址字段中。

第二方面, 提供了一种报文传输的方法, 应用在自组织网络中, 该方法包括: 第二网络设备根据介质访问控制安全 MACSec 协议, 与第一网络设备建立 MACSec 通道; 该第二网络设备通过该 MACSec 通道, 接收该第一网络设备发送的 MACSec 帧; 该第二网络设备根据该 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息, 确定该 ACP 报文。

结合第二方面, 在第二方面的一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的以太网类型字段中, 该以太网类型字段用于指示该 MACSec 帧用于承载该 ACP 报文。

结合第二方面及其上述实现方式, 在第二方面的另一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的标志位字段中, 该标识位字段为新增字段或版本字段。

结合第二方面及其上述实现方式, 在第二方面的另一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的 MAC 地址字段中。

第三方面, 提供了一种用于报文传输的第一网络设备, 应用在自组织网络中, 该第一网络设备包括: 建立模块, 用于该第一网络设备根据介质访问控制安全 MACSec 协议, 与第二网络设备建立 MACSec 通道; 发送模块, 用于该第一网络设备通过该建立模块建立的该 MACSec 通道, 向该第二网络设备发送自组织控制平面 ACP 报文, 该 ACP 报文承载在 MACSec 帧中, 该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息。

结合第三方面, 在第三方面的一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的以太网类型字段中, 该以太网类型字段用于指示该 MACSec 帧用于承载该 ACP 报文。

结合第三方面及其上述实现方式, 在第三方面的另一种实现方式中, 该识别信息携带在该 MACSec 帧的帧头中的标志位字段中, 该标识位字段为新增

增字段或版本字段。

结合第三方面及其上述实现方式，在第三方面的另一种实现方式中，该识别信息携带在该 MACSec 帧的帧头中的 MAC 地址字段中。

5 第四方面，提供了一种用于报文传输的第二网络设备，应用在自组织网络中，该第二网络设备包括：建立模块，用于该第二网络设备根据介质访问控制安全 MACSec 协议，与第一网络设备建立 MACSec 通道；接收模块，用于该第二网络设备通过该建立模块建立的该 MACSec 通道，接收该第一网络设备发送的 MACSec 帧；确定模块，用于该第二网络设备根据该接收模块接收的该 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的  
10 识别信息，确定该 ACP 报文。

结合第四方面，在第四方面的一种实现方式中，该识别信息携带在该 MACSec 帧的帧头中的以太网类型字段中，该以太网类型字段用于指示该 MACSec 帧用于承载该 ACP 报文。

结合第四方面及其上述实现方式，在第四方面的另一种实现方式中，该  
15 识别信息携带在该 MACSec 帧的帧头中的标志位字段中，该标志位字段为新增字段或版本字段。

结合第四方面及其上述实现方式，在第四方面的另一种实现方式中，该识别信息携带在该 MACSec 帧的帧头中的 MAC 地址字段中。

20 第五方面，提供了一种用于报文传输的系统，应用在自组织网络中，该系统包括：上述的第一网络设备和第二网络设备，该第一网络设备根据介质访问控制安全 MACSec 协议，与该第二网络设备建立 MACSec 通道；通过该 MACSec 通道，该第一网络设备向该第二网络设备发送自组织控制平面 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息；该第二网络设备接收该 MACSec 帧；  
25 该第二网络设备根据该 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息，确定该 ACP 报文。

基于上述技术方案，本发明实施例的报文传输的方法、装置和系统，根据 MACSec 协议，自组织网络中的第一网络设备和第二网络设备之间建立 MACSec 通道，通过该 MACSec 通道，第一网络设备与第二网络设备之间可  
30 以传输 MACSec 帧，该 MACSec 帧的帧头中携带了识别信息，可以根据该识别信息表示 ACP 报文，从而不需要在接口上同时配置可路由的接口地址

和用于建立 IPSec 的链路本地地址，而是根据 MACSec 协议，为 ACP 提供 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过识别信息区分 MACSec 帧中的 ACP 报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

5

#### 附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中所需要使用的附图作简单地介绍，显而易见地，下面所描述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的前提下，还可以根据这些附图获得其他的附图。

10

图 1 是根据本发明实施例的报文传输的方法的示意性流程图。

图 2 是根据本发明实施例的报文传输的方法中 MACSec 帧结构的示意图。

15

图 3 是根据本发明实施例的报文传输的方法中另一 MACSec 帧结构的示意图。

图 4 是根据本发明实施例的报文传输的方法中再一 MACSec 帧结构的示意图。

图 5 是根据本发明另一实施例的报文传输的方法的示意性流程图。

20

图 6 是根据本发明实施例的用于报文传输的第一网络设备的示意性框图。

图 7 是根据本发明实施例的用于报文传输的第二网络设备的示意性框图。

图 8 是根据本发明实施例的用于报文传输的系统的示意性框图。

25

图 9 是根据本发明另一实施例的用于报文传输的第一网络设备的示意性框图。

图 10 是根据本发明另一实施例的自用于报文传输的第二网络设备的示意性框图。

#### 具体实施方式

30

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的一部分实施例，而不

是全部实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都应属于本发明保护的范围。

图 1 示出了根据本发明实施例的报文传输的方法 100 的示意性流程图，该方法 100 可以应用于自组织网络中，由自组织网络中的第一网络设备执行，该第一网络设备可以为发送节点。如图 1 所示，该方法 100 包括：

S110，第一网络设备根据介质访问控制安全 MACSec 协议，与第二网络设备建立 MACSec 通道；

S120，该第一网络设备通过该 MACSec 通道，向该第二网络设备发送自组织控制平面 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息。

具体地，在自组织网络中，可以将一个节点设置为认证（Registrar）节点，该 Registrar 节点配置了自组织节点的唯一设备标识（Unique Device Identification，简称“UDI”）白名单，该 UDI 白名单内的节点可以加入该自组织域，并且 Registrar 节点本身连接到 domain CA（自组织域数字证书认证机构），支持分配域证书（domain certificate）。网络中各个节点发起邻居发现（AD）消息，通过该 AD 消息寻找邻居节点，该 AD 消息中包括 UDI 或域证书。根据该 AD 消息，各个节点可以创建邻居列表；Registrar 节点收到该 AD 消息后，对比 UDI 白名单，向属于 UDI 白名单的该邻居节点发送域证书。基于该域证书，邻居节点与 Registrar 节点相互认证，并在认证成功后基于认证过程中生成的密钥协商出报文加密密钥，根据介质访问控制安全（Media Access Control Security，简称“MACSec”）协议，建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地，针对 Registrar 节点的邻居节点的邻居节点，需要 Registrar 节点的邻居节点作为代理服务器（Proxy）以及认证点，其它步骤一致，从而建立自组织网络中相邻节点之间的 MACSec 通道，使得属于同一域的多个节点构成一个 ACP。在该 ACP 内，各个节点之间可以通过 MACSec 通道，互相传输根据 MACSec 协议封装的 ACP 报文。

因此，本发明实施例的报文传输的方法，根据 MACSec 协议，自组织网络中的第一网络设备与第二网络设备之间建立 MACSec 通道，通过该 MACSec 通道，第一网络设备向第二网络设备发送 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息，从而不需要在接口上同时配置可路由的接口地址和用于建立

IPSec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

5        在本发明实施例中，自组织网络中各个节点支持自组织特性，每个节点都有自己的 UDI 或者设备 ID 证书（IDevID certificate），可选地，这里以各个节点通过 UDI 获取域证书为例进行说明，但本发明并不限于此。在该网络中，设置其中一个节点为认证（Registrar）节点，该 Registrar 节点支持分配域证书，并且配置了自组织节点的 UDI 白名单，该 UDI 白名单内的节点属于同一个自组织域。可选地，可以预配置该 Registrar 节点，Registrar 节点能够支持分配域证书的节点，即该 Registrar 节点与数字证书认证管理机构有连接，可以进行通信，换句话说，该 Registrar 节点能够通过数字证书认证管理结构为其他节点分配域证书。

10

在本发明实施例中，自组织特性使能后，自组织节点可以向邻居节点发送 AD 消息，从而寻找自己的邻居节点。可选地，各个节点可以每隔一段时间，例如 10s，发起一次 AD 消息。该 AD 消息可以包括 UDI 或者域证书，例如，对于 Registrar 节点发送的 AD 消息，Registrar 节点支持分配域证书，它会先给自己配置一个域证书，Registrar 节点发送的该 AD 消息中可以包括域证书；而对于没有域证书的节点发送的 AD 消息，该 AD 消息中可以包括 UDI。

15

20

在本发明实施例中，由于自组织节点发送的 AD 消息只能发送一跳的距离，即只有邻居节点可以收到该 AD 消息，因此当节点收到邻居节点发送的 AD 消息后，可以建立一个邻居列表，用于记录属于该节点的邻居节点。可选地，该邻居列表可以包括邻居节点的 UDI，该 UDI 通过邻居节点发送的 AD 消息获得，邻居列表还可以包括地址信息，该地址信息可以为 IPv6 地址，或 IPv4 地址，或介质访问控制（Media Access Control，简称“MAC”）地址，该地址信息可以通过发送的 AD 消息的报文确定，但本发明并不限于此。根据节点确定的邻居节点列表，可以确定各个节点的邻居节点的 UDI 以及地址信息。

25

30        在本发明实施例中，当 Registrar 节点收到邻居节点发送的 AD 消息后，将 AD 消息中的 UDI 对比 Registrar 节点中的 UDI 白名单，如果邻居节点的

UDI 匹配 UDI 白名单, 则 Registrar 节点根据该 UDI 生成一个域证书, 将该域证书发送给该邻居节点, 后续 AD 广播中将使用该域证书。此时, 具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

5 在本发明实施例中, 对于 Registrar 节点接收到的邻居节点发送的 AD 消息, 可以为该邻居节点的 AD 消息, 也可以为该邻居节点转发自己的邻居节点的 AD 消息, 并比照 UDI 白名单, 对于属于同一个域, 的节点, Registrar 节点均发送域证书, 可选地, 可以通过邻居节点互相转发, 具有该域证书的节点均属于同一个域, 该自组织网络中的这些节点属于同一个 ACP。

10 在本发明实施例中, 当自组织网络中每个节点有自己的 IDevID certificate 时, 则节点向邻居节点发送的 AD 消息包括域证书或 SUDI, 其中, Registrar 节点的 AD 消息可以包括域证书, 而没有域证书的节点的 AD 消息中包括 SUDI。邻居节点将自己的 802.1AR 证书发给 Registrar 节点, 可选地, 可以经过一个 Proxy。收到该消息的 Registrar 节点使用公钥验证该证书, 并且连接到验证服务器验证该设备是否可以接入域。如果验证成功, Registrar 节点根据该 SUDI 生成一个域证书, 发给对应的邻居节点, 该邻居节点接收到域证书, 后续 AD 广播中将使用域证书。同样地, Registrar 节点的邻居节点的邻居节点同样可以通过该方法获得域证书, 具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

20 在 S110 中, 根据介质访问控制安全 MACSec 协议, 自组织网络中的第一网络设备和第二网络设备可以建立 MACSec 通道, 其中, 该第一网络设备和第二网络设备可以为该自组织网络中的任意两个节点, 可选地, 该第一网络设备和第二网络设备可以为相邻的两个节点。具体地, 基于域证书, 获得域证书的邻居节点可以与 Registrar 节点相互认证, 并在认证成功后基于认证过程中生成的密钥协商出报文加密密钥, 根据 MACSec 协议, 建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地, 对于 Registrar 节点的邻居节点的邻居节点, 可以将 Registrar 节点的邻居节点作为代理服务器 (Proxy) 以及认证点, 其它步骤一致, 从而建立属于同一个域的各个节点中相邻节点之间的 MACSec 通道。这样, 对于该 ACP 中的任意两个节点, 即第一网络设备和第二网络设备之间可以通过该 MACSec 通道进行报文传输。

30 具体地, 获得 Registrar 节点发送的域证书的邻居节点, 可以向 Registrar 节点发起认证, 例如可以发起基于 802.1X 的认证, Registrar 节点可以作为

认证者 (Authenticator) 和认证服务器, 实现 Registrar 节点和邻居节点之间的相互认证, 例如, 可以选择 EAP-TLS (Extensible Authentication Protocol, 扩展的认证协议) (Transport Layer Security Protocol, 安全传输层协议) 的认证方式, 遵守 802.1af 的标准。

5        在本发明实施例中, Registrar 节点与邻居节点认证成功后, 基于认证过程中生成的密钥协商出报文加密密钥, 建立起 ACP 专用的安全 MACSec 通道。具体地, 按照 MACSec 密钥协议 (MACsec Key Agreement, 简称“MKA”), 将之前的 Registrar 节点与邻居节点认证中生成的成对主密钥 (pairwise master key, 简称“PMK”) 作为连通性关联密钥 (Connectivity Association Key, 简称“CAK”)。Registrar 节点作为 Authenticator, 默认被选择为 MKA 10        协议中的密钥服务器 (key server), 可以按照 802.1X 协议, 根据 CAK, 随机数等产生一个安全关联密钥 (secure association key, 简称“SAK”), 加密后发给邻居节点, 以便于在后续的通信中, 启用这个 SAK 作以太帧的加密和签名。

15        在本发明实施例中, Registrar 节点与邻居节点通过上述方法建立 MACSec 通道后, 对于 Registrar 节点的邻居节点的邻居节点加入该 ACP 时, Registrar 节点的邻居节点可以作为代理服务器 (Proxy) 以及认证点, 同样通过上述方法获得域证书, 进而加入该 ACP, 并通过验证, 建立与邻居节点之间的 MACSec 通道。

20        在 S120 中, 在自组织网络中的 ACP 内, 第一网络设备可以通过建立的 MACSec 通道向第二网络设备发送 ACP 报文, 具体地, 自组织网络中任意一个节点可以通过 MACSec 通道向邻居节点发送 ACP 报文, 经过至少一次转发, 自组织网络中的任意两个节点, 第一网络设备和第二网络设备之间可以传输 ACP 报文。由于在 MAC 层, 还可以通过 MACSec 通道传输其它报 25        文, 因此, 具体地, 可以在 MACSec 帧的帧头中携带识别信息, 可以通过该识别信息区分该 MACSec 帧是否承载 ACP 报文, 可选地, 可以通过下面几种方法确定根据 MACSec 协议封装的报文中的 ACP 报文以及其它报文。

30        可选地, 作为一个实施例, 以邻居节点之间传输报文为例, 当节点向邻居节点发送 MACSec 协议封装的 MACSec 帧时, 该 MACSec 帧的帧头中可以携带识别信息, 该识别信息用于指示该帧结构用于承载 ACP 报文。具体地, 若整个自组织网络不启用数据面的 MACSec 时, 则根据 MACSec 协议

封装的报文即为 ACP 报文，而其它报文可以通过 MAC 封装，该报文解封装后，由 Global 路由处理。例如，整个自组织网络不启用数据面的 MACSec 时，节点向邻居节点发送的 802.1ae 格式封装的报文即为根据 MACSec 协议封装的报文，该报文即可被理解为 ACP 报文。具体地，如图 2 所示，802.1ae 格式封装的 MACSec 帧，该 MACSec 帧的帧头可以包括如图 2 所示的几种字段，其中，该 802.1AE 头（802.1AE Header）字段可以为识别信息，表示该帧结构为根据 MACSec 协议封装的报文，则该 MACSec 帧用于承载 ACP 报文，相反的，如果不包括该 802.1AE Header 字段，则可以确定该帧结构为其它的普通报文。

10 可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点向邻居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以携带识别信息，该识别信息用于指示该帧结构用于承载 ACP 报文，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的以太网类型字段中。具体地，传输的报文中可以包括以太网类型（Ethertype）字段，例如，如图 2 所示，该以太网类型字段可以位于 802.1AE Header 字段中，具体地，如图 3 所示，该 802.1AE Header 字段可以包括 MACSec Ethertype 字段、TCI（TAG control information，标签控制信息）字段、AN（Association Number）字段、SL（Short Length）字段、PN（Packet Number）字段以及 SCI（Secure Channel Identifier，安全通道标识）字段，其中，MACSec Ethertype 字段可以包括两个八位位组，一个八位位组可以包括 8 比特，TCI 字段和 AN 字段一共可以包括一个八位位组，SL 字段可以包括一个八位位组，PN 字段可以包括 4 个八位位组，SCI 字段可以包括 8 个八位位组，但发明并不限于此。在该 802.1AE Header 字段中，该 MACSec Ethertype 字段，即携带识别信息的以太网类型字段，可选的，该 MACSec Ethertype 字段中可以包括识别信息，也可以直接将该字段作为识别信息。可选地，如果将该字段作为识别信息，可以设置为当该 MACSec Ethertype 值字段为预设值时，则该报文为 ACP 报文；当该 MACSec Ether type 值不是该预设值时，则该报文为其它报文。例如，对于 802.1ae 格式封装的报文中，可以用 88e5 表示 MACSec Ethertype 值，则该报文为普通报文；设置一个新的 MACSec Ethertype 值为预设值，例如 88e6，  
30 则该报文即为 ACP 报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点向邻

居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以包括用于区别 ACP 报文的识别信息，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的标志位字段中，该标志位字段可以为新增字段，也可以为现有的某个字段。具体地，该标志位字段可以为该报文中原有的有一个指示位，例如，在 802.1ae 格式封装的报文中，如图 3 所示的 TCI 字段和 AN 5 字段占用一个八位位组，即这两个字段一共占用 8 比特，可以展开如图 4 所示，其中第 8 位的 v=0 表示版本 (version) 位，该版本位原本用于指示 MACSec 的版本，目前为 0，在本发明实施例中，可以将该版本位用于指示 ACP 报文，当该位的比特为 “1” 时，指示该报文为 ACP 报文；当该位的比特为 “0” 10 时，指示该报文为其它报文。可选地，也可以在传输报文中增加一个新的标志位，该标志位包括 ACP 报文的识别信息，例如，当该标志位为 “0” 时，指示该报文为 ACP 报文；当该标志位为 “1” 时，指示该报文为其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点向邻居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以 15 包括 ACP 报文的识别信息，用于指示该报文为 ACP 报文，例如该识别信息可以被携带在该传输报文中的 MAC 地址字段中，根据该 MAC 地址字段确定该传输报文是否为 ACP 报文。例如，现有的 MAC 地址的最高位的 8 比特，其中第二比特 b2 用于区分该 MAC 地址为本地管理 MAC 地址，还是全球 (global) MAC 地址，由于现有 MAC 地址大多为 global，因此，可以将 b2 20 位作为识别信息，用于指示该报文是否为 ACP 报文。这时，设备接口上同时使用本地管理 MAC 地址 (虚拟 MAC) 和全球 MAC 地址，当使用本地管理 MAC 地址传输报文时，即 b2 的值为 1 时，该传输报文为 ACP 报文；当使用全球 MAC 地址传输报文时，即 b2 的值为 0 时，该传输报文为其它报文，但本发明并不限于此。可选地，也可以在 MAC 地址字段中的其他位置携带 25 ACP 报文的识别信息，也可以在 MAC 地址字段中新增加一个或多个比特用于携带识别信息。

在本发明实施例中，ACP 各个节点可以通过上述方法，生成并向邻居节点发送 MACSec 协议封装的 ACP 报文。

因此，本发明实施例的报文传输的方法，根据 MACSec 协议，自组织网 30 络中的第一网络设备与第二网络设备之间建立 MACSec 通道，通过该 MACSec 通道，第一网络设备向第二网络设备发送 ACP 报文，该 ACP 报文

承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPSec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

上文中结合图 1 至图 4，从发送端即第一网络设备的角度详细描述了根据本发明实施例的报文传输的方法，下面将结合图 5，从接收端即第二网络设备的角度描述根据本发明实施例的报文传输的方法。

图 5 示出了根据本发明另一实施例的报文传输的方法 200 的示意性流程图，该方法 200 可以应用于自组织网络中，由自组织网络中的第一网络设备执行，该第一网络设备可以为接收节点。如图 5 所示，该方法 200 包括：

S210，第二网络设备根据介质访问控制安全 MACSec 协议，与第一网络设备建立 MACSec 通道；

S220，该第二网络设备通过该 MACSec 通道，接收该第一网络设备发送的 MACSec 帧；

S230，该第二网络设备根据该 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息，确定该 ACP 报文。

具体地，在自组织网络中，可以将一个节点设置为认证（Registrar）节点，该 Registrar 节点配置了自组织节点的 UDI 白名单，该 UDI 白名单内的节点可以加入该自组织域，并且 Registrar 节点本身连接到 domain CA（自组织域数字证书认证机构），支持分配域证书（domain certificate）。网络中各个节点发起邻居发现（AD）消息，通过该 AD 消息寻找邻居节点，该 AD 消息中包括 UDI 或域证书。根据该 AD 消息，各个节点可以创建邻居列表；

Registrar 节点收到该 AD 消息后，对比 UDI 白名单，向属于 UDI 白名单的该邻居节点发送域证书。基于该域证书，邻居节点与 Registrar 节点相互认证，并在认证成功后基于认证过程中生成的密钥协商出报文加密密钥，根据 MACSec 协议，建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地，针对 Registrar 节点的邻居节点的邻居节点，需要 Registrar 节点的邻居节点作为代理服务器（Proxy）以及认证点，其它步骤一致，从而建立自组织网络中相邻节点之间的 MACSec 通道，使得属于同一域的多个节点构成一

个 ACP。在该 ACP 内，各个节点之间可以通过 MACSec 通道，互相传输根据 MACSec 协议封装的 ACP 报文。

因此，本发明实施例的报文传输的方法，根据 MACSec 协议，自组织网络中的第二网络设备与第一网络设备之间建立 MACSec 通道，通过该  
5 MACSec 通道，第二网络设备接收第一网络设备发送的 MACSec 帧，根据该 MACSec 帧的帧头中的识别信息，确定 ACP 报文，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPSec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，  
10 从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

在本发明实施例中，自组织网络中各个节点支持自组织特性，每个节点都有自己的 UDI 或者设备 ID 证书 (IDevID certificate)，可选地，这里以各个节点通过 UDI 获取域证书为例进行说明，但本发明并不限于此。在该网络  
15 中，设置其中一个节点为认证 (Registrar) 节点，该 Registrar 节点支持分配域证书，并且配置了自组织节点的 UDI 白名单，该 UDI 白名单内的节点属于同一个自组织域。可选地，可以预配置该 Registrar 节点，Registrar 节点能够支持分配域证书的节点，即该 Registrar 节点与数字证书认证管理机构有连接，可以进行通信，换句话说，该 Registrar 节点能够通过数字证书认证管理  
20 结构为其他节点分配域证书。

在本发明实施例中，自组织特性使能后，自组织节点可以向邻居节点发送 AD 消息，从而寻找自己的邻居节点。可选地，各个节点可以每隔一段时间，例如 10s，发起一次 AD 消息。该 AD 消息可以包括 UDI 或者域证书，例如，对于 Registrar 节点发送的 AD 消息，Registrar 节点支持分配域证书，  
25 它会先给自己配置一个域证书，Registrar 节点发送的该 AD 消息中可以包括域证书；而对于没有域证书的节点发送的 AD 消息，该 AD 消息中可以包括 UDI。

在本发明实施例中，由于自组织节点发送的 AD 消息只能发送一跳的距离，即只有邻居节点可以收到该 AD 消息，因此当节点收到邻居节点发送的  
30 AD 消息后，可以建立一个邻居列表，用于记录属于该节点的邻居节点。可选地，该邻居列表可以包括邻居节点的 UDI，该 UDI 通过邻居节点发送的

AD 消息获得, 邻居列表还可以包括地址信息, 该地址信息可以为 IPv6 地址, 或 IPv4 地址, 或 MAC 地址, 该地址信息可以通过发送的 AD 消息的报文确定, 但本发明并不限于此。根据节点确定的邻居节点列表, 可以确定各个节点的邻居节点的 UDI 以及地址信息。

5        在本发明实施例中, 当 Registrar 节点收到邻居节点发送的 AD 消息后, 将 AD 消息中的 UDI 对比 Registrar 节点中的 UDI 白名单, 如果邻居节点的 UDI 匹配 UDI 白名单, 则 Registrar 节点根据该 UDI 生成一个域证书, 将该域证书发送给该邻居节点, 后续 AD 广播中将使用该域证书。此时, 具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

10       在本发明实施例中, 对于 Registrar 节点接收到的邻居节点发送的 AD 消息, 可以为该邻居节点的 AD 消息, 也可以为该邻居节点转发自己的邻居节点的 AD 消息, 并比照 UDI 白名单, 对于属于同一个域, 的节点, Registrar 节点均发送域证书, 可选地, 可以通过邻居节点互相转发, 具有该域证书的节点均属于同一个域, 该自组织网络中的这些节点属于同一个 ACP。

15       在本发明实施例中, 当自组织网络中每个节点有自己的 IDevID certificate 时, 则节点向邻居节点发送的 AD 消息包括域证书或 SUDI, 其中, Registrar 节点的 AD 消息可以包括域证书, 而没有域证书的节点的 AD 消息中包括 SUDI。邻居节点将自己的 802.1AR 证书发给 Registrar 节点, 可选地, 可以经过一个 Proxy。收到该消息的 Registrar 节点使用公钥验证该证书, 并且连接到验证服务器验证该设备是否可以接入域。如果验证成功, Registrar 节点根据该 SUDI 生成一个域证书, 发给对应的邻居节点, 该邻居节点接收到域证书, 后续 AD 广播中将使用域证书。同样地, Registrar 节点的邻居节点的邻居节点同样可以通过该方法获得域证书, 具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

25       在 S210 中, 根据介质访问控制安全 MACSec 协议, 自组织网络中的第一网络设备和第二网络设备可以建立 MACSec 通道, 其中, 该第一网络设备和第二网络设备可以为该自组织网络中的任意两个节点, 可选地, 该第一网络设备和第二网络设备可以为相邻的两个节点。具体地, 基于域证书, 获得域证书的邻居节点可以与 Registrar 节点相互认证, 并在认证成功后基于认证过程中生成的密钥协商出报文加密密钥, 根据 MACSec 协议, 建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地, 对于 Registrar 节点的邻居

30

节点的邻居节点，可以将 Registrar 节点的邻居节点作为代理服务器（Proxy）以及认证点，其它步骤一致，从而建立属于同一个域的各个节点中相邻节点之间的 MACSec 通道。这样，对于该 ACP 中的任意两个节点，即第一网络设备和第二网络设备之间可以通过该 MACSec 通道进行报文传输。

5       具体地，获得 Registrar 节点发送的域证书的邻居节点，可以向 Registrar 节点发起认证，例如可以发起基于 802.1X 的认证，Registrar 节点可以作为认证者（Authenticator）和认证服务器，实现 Registrar 节点和邻居节点之间的相互认证，例如，可以选择 EAP-TLS 的认证方式，遵守 802.1af 的标准。

10       在本发明实施例中，Registrar 节点与邻居节点认证成功后，基于认证过程中生成的密钥协商出报文加密密钥，建立起 ACP 专用的安全 MACSec 通道。具体地，按照 MKA 协议，将之前的 Registrar 节点与邻居节点认证中生成的 PMK 作为 CAK。Registrar 节点作为 Authenticator，默认被选择为 MKA 协议中的密钥服务器（key server），可以按照 802.1X 协议，根据 CAK，随机数等产生一个 SAK，加密后发给邻居节点，以便于在后续的通信中，启用  
15       这个 SAK 作以太帧的加密和签名。

20       在本发明实施例中，Registrar 节点与邻居节点通过上述方法建立 MACSec 通道后，对于 Registrar 节点的邻居节点的邻居节点加入该 ACP 时，Registrar 节点的邻居节点可以作为代理服务器（Proxy）以及认证点，同样通过上述方法获得域证书，进而加入该 ACP，并通过验证，建立与邻居节点之间的 MACSec 通道。

25       在 S220 中，在自组织网络中的 ACP 内，第二网络设备可以通过 MACSec 通道接收第一网络设备发送的 MACSec 帧。具体地，自组织网络中任意一个节点可以通过 MACSec 通道向邻居节点发送 ACP 报文，经过至少一次转发，自组织网络中的任意两个节点，第一网络设备和第二网络设备之间可以传输  
30       MACSec 帧。

30       在本发明实施例中，由于第二网络设备接收的该 MACSec 帧的帧头中可以包括识别信息，该识别信息用于区别该 MACSec 帧是否为 ACP 报文。因此，在 S230 中，第二网络设备可以根据 MACSec 帧的帧头中的识别信息，确定该 MACSec 帧为 ACP 报文。由于在 MAC 层，还可以通过 MACSec 通道传输其它报文，因此，具体地，可以根据在 MACSec 帧的帧头中携带的识别信息，区分该 MACSec 帧是否承载 ACP 报文，可选地，可以通过下面几

种方法确定接收到的根据 MACSec 协议封装的报文中的 ACP 报文以及其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以携带识别信息，该识别信息用于指示该帧结构用于承载 ACP 报文。具体地，若整个自组织网络不启用数据面的 MACSec 时，则根据 MACSec 协议封装的报文即为 ACP 报文，而其它报文可以通过 MAC 封装，该报文解封装后，由 Global 路由处理。例如，整个自组织网络不启用数据面的 MACSec 时，节点接收邻居节点发送的 802.1ae 格式封装的报文即为根据 MACSec 协议封装的报文，该报文即可被理解为 ACP 报文。具体地，如图 2 所示，802.1ae 格式封装的 MACSec 帧，该 MACSec 帧的帧头可以包括如图 2 所示的几种字段，其中，该 802.1AE 头（802.1AE Header）字段可以为识别信息，表示该帧结构为根据 MACSec 协议封装的报文，则该 MACSec 帧用于承载 ACP 报文，相反的，如果不包括该 802.1AE Header 字段，则可以确定该帧结构为其它的普通报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，该 MACSec 帧中包括 ACP 报文的识别信息，用于指示该报文为 ACP 报文，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的以太网类型字段中。具体地，传输的报文中可以包括以太网类型（Ethertype）字段，例如，如图 2 所示，该以太网类型字段可以位于 802.1AE Header 字段中，具体地，如图 3 所示，该 802.1AE Header 字段可以包括 MACSec Ethertype 字段、TCI 字段、AN 字段、SL 字段、PN 字段以及 SCI 字段。在该 802.1AE Header 字段中，该 MACSec Ethertype 字段，即携带识别信息的以太网类型字段，可选的，该 MACSec Ethertype 字段中可以包括识别信息，也可以直接将该字段作为识别信息。可选地，如果将该字段作为识别信息，可以设置为当该 MACSec Ethertype 值字段为预设值时，则该报文为 ACP 报文；当该 MACSec Ether type 值不是该预设值时，则该报文为其它报文。例如，对于 802.1ae 格式封装的报文中，可以用 88e5 表示 MACSec Ethertype 值，则该报文为普通报文；设置一个新的 MACSec Ethertype 值为预设值，例如 88e6，则该报文即为 ACP 报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点接收

邻居节点发送的 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中包括 ACP 报文的识别信息，用于指示该报文为 ACP 报文，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的标志位字段中，该标志位字段可以为新增字段，也可以为现有的某个字段。具体地，该标志位字段可以为该报文中原有的有一个指示位，例如，在 802.1ae 格式封装的报文中，如图 3 所示的 TCI 字段和 AN 字段可以展开如图 4 所示，其中 v=0 表示版本 (version) 位，该版本位原本用于指示 MACSec 的版本，目前为 0，在本发明实施例中，可以将该版本位用于指示 ACP 报文，当该位的比特为 “1” 时，指示该报文为 ACP 报文；当该位的比特为 “0” 时，指示该报文为其它报文。可选地，也可以在传输报文中增加一个新的标志位，该标志位包括 ACP 报文的识别信息，例如，当该标志位为 “0” 时，指示该报文为 ACP 报文；当该标志位为 “1” 时，指示该报文为其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中包括 ACP 报文的识别信息，用于指示该报文为 ACP 报文，例如该识别信息可以被携带在该传输报文中的 MAC 地址字段中，根据该 MAC 地址字段确定该传输报文是否为 ACP 报文。例如，现有的 MAC 地址的最高位的 8 比特，其中第二比特 b2 用于区分该 MAC 地址为本地管理 MAC 地址，还是全球 (global) MAC 地址，由于现有 MAC 地址大多为 global，因此，可以将 b2 位作为识别信息，用于指示该报文是否为 ACP 报文。这时，设备接口上同时使用本地管理 MAC 地址 (虚拟 MAC) 和全球 MAC 地址，当使用本地管理 MAC 地址传输报文时，即 b2 的值为 1 时，该传输报文为 ACP 报文；当使用全球 MAC 地址传输报文时，即 b2 的值为 0 时，该传输报文为其它报文，但本发明并不限于此。可选地，也可以在 MAC 地址字段中的其他位置携带 ACP 报文的识别信息，也可以在 MAC 地址字段中新增加一个或多个比特用于携带识别信息。

在本发明实施例中，自组织网络中的节点接收邻居节点发送的 MACSec 协议封装 MACSec 帧，根据该 MACSec 帧的帧头中包括的识别信息，确定 ACP 报文，具体地，可以通过上述方法确定哪些为 ACP 报文。

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。

因此，本发明实施例的报文传输的方法，根据 MACSec 协议，自组织网络中的第二网络设备与第一网络设备之间建立 MACSec 通道，通过该 MACSec 通道，第二网络设备接收第一网络设备发送的 MACSec 帧，根据该 MACSec 帧的帧头中的识别信息，确定 ACP 报文，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

上文中结合图 1 至图 5，详细描述了根据本发明实施例的报文传输的方法，下面将结合图 6 和图 7，描述根据本发明实施例的用于报文传输的装置。

图 6 示出了根据本发明实施例的用于报文传输的第一网络设备 300 的示意性流程图，该第一网络设备 300 可以为自组织网络中的发送节点。如图 6 所示，该第一网络设备 300 包括：

建立模块 310，用于该第一网络设备根据介质访问控制安全 MACSec 协议，与第二网络设备建立 MACSec 通道；

发送模块 320，用于该第一网络设备通过该建立模块建立的该 MACSec 通道，向该第二网络设备发送自组织控制平面 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息。

具体地，可以将自组织网络中的一个节点设置为认证 (Registrar) 节点，该 Registrar 节点配置了自组织节点的 UDI 白名单，该 UDI 白名单内的节点可以加入该自组织域，并且 Registrar 节点本身连接到 domain CA (自组织域数字证书认证机构)，支持分配域证书 (domain certificate)。网络中各个节点发起邻居发现 (AD) 消息，通过该 AD 消息寻找邻居节点，该 AD 消息中包括 UDI 或域证书。根据该 AD 消息，各个节点可以创建邻居列表；Registrar 节点收到该 AD 消息后，对比 UDI 白名单，向属于 UDI 白名单的该邻居节点发送域证书。基于该域证书，邻居节点与 Registrar 节点相互认证，并在认证成功基于认证过程中生成的密钥协商出报文加密密钥，根据 MACSec 协议，建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地，针对

Registrar 节点的邻居节点的邻居节点, 需要 Registrar 节点的邻居节点作为代理服务器 (Proxy) 以及认证点, 其它步骤一致, 从而建立自组织网络中相邻节点之间的 MACSec 通道, 使得属于同一域的多个节点构成一个 ACP。

在该 ACP 内, 各个节点之间可以通过 MACSec 通道, 互相传输根据 MACSec 协议封装的 ACP 报文。

因此, 本发明实施例的用于报文传输的第一网络设备, 根据 MACSec 协议, 自组织网络中的第一网络设备的建立模块与第二网络设备之间建立 MACSec 通道, 通过该 MACSec 通道, 第一网络设备的发送模块向第二网络设备发送 ACP 报文, 该 ACP 报文承载在 MACSec 帧中, 该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息, 从而不需要在接口上同时配置可路由的接口地址和用于建立 IPSec 的链路本地地址, 为传输 ACP 报文提供的 MACSec 安全机制, 不需要使用 L3 隧道, 进而提高了效率。并且, 可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文, 从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

在本发明实施例中, 自组织网络中各个节点支持自组织特性, 每个节点都有自己的 UDI 或者设备 ID 证书 (IDevID certificate), 可选地, 这里以各个节点通过 UDI 获取域证书为例进行说明, 但本发明并不限于此。在该网络中, 设置其中一个节点为认证 (Registrar) 节点, 该 Registrar 节点支持分配域证书, 并且配置了自组织节点的 UDI 白名单, 该 UDI 白名单内的节点属于同一个自组织域。可选地, 可以预配置该 Registrar 节点, Registrar 节点能够支持分配域证书的节点, 即该 Registrar 节点与数字证书认证管理机构有连接, 可以进行通信, 换句话说, 该 Registrar 节点能够通过数字证书认证管理结构为其他节点分配域证书。

在本发明实施例中, 自组织特性使能后, 自组织节点可以向邻居节点发送 AD 消息, 从而寻找自己的邻居节点。可选地, 各个节点可以每隔一段时间, 例如 10s, 发起一次 AD 消息。该 AD 消息可以包括 UDI 或者域证书, 例如, 对于 Registrar 节点发送的 AD 消息, Registrar 节点支持分配域证书, 它会先给自己配置一个域证书, Registrar 节点发送的该 AD 消息中可以包括域证书; 而对于没有域证书的节点发送的 AD 消息, 该 AD 消息中可以包括 UDI。

在本发明实施例中, 由于自组织节点发送的 AD 消息只能发送一跳的距

离，即只有邻居节点可以收到该 AD 消息，因此当节点收到邻居节点发送的 AD 消息后，可以建立一个邻居列表，用于记录属于该节点的邻居节点。可选地，该邻居列表可以包括邻居节点的 UDI，该 UDI 通过邻居节点发送的 AD 消息获得，邻居列表还可以包括地址信息，该地址信息可以为 IPv6 地址，或 IPv4 地址，或 MAC 地址，该地址信息可以通过发送的 AD 消息的报文确定，但本发明并不限于此。根据节点确定的邻居节点列表，可以确定各个节点的邻居节点的 UDI 以及地址信息。

在本发明实施例中，当 Registrar 节点收到邻居节点发送的 AD 消息后，将 AD 消息中的 UDI 对比 Registrar 节点中的 UDI 白名单，如果邻居节点的 UDI 匹配 UDI 白名单，则 Registrar 节点根据该 UDI 生成一个域证书，将该域证书发送给该邻居节点，后续 AD 广播中将使用该域证书。此时，具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

在本发明实施例中，对于 Registrar 节点接收到的邻居节点发送的 AD 消息，可以为该邻居节点的 AD 消息，也可以为该邻居节点转发自己的邻居节点的 AD 消息，并比照 UDI 白名单，对于属于同一个域的点，Registrar 节点均发送域证书，可选地，可以通过邻居节点互相转发，具有该域证书的节点均属于同一个域，该自组织网络中的这些节点属于同一个 ACP。

在本发明实施例中，当自组织网络中每个节点有自己的 IDevID certificate 时，则节点向邻居节点发送的 AD 消息包括域证书或 SUDI，其中，Registrar 节点的 AD 消息可以包括域证书，而没有域证书的节点的 AD 消息中包括 SUDI。邻居节点将自己的 802.1AR 证书发给 Registrar 节点，可选地，可以经过一个 Proxy。收到该消息的 Registrar 节点使用公钥验证该证书，并且连接到验证服务器验证该设备是否可以接入域。如果验证成功，Registrar 节点根据该 SUDI 生成一个域证书，发给对应的邻居节点，该邻居节点接收到域证书，后续 AD 广播中将使用域证书。同样地，Registrar 节点的邻居节点的邻居节点同样可以通过该方法获得域证书，具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

在本发明实施例中，根据 MACSec 协议，自组织网络中的第一网络设备的建立模块 310 建立与第二网络设备之间的 MACSec 通道，其中，该第一网络设备和第二网络设备可以为该自组织网络中的任意两个节点，可选地，该第一网络设备和第二网络设备可以为相邻的两个节点。具体地，基于该域证

书，获得域证书的邻居节点可以与 Registrar 节点相互认证，并在认证成功后基于认证过程中生成的密钥协商出报文加密密钥，根据 MACSec 协议，建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地，对于 Registrar 节点的邻居节点的邻居节点，可以将 Registrar 节点的邻居节点作为代理服务器（Proxy）以及认证点，其它步骤一致，从而建立属于同一个域的各个节点中相邻节点之间的 MACSec 通道。这样，对于该 ACP 中的任意两个节点，即第一网络设备和第二网络设备之间可以通过该 MACSec 通道进行报文传输。

具体地，获得 Registrar 节点发送的域证书的邻居节点，可以向 Registrar 节点发起认证，例如可以发起基于 802.1X 的认证，Registrar 节点可以作为认证者（Authenticator）和认证服务器，实现 Registrar 节点和邻居节点之间的相互认证，例如，可以选择 EAP-TLS 的认证方式，遵守 802.1af 的标准。

在本发明实施例中，Registrar 节点与邻居节点认证成功后，基于认证过程中生成的密钥协商出报文加密密钥，建立起 ACP 专用的安全 MACSec 通道。具体地，按照 MKA 协议，将之前的 Registrar 节点与邻居节点认证中生成的 PMK 作为 CAK。Registrar 节点作为 Authenticator，默认被选择为 MKA 协议中的密钥服务器（key server），可以按照 802.1X 协议，根据 CAK，随机数等产生一个 SAK，加密后发给邻居节点，以便于在后续的通信中，启用这个 SAK 作以太帧的加密和签名。

在本发明实施例中，Registrar 节点与邻居节点通过上述方法建立 MACSec 通道后，对于 Registrar 节点的邻居节点的邻居节点加入该 ACP 时，Registrar 节点的邻居节点可以作为代理服务器（Proxy）以及认证点，同样通过上述方法获得域证书，进而加入该 ACP，并通过验证，建立与邻居节点之间的 MACSec 通道。

在本发明实施例中，在自组织网络中的 ACP 内，第一网络设备的发送模块 320 可以通过建立模块 310 建立的 MACSec 通道向第二网络设备发送 ACP 报文，具体地，自组织网络中任意一个节点的发送模块 320 可以通过 MACSec 通道向邻居节点发送 ACP 报文，经过至少一次转发，自组织网络中的任意两个节点，第一网络设备和第二网络设备之间可以传输 ACP 报文。由于在 MAC 层，还可以通过 MACSec 通道传输其它报文，因此，具体地，可以在 MACSec 帧的帧头中携带识别信息，可以通过该识别信息区分该

MACSec 帧是否承载 ACP 报文，可选地，可以通过下面几种方法确定根据 MACSec 协议封装的报文中的 ACP 报文以及其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，节点的发送模块 320 向邻居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以携带识别信息，该识别信息用于指示该帧结构用于承载 ACP 5 报文。具体地，若整个自组织网络不启用数据面的 MACSec 时，则根据 MACSec 协议封装的报文即为 ACP 报文，而其它报文可以通过 MAC 封装，该报文解封装后，由 Global 路由处理。例如，整个自组织网络不启用数据面的 MACSec 时，节点向邻居节点发送的 802.1ae 格式封装的报文即为根据 10 MACSec 协议封装的报文，该报文即可被理解为 ACP 报文。具体地，如图 2 所示，802.1ae 格式封装的 MACSec 帧，该 MACSec 帧的帧头可以包括如图 2 所示的几种字段，其中，该 802.1AE 头（802.1AE Header）字段可以为识别信息，表示该帧结构为根据 MACSec 协议封装的报文，则该 MACSec 帧用于承载 ACP 报文，相反的，如果不包括该 802.1AE Header 字段，则可以 15 确定该帧结构为其它的普通报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，节点的发送模块 320 向邻居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以携带识别信息，该识别信息用于指示该帧结构用于承载 ACP 报文，例如该识别信息可以被携带在传输的报文中的以太网类型字段中。具体地，传输的报文中可以包括以太网类型（Ethertype）字段，例如，如图 2 20 所示，该以太网类型字段可以位于 802.1AE Header 字段中，具体地，如图 3 所示，该 802.1AE Header 字段可以包括 MACSec Ethertype 字段、TCI 字段、AN 字段、SL 字段、PN 字段以及 SCI 字段。在该 802.1AE Header 字段中，该 MACSec Ethertype 字段，即携带识别信息的以太网类型字段，可选的， 25 该 MACSec Ethertype 字段中可以包括识别信息，也可以直接将该字段作为识别信息。可选地，如果将该字段作为识别信息，可以设置为当该 MACSec Ethertype 值字段为预设值时，则该报文为 ACP 报文；当该 MACSec Ether type 值不是该预设值时，则该报文为其它报文。例如，对于 802.1ae 格式封装的报文中，可以用 88e5 表示 MACSec Ethertype 值，则该报文为普通报文；设 30 置一个新的 MACSec Ethertype 值为预设值，例如 88e6，则该报文即为 ACP 报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，节点的发送模块 320 向邻居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以包括用于区别 ACP 报文的识别信息，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的标志位字段中，该标志位字段可以为新增字段，也可以为现有的某个字段。具体地，该标志位字段可以为该报文中原有的有一个指示位，例如，在 802.1ae 格式封装的报文中，如图 3 所示的 TCI 字段和 AN 字段可以展开如图 4 所示，其中 v=0 表示版本 (version) 位，该版本位原本用于指示 MACSec 的版本，目前为 0，在本发明实施例中，可以将该版本位用于指示 ACP 报文，当该位的比特为 “1” 时，指示该报文为 ACP 报文；当该位的比特为 “0” 时，指示该报文为其它报文。可选地，也可以在传输报文中增加一个新的标志位，该标志位包括 ACP 报文的识别信息，例如，当该标志位为 “0” 时，指示该报文为 ACP 报文；当该标志位为 “1” 时，指示该报文为其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，节点的发送模块 320 向邻居节点发送 MACSec 协议封装的 MACSec 帧，该 MACSec 帧的帧头中可以包括 ACP 报文的识别信息，用于指示该报文为 ACP 报文，例如该识别信息可以被携带在该传输报文中的 MAC 地址字段中，根据该 MAC 地址字段确定该传输报文是否为 ACP 报文。例如，现有的 MAC 地址的最高位的 8 比特，其中第二比特 b2 用于区分该 MAC 地址为本地管理 MAC 地址，还是全球 (global) MAC 地址，由于现有 MAC 地址大多为 global，因此，可以将 b2 位作为识别信息，用于指示该报文是否为 ACP 报文。这时，设备接口上同时使用本地管理 MAC 地址 (虚拟 MAC) 和全球 MAC 地址，当使用本地管理 MAC 地址传输报文时，即 b2 的值为 1 时，该传输报文为 ACP 报文；当使用全球 MAC 地址传输报文时，即 b2 的值为 0 时，该传输报文为其它报文，但本发明并不限于此。可选地，也可以在 MAC 地址字段中的其他位置携带 ACP 报文的识别信息，也可以在 MAC 地址字段中新增加一个或多个比特用于携带识别信息。

在本发明实施例中，ACP 各个节点可以通过上述方法，由发送模块 320 向邻居节点发送 MACSec 协议封装的 ACP 报文。

应理解，根据本发明实施例的用于报文传输的第一网络设备 300 可对应于执行本发明实施例中的方法 100，并且用于报文传输的第一网络设备 300

中的各个模块的上述和其它操作和/或功能分别为了实现图 1 中的各个方法的相应流程,为了简洁,在此不再赘述。

因此,本发明实施例的用于报文传输的第一网络设备,根据 MACSec 协议,自组织网络中的第一网络设备的建立模块与第二网络设备之间建立  
5 MACSec 通道,通过该 MACSec 通道,第一网络设备的发送模块向第二网络设备发送 ACP 报文,该 ACP 报文承载在 MACSec 帧中,该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息,从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址,为传输 ACP 报文提供的 MACSec 安全机制,不需要使用 L3 隧道,进而提高了效率。并且,  
10 可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文,从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

图 7 示出了根据本发明另一实施例的报文传输的第二网络设备 400 的示意性流程图,该第二网络设备 400 可以自组织网络中的接收节点。如图 7 所示,该第二网络设备 400 包括:

15 建立模块 410,用于该第二网络设备根据介质访问控制安全 MACSec 协议,与第一网络设备建立 MACSec 通道;

接收模块 420,用于该第二网络设备通过该建立模块建立的该 MACSec 通道,接收该第一网络设备发送的 MACSec 帧;

20 确定模块 430,用于该第二网络设备根据该接收模块接收的该 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息,确定该 ACP 报文。

具体地,可以将自组织网络中的一个节点设置为认证(Registrar)节点,该 Registrar 节点配置了自组织节点的 UDI 白名单,该 UDI 白名单内的节点可以加入该自组织域,并且 Registrar 节点本身连接到 domain CA,支持分配  
25 域证书(domain certificate)。网络中各个节点发起邻居发现(AD)消息,通过该 AD 消息寻找邻居节点,该 AD 消息中包括 UDI 或域证书。根据该 AD 消息,各个节点可以创建邻居列表;Registrar 节点收到该 AD 消息后,对比 UDI 白名单,向属于 UDI 白名单的该邻居节点发送域证书。基于该域证书,邻居节点与 Registrar 节点相互认证,并在认证成功后基于认证过程中生成的  
30 密钥协商出报文加密密钥,根据 MACSec 协议,建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地,针对 Registrar 节点的邻居节点的邻居

节点，需要 Registrar 节点的邻居节点作为代理服务器（Proxy）以及认证点，其它步骤一致，从而建立自组织网络中相邻节点之间的 MACSec 通道，使得属于同一域的多个节点构成一个 ACP。在该 ACP 内，各个节点之间可以通过 MACSec 通道，互相传输根据 MACSec 协议封装的 ACP 报文。

5       因此，本发明实施例的用于报文传输的第二网络设备，根据 MACSec 协议，该第二网络设备与第一网络设备之间建立 MACSec 通道，通过该 MACSec 通道，该第二网络设备接收第一网络设备发送的 MACSec 帧，根据该 MACSec 帧中的识别信息确定 ACP 报文，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址，为传输 ACP 报文提供  
10       的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以通过 MACSec 通道传输 ACP 报文。

      在本发明实施例中，自组织网络中各个节点支持自组织特性，每个节点  
15       都有自己的 UDI 或者设备 ID 证书（IDevID certificate），可选地，这里以各个节点通过 UDI 获取域证书为例进行说明，但本发明并不限于此。在该网络中，设置其中一个节点为认证（Registrar）节点，该 Registrar 节点支持分配域证书，并且配置了自组织节点的 UDI 白名单，该 UDI 白名单内的节点属于同一个自组织域。可选地，可以预配置该 Registrar 节点，Registrar 节点能  
20       够支持分配域证书的节点，即该 Registrar 节点与数字证书认证管理机构有连接，可以进行通信，换句话说，该 Registrar 节点能够通过数字证书认证管理结构为其他节点分配域证书。

      在本发明实施例中，自组织特性使能后，自组织节点可以向邻居节点发送 AD 消息，从而寻找自己的邻居节点。可选地，各个节点可以每隔一段时间，例如 10s，发起一次 AD 消息。该 AD 消息可以包括 UDI 或者域证书，  
25       例如，对于 Registrar 节点发送的 AD 消息，Registrar 节点支持分配域证书，它会先给自己配置一个域证书，Registrar 节点发送的该 AD 消息中可以包括域证书；而对于没有域证书的节点发送的 AD 消息，该 AD 消息中可以包括 UDI。

30       在本发明实施例中，由于自组织节点发送的 AD 消息只能发送一跳的距离，即只有邻居节点可以收到该 AD 消息，因此当节点收到邻居节点发送的

AD 消息后，可以建立一个邻居列表，用于记录属于该节点的邻居节点。可选地，该邻居列表可以包括邻居节点的 UDI，该 UDI 通过邻居节点发送的 AD 消息获得，邻居列表还可以包括地址信息，该地址信息可以为 IPv6 地址，或 IPv4 地址，或 MAC 地址，该地址信息可以通过发送的 AD 消息的报文确定，但本发明并不限于此。根据节点确定的邻居节点列表，可以确定各个节点的邻居节点的 UDI 以及地址信息。

在本发明实施例中，当 Registrar 节点收到邻居节点发送的 AD 消息后，将 AD 消息中的 UDI 对比 Registrar 节点中的 UDI 白名单，如果邻居节点的 UDI 匹配 UDI 白名单，则 Registrar 节点根据该 UDI 生成一个域证书，将该域证书发送给该邻居节点，后续 AD 广播中将使用该域证书。此时，具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

在本发明实施例中，对于 Registrar 节点接收到的邻居节点发送的 AD 消息，可以为该邻居节点的 AD 消息，也可以为该邻居节点转发自己的邻居节点的 AD 消息，并比照 UDI 白名单，对于属于同一个域的点，Registrar 节点均发送域证书，可选地，可以通过邻居节点互相转发，具有该域证书的节点均属于同一个域，该自组织网络中的这些节点属于同一个 ACP。

在本发明实施例中，当自组织网络中每个节点有自己的 IDevID certificate 时，则节点向邻居节点发送的 AD 消息包括域证书或 SUDI，其中，Registrar 节点的 AD 消息可以包括域证书，而没有域证书的节点的 AD 消息中包括 SUDI。邻居节点将自己的 802.1AR 证书发给 Registrar 节点，可选地，可以经过一个 Proxy。收到该消息的 Registrar 节点使用公钥验证该证书，并且连接到验证服务器验证该设备是否可以接入域。如果验证成功，Registrar 节点根据该 SUDI 生成一个域证书，发给对应的邻居节点，该邻居节点接收到域证书，后续 AD 广播中将使用域证书。同样地，Registrar 节点的邻居节点的邻居节点同样可以通过该方法获得域证书，具有域证书的该 Registrar 节点和邻居节点属于同一个 ACP。

在本发明实施例中，根据 MACSec 协议，自组织网络中的第一网络设备的建立模块 410 建立与第一网络设备之间的 MACSec 通道，其中，该第一网络设备和第二网络设备可以为该自组织网络中的任意两个节点，可选地，该第一网络设备和第二网络设备可以为相邻的两个节点。具体地，基于域证书，获得域证书的邻居节点可以与 Registrar 节点相互认证，并在认证成功后基于

认证过程中生成的密钥协商出报文加密密钥，根据 MACSec 协议，建立 Registrar 节点与邻居节点之间的 MACSec 通道。同样地，对于 Registrar 节点的邻居节点的邻居节点，可以将 Registrar 节点的邻居节点作为代理服务器（Proxy）以及认证点，其它步骤一致，从而建立属于同一个域的各个节点中相邻节点之间的 MACSec 通道。这样，对于该 ACP 中的任意两个节点，即第一网络设备和第二网络设备之间可以通过该 MACSec 通道进行报文传输。

具体地，获得 Registrar 节点发送的域证书的邻居节点，可以向 Registrar 节点发起认证，例如可以发起基于 802.1X 的认证，Registrar 节点可以作为认证者（Authenticator）和认证服务器，实现 Registrar 节点和邻居节点之间的相互认证，例如，可以选择 EAP-TLS 的认证方式，遵守 802.1af 的标准。

在本发明实施例中，Registrar 节点与邻居节点认证成功后，基于认证过程中生成的密钥协商出报文加密密钥，建立起 ACP 专用的安全 MACSec 通道。具体地，按照 MKA 协议，将之前的 Registrar 节点与邻居节点认证中生成的 PMK 作为 CAK。Registrar 节点作为 Authenticator，默认被选择为 MKA 协议中的密钥服务器（key server），可以按照 802.1X 协议，根据 CAK，随机数等产生一个 SAK，加密后发给邻居节点，以便于在后续的通信中，启用这个 SAK 作以太帧的加密和签名。

在本发明实施例中，Registrar 节点与邻居节点通过上述方法建立 MACSec 通道后，对于 Registrar 节点的邻居节点的邻居节点加入该 ACP 时，Registrar 节点的邻居节点可以作为代理服务器（Proxy）以及认证点，同样通过上述方法获得域证书，进而加入该 ACP，并通过验证，建立与邻居节点之间的 MACSec 通道。

在本发明实施例中，在自组织网络中的 ACP 内，第二网络设备的接收模块 420 可以通过 MACSec 通道接收第一网络设备发送的 MACSec 帧。具体地，自组织网络中任意一个节点可以通过 MACSec 通道向邻居节点发送 ACP 报文，经过至少一次转发，自组织网络中的任意两个节点，第一网络设备和第二网络设备之间可以传输 MACSec 帧。

在本发明实施例中，由于第二网络设备的接收模块 420 接收的该 MACSec 帧的帧头中可以包括识别信息，该识别信息用于区别该 MACSec 帧是否为 ACP 报文。因此，第二网络设备的确定模块 430 可以根据 MACSec

帧的帧头中的识别信息，确定该 MACSec 帧为 ACP 报文。由于在 MAC 层，还可以通过 MACSec 通道传输其它报文，因此，具体地，可以根据在 MACSec 帧的帧头中携带的识别信息，区分该 MACSec 帧是否承载 ACP 报文，可选地，可以通过下面几种方法确定接收到的根据 MACSec 协议封装的报文中的

## 5 ACP 报文以及其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点的接收模块 420 接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，确定模块 430 可以根据该 MACSec 帧的帧头中携带的识别信息确定 ACP 报文。具体地，若整个自组织网络不启用数据面的 MACSec 时，则根据 MACSec 协议封装的报文即为 ACP 报文，而其它报文可以通过 MAC 封装，该报文解封后，由 Global 路由处理。例如，整个自组织网络不启用数据面的 MACSec 时，节点接收邻居节点发送的 802.1ae 格式封装的报文即为根据 MACSec 协议封装的报文，该报文即可被理解为 ACP 报文。具体地，如图 2 所示，802.1ae 格式封装的 MACSec 帧，该 MACSec 帧的帧头可以包括如图 2 所示的几种字段，其中，该 802.1AE 头（802.1AE Header）字段可以为识别信息，表示该帧结构为根据 MACSec 协议封装的报文，则该 MACSec 帧用于承载 ACP 报文，相反的，如果不包括该 802.1AE Header 字段，则可以确定该帧结构为其它的普通报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点的接收模块 420 接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，确定模块 430 可以根据该 MACSec 帧中包括的 ACP 报文的识别信息，确定该报文为 ACP 报文，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的以太网类型字段中。具体地，传输的报文中可以包括以太网类型（Ethernet type）字段，例如，如图 2 所示，该以太网类型字段可以位于 802.1AE Header 字段中，具体地，如图 3 所示，该 802.1AE Header 字段可以包括 MACSec Ethernet type 字段、TCI 字段、AN 字段、SL 字段、PN 字段以及 SCI 字段。在该 802.1AE Header 字段中，该 MACSec Ethernet type 字段，即携带识别信息的以太网类型字段，可选的，该 MACSec Ethernet type 字段中可以包括识别信息，也可以直接将该字段作为识别信息。可选地，如果将该字段作为识别信息，可以设置为当该 MACSec Ethernet type 值字段为预设值时，则该报文为 ACP 报文；当该 MACSec Ethernet type 值不是该预设值时，则该报文为其它报文。例如，对于

802.1ae 格式封装的报文中，可以用 88e5 表示 MACSec Ethertype 值，则该报文为普通报文；设置一个新的 MACSec Ethertype 值为预设值，例如 88e6，则该报文即为 ACP 报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点的接收模块 420 接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，确定模块 430 可以根据该 MACSec 帧的帧头中包括的 ACP 报文的识别信息，确定该报文为 ACP 报文，例如该识别信息可以被携带在传输的 MACSec 帧的帧头中的标志位字段中，该标志位字段可以为新增字段，也可以为现有的某个字段。具体地，该标志位字段可以为该报文中原有的有一个指示位，例如，在 802.1ae 格式封装的报文中，如图 3 所示的 TCI 字段和 AN 字段可以展开如图 4 所示，其中 v=0 表示版本(version)位，该版本位原本用于指示 MACSec 的版本，目前为 0，在本发明实施例中，可以将该版本位用于指示 ACP 报文，当该位的比特为“1”时，指示该报文为 ACP 报文；当该位的比特为“0”时，指示该报文为其它报文。可选地，也可以在传输报文中增加一个新的标志位，该标志位包括 ACP 报文的识别信息，例如，当该标志位为“0”时，指示该报文为 ACP 报文；当该标志位为“1”时，指示该报文为其它报文。

可选地，作为一个实施例，以邻居节点之间传输报文为例，当节点的接收模块 420 接收邻居节点发送的 MACSec 协议封装的 MACSec 帧，确定模块 430 可以根据该 MACSec 帧的帧头中包括的 ACP 报文的识别信息，确定该报文为 ACP 报文，例如该识别信息可以被携带在该传输报文中的 MAC 地址字段中，根据该 MAC 地址字段确定该传输报文是否为 ACP 报文。例如，现有的 MAC 地址的最高位的 8 比特，其中第二比特 b2 用于区分该 MAC 地址为本地管理 MAC 地址，还是全球(global) MAC 地址，由于现有 MAC 地址大多为 global，因此，可以将 b2 位作为识别信息，用于指示该报文是否为 ACP 报文。这时，设备接口上同时使用本地管理 MAC 地址(虚拟 MAC)和全球 MAC 地址，当使用本地管理 MAC 地址传输报文时，即 b2 的值为 1 时，该传输报文为 ACP 报文；当使用全球 MAC 地址传输报文时，即 b2 的值为 0 时，该传输报文为其它报文，但本发明并不限于此。可选地，也可以在 MAC 地址字段中的其他位置携带 ACP 报文的识别信息，也可以在 MAC 地址字段中新增加一个或多个比特用于携带识别信息。

在本发明实施例中，自组织网络中的节点的接收模块 420 接收邻居节点

发送的 MACSec 协议封装的 MACSec 帧，确定模块 430 根据该 MACSec 帧的帧头中包括的识别信息，确定 ACP 报文，具体地，可以通过上述方法确定哪些为 ACP 报文。

5 应理解，根据本发明实施例的用于报文传输的第二网络设备 400 可对应于执行本发明实施例中的方法 200，并且用于报文传输的第二网络设备 400 中的各个模块的上述和其它操作和/或功能分别为了实现图 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

因此，本发明实施例的用于报文传输的第二网络设备，根据 MACSec 协议，该第二网络设备与第一网络设备之间建立 MACSec 通道，通过该  
10 MACSec 通道，该第二网络设备接收第一网络设备发送的 MACSec 帧，根据该 MACSec 帧中的识别信息确定 ACP 报文，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得  
15 自组织网络中的第一网络设备和第二网络设备之间可以通过 MACSec 通道传输 ACP 报文。

如图 8 所示，本发明实施例还提供了一种用于报文传输的系统 500，该系统 500 可以包括第一网络设备 510 和第二网络设备 520。该第一网络设备 510 根据 MACSec 协议，与该第二网络设备 520 建立 MACSec 通道；通过该  
20 MACSec 通道，该第一网络设备 510 向该第二网络设备 520 发送 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息；该第二网络设备 520 接收该 MACSec 帧；该第二网络设备 520 根据该 MACSec 帧的帧头中携带的用于标识 ACP 报文的识别信息，确定该 ACP 报文。

25 该第一网络设备 510 可以是如图 6 所示的所示的第一网络设备 300，第二网络设备 520 可以是如图 7 所示的第二网络设备 400。

该第一网络设备 510 还可以包括如图 6 所示的建立模块 310 和发送模块 320；该第二网络设备 520 还可以包括如图 7 所示的建立模块 410，接收模块 420 和确定模块 430。

30 因此，本发明实施例的用于报文传输的系统，包括自组织网络中的第一网络设备和第二网络设备，根据 MACSec 协议，该第一网络设备和第二网络

设备之间建立 MACSec 通道, 通过该 MACSec 通道, 第一网络设备与第二网络设备之间可以传输 MACSec 帧, 该 MACSec 帧的帧头中携带了识别信息, 可以根据该识别信息表示 ACP 报文, 从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址, 而是根据 MACSec 协议, 为 ACP 提供 MACSec 安全机制, 不需要使用 L3 隧道, 进而提高了效率。并且, 可以通过识别信息区分 MACSec 帧中的 ACP 报文, 从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

如图 9 所示, 本发明实施例还提供了一种用于报文传输的第一网络设备 600, 该第一网络设备 600 包括处理器 610、存储器 620、发送器 630 和总线系统 640。其中, 处理器 610、存储器 620 和发送器 630 通过总线系统 640 相连, 该存储器 620 用于存储指令, 该处理器 610 用于执行该存储器 620 存储的指令, 以控制发送器 630 发送信号。其中, 该处理器 610 用于第一网络设备根据介质访问控制安全 MACSec 协议, 与第二网络设备建立 MACSec 通道; 发送器 630 用于该第一网络设备通过该 MACSec 通道, 向该第二网络设备发送自组织控制平面 ACP 报文, 该 ACP 报文承载在 MACSec 帧中, 该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息。

因此, 本发明实施例的用于报文传输的第一网络设备, 根据 MACSec 协议, 自组织网络中的第一网络设备的建立模块与第二网络设备之间建立 MACSec 通道, 通过该 MACSec 通道, 第一网络设备的发送模块向第二网络设备发送 ACP 报文, 该 ACP 报文承载在 MACSec 帧中, 该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息, 从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址, 为传输 ACP 报文提供的 MACSec 安全机制, 不需要使用 L3 隧道, 进而提高了效率。并且, 可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文, 从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

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

该存储器 620 可以包括只读存储器和随机存取存储器, 并向处理器 610

提供指令和数据。存储器 620 的一部分还可以包括非易失性随机存取存储器。例如，存储器 620 还可以存储设备类型的信息。

该总线系统 640 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统 640。

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

可选地，作为一个实施例，该识别信息携带在该 MACSec 帧的帧头中的以太网类型字段中，该以太网类型字段用于指示该 MACSec 帧用于承载该 ACP 报文。

可选地，作为一个实施例，该识别信息携带在该 MACSec 帧的帧头中的标志位字段中，该标志位字段为新增字段或版本字段。

可选地，作为一个实施例，该识别信息携带在该 MACSec 帧的帧头中的 MAC 地址字段中。

应理解，根据本发明实施例的用于报文传输的第一网络设备 600 可对应于本发明实施例中的用于报文传输的第一网络设备 300，并可以对应于执行根据本发明实施例的方法 100 中的相应主体，并且第一网络设备 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 中的各个方法的相应流程，为了简洁，在此不再赘述。

因此，本发明实施例的用于报文传输的第一网络设备，根据 MACSec 协议，自组织网络中的第一网络设备的建立模块与第二网络设备之间建立 MACSec 通道，通过该 MACSec 通道，第一网络设备的发送模块向第二网络设备发送 ACP 报文，该 ACP 报文承载在 MACSec 帧中，该 MACSec 帧的帧头中携带了用于标识该 ACP 报文的识别信息，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，

可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以传输 ACP 报文。

如图 10 所示，本发明实施例还提供了一种用于报文传输的第二网络设备 700，该第二网络设备 700 包括处理器 710、存储器 720、接收器 730 和总线系统 740。其中，处理器 710、存储器 720 和接收器 730 通过总线系统 740 相连，该存储器 720 用于存储指令，该处理器 710 用于执行该存储器 720 存储的指令，以控制接收器 730 接收信号。其中，该处理器 710 用于第二网络设备根据介质访问控制安全 MACSec 协议，与第一网络设备建立 MACSec 通道；接收器 730 用于该第二网络设备通过该 MACSec 通道，接收该第一网络设备发送的 MACSec 帧该处理器 710 还用于该第二网络设备根据该 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息，确定该 ACP 报文。

因此，本发明实施例的用于报文传输的第二网络设备，根据 MACSec 协议，该第二网络设备与第一网络设备之间建立 MACSec 通道，通过该 MACSec 通道，该第二网络设备接收第一网络设备发送的 MACSec 帧，根据该 MACSec 帧中的识别信息确定 ACP 报文，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以通过 MACSec 通道传输 ACP 报文。

应理解，在本发明实施例中，该处理器 710 可以是中央处理单元 (Central Processing Unit，简称为“CPU”)，该处理器 710 还可以是其他通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现成可编程门阵列 (FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

该存储器 720 可以包括只读存储器和随机存取存储器，并向处理器 710 提供指令和数据。存储器 720 的一部分还可以包括非易失性随机存取存储器。例如，存储器 720 还可以存储设备类型的信息。

该总线系统 740 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线

系统 740。

在实现过程中，上述方法的各步骤可以通过处理器 710 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本发明实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 720，处理器 710 读取存储器 720 中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

可选地，作为一个实施例，该识别信息携带在该 MACSec 帧的帧头中的以太网类型字段中，该以太网类型字段用于指示该 MACSec 帧用于承载该 ACP 报文。

可选地，作为一个实施例，该识别信息携带在该 MACSec 帧的帧头中的标志位字段中，该标志位字段为新增字段或版本字段。

可选地，作为一个实施例，该识别信息携带在该 MACSec 帧的帧头中的 MAC 地址字段中。

应理解，根据本发明实施例的用于报文传输的第二网络设备 700 可对应于本发明实施例中的用于报文传输的第二网络设备 400，并可以对应于执行根据本发明实施例的方法 200 中的相应主体，并且第二网络设备 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 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

因此，本发明实施例的用于报文传输的第二网络设备，根据 MACSec 协议，该第二网络设备与第一网络设备之间建立 MACSec 通道，通过该 MACSec 通道，该第二网络设备接收第一网络设备发送的 MACSec 帧，根据该 MACSec 帧中的识别信息确定 ACP 报文，从而不需要在接口上同时配置可路由的接口地址和用于建立 IPsec 的链路本地地址，为传输 ACP 报文提供的 MACSec 安全机制，不需要使用 L3 隧道，进而提高了效率。并且，可以通过 MACSec 帧的帧头中的识别信息区分 ACP 报文和其他报文，从而使得自组织网络中的第一网络设备和第二网络设备之间可以通过 MACSec 通道传输 ACP 报文。

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  
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。

5 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。

10 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。

15 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。

20 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。

25 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。

30 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所述以权利要求的保护范围为准。

## 权利要求

1. 一种报文传输的方法, 应用在自组织网络中, 其特征在于, 所述方法包括:

5 第一网络设备根据介质访问控制安全 MACSec 协议, 与第二网络设备建立 MACSec 通道;

所述第一网络设备通过所述 MACSec 通道, 向所述第二网络设备发送自组织控制平面 ACP 报文, 所述 ACP 报文承载在 MACSec 帧中, 所述 MACSec 帧的帧头中携带了用于标识所述 ACP 报文的识别信息。

10 2. 根据权利要求 1 所述的方法, 其特征在于, 所述识别信息携带在所述 MACSec 帧的帧头中的以太网类型字段中, 所述以太网类型字段用于指示所述 MACSec 帧用于承载所述 ACP 报文。

3. 根据权利要求 1 所述的方法, 其特征在于, 所述识别信息携带在所述 MACSec 帧的帧头中的标志位字段中, 所述标志位字段为新增字段或版本字段。

15 4. 根据权利要求 1 所述的方法, 其特征在于, 所述识别信息携带在所述 MACSec 帧的帧头中的 MAC 地址字段中。

5. 一种报文传输的方法, 应用在自组织网络中, 其特征在于, 所述方法包括:

20 第二网络设备根据介质访问控制安全 MACSec 协议, 与第一网络设备建立 MACSec 通道;

所述第二网络设备通过所述 MACSec 通道, 接收所述第一网络设备发送的 MACSec 帧;

所述第二网络设备根据所述 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息, 确定所述 ACP 报文。

25 6. 根据权利要求 5 所述的方法, 其特征在于, 所述识别信息携带在所述 MACSec 帧的帧头中的以太网类型字段中, 所述以太网类型字段用于指示所述 MACSec 帧用于承载所述 ACP 报文。

30 7. 根据权利要求 5 所述的方法, 其特征在于, 所述识别信息携带在所述 MACSec 帧的帧头中的标志位字段中, 所述标志位字段为新增字段或版本字段。

8. 根据权利要求 5 所述的方法, 其特征在于, 所述识别信息携带在所

述 MACSec 帧的帧头中的 MAC 地址字段中。

9. 一种用于报文传输的第一网络设备，应用在自组织网络中，其特征在于，所述第一网络设备包括：

5 建立模块，用于所述第一网络设备根据介质访问控制安全 MACSec 协议，与第二网络设备建立 MACSec 通道；

发送模块，用于所述第一网络设备通过所述建立模块建立的所述 MACSec 通道，向所述第二网络设备发送自组织控制平面 ACP 报文，所述 ACP 报文承载在 MACSec 帧中，所述 MACSec 帧的帧头中携带了用于标识所述 ACP 报文的识别信息。

10 10. 根据权利要求 9 所述的第一网络设备，其特征在于，所述识别信息携带在所述 MACSec 帧的帧头中的以太网类型字段中，所述以太网类型字段用于指示所述 MACSec 帧用于承载所述 ACP 报文。

11. 根据权利要求 9 所述的第一网络设备，其特征在于，所述识别信息携带在所述 MACSec 帧的帧头中的标志位字段中，所述标志位字段为新增字  
15 段或版本字段。

12. 根据权利要求 9 所述的第一网络设备，其特征在于，所述识别信息携带在所述 MACSec 帧的帧头中的 MAC 地址字段中。

13. 一种用于报文传输的第二网络设备，应用在自组织网络中，其特征在于，所述第二网络设备包括：

20 建立模块，用于所述第二网络设备根据介质访问控制安全 MACSec 协议，与第一网络设备建立 MACSec 通道；

接收模块，用于所述第二网络设备通过所述建立模块建立的所述 MACSec 通道，接收所述第一网络设备发送的 MACSec 帧；

25 确定模块，用于所述第二网络设备根据所述接收模块接收的所述 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息，确定所述 ACP 报文。

14. 根据权利要求 13 所述的第二网络设备，其特征在于，所述识别信息携带在所述 MACSec 帧的帧头中的以太网类型字段中，所述以太网类型字段用于指示所述 MACSec 帧用于承载所述 ACP 报文。

30 15. 根据权利要求 13 所述的第二网络设备，其特征在于，所述识别信息携带在所述 MACSec 帧的帧头中的标志位字段中，所述标志位字段为新增

字段或版本字段。

16. 根据权利要求 13 所述的第二网络设备, 其特征在于, 所述识别信息携带在所述 MACSec 帧的帧头中的 MAC 地址字段中。

17. 一种用于报文传输的系统, 应用在自组织网络中, 其特征在于, 所述系统包括: 如权利要求 9 至 12 中任一项所述的第一网络设备, 以及如权利要求 13 至 16 中任一项所述的第二网络设备,

所述第一网络设备根据介质访问控制安全 MACSec 协议, 与所述第二网络设备建立 MACSec 通道;

10 通过所述 MACSec 通道, 所述第一网络设备向所述第二网络设备发送自组织控制平面 ACP 报文, 所述 ACP 报文承载在 MACSec 帧中, 所述 MACSec 帧的帧头中携带了用于标识所述 ACP 报文的识别信息;

所述第二网络设备接收所述 MACSec 帧;

所述第二网络设备根据所述 MACSec 帧的帧头中携带的用于标识自组织控制平面 ACP 报文的识别信息, 确定所述 ACP 报文。

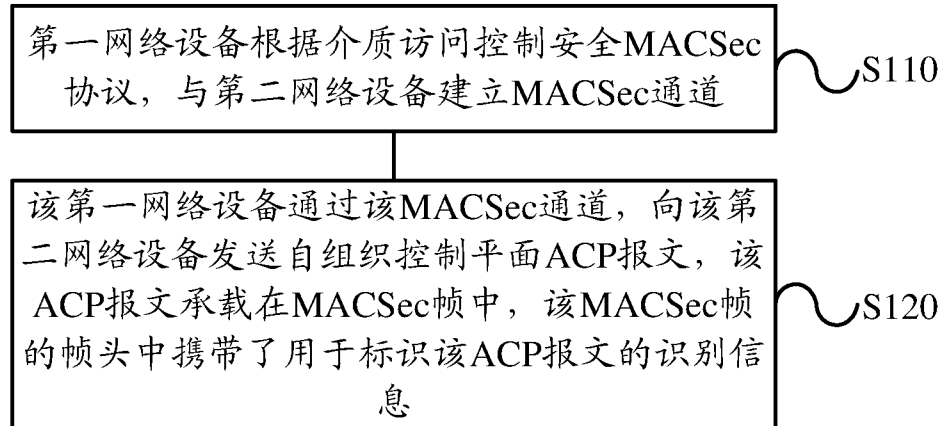
100

图1

|                        |                                |                |                          |                      |         |                                   |                |     |
|------------------------|--------------------------------|----------------|--------------------------|----------------------|---------|-----------------------------------|----------------|-----|
| MAC Header<br>( MAC头 ) | 802.1AE Header<br>( 802.1AE头 ) | 802.1Q<br>VLAN | Type/Length<br>( 类型/长度 ) | IP Header<br>( IP头 ) | TCP/UDP | Higher Layer Protocol<br>( 高层协议 ) | 802.1AE<br>ICV | CRC |
|------------------------|--------------------------------|----------------|--------------------------|----------------------|---------|-----------------------------------|----------------|-----|

图 2

|                                     |     |    |    |    |     |
|-------------------------------------|-----|----|----|----|-----|
| MACSec Ethertype<br>( MACSec以太网类型 ) | TCI | AN | SL | PN | SCI |
|-------------------------------------|-----|----|----|----|-----|

图 3

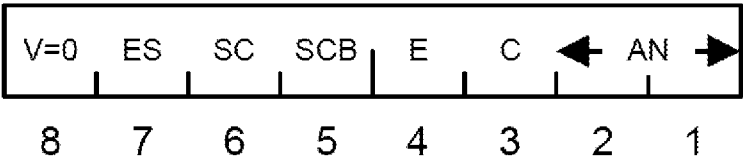


图4

200

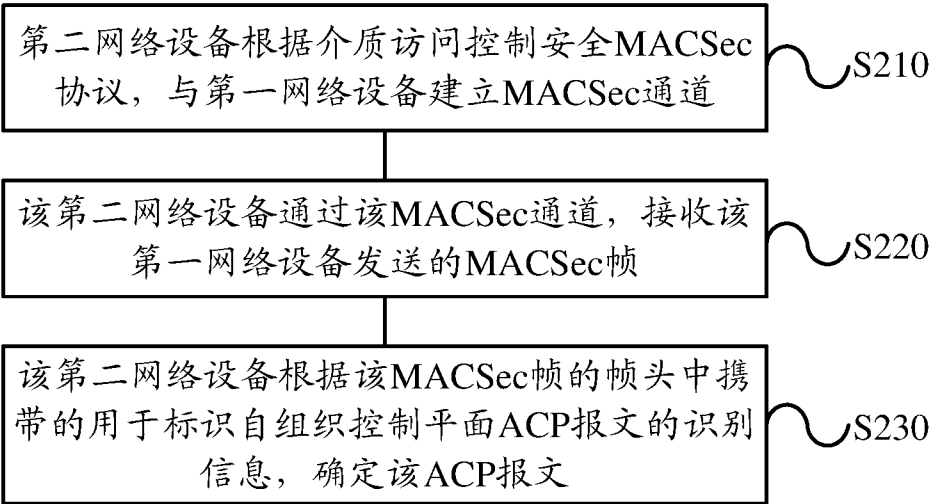


图5

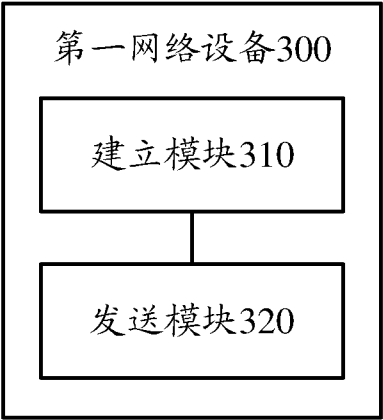


图6

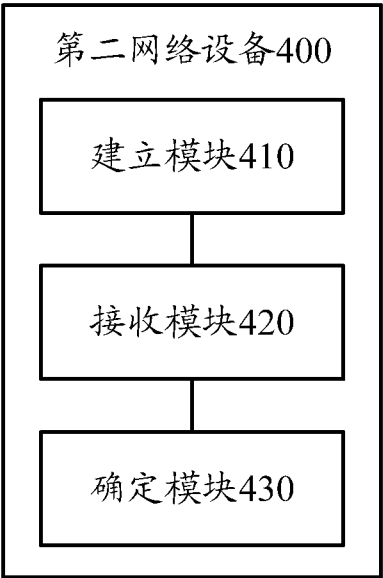


图7

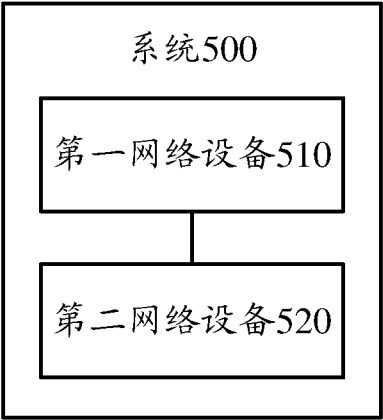


图8

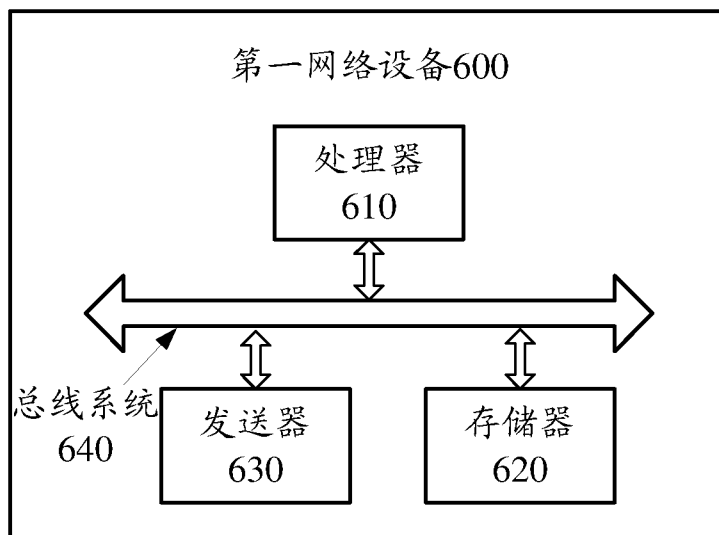


图 9

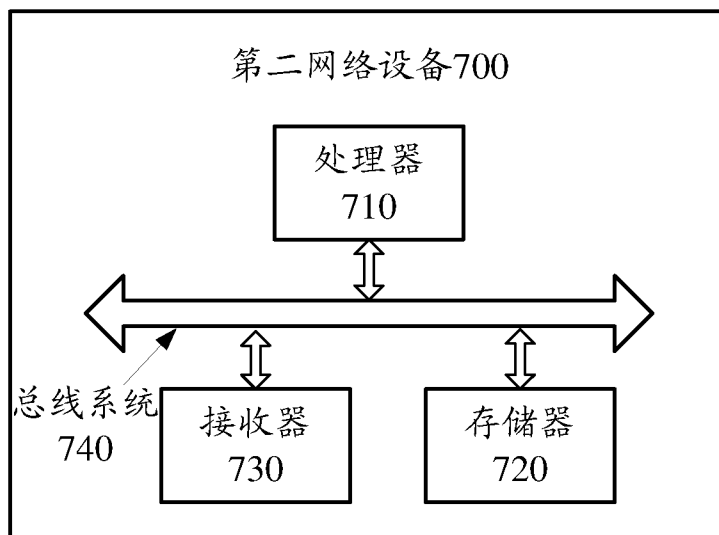


图 10

# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2015/084384**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/70 (2013.01) i; H04L 29/06 (2006.01) i

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

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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

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

VEN, CNTXT, USTXT, CPRSABS, CNKI: data package, media access control, MACSEC, IPSEC, self-organize, control plane, ACP, carry, package, message, frame, safe, key, tunnel, channel, link, autonomic, control, plane, CP, carri+

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                     | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | CN 101193064 A (BROADCOM CORPORATION), 04 June 2008 (04.06.2008), description, paragraphs [0064]-[0088]                | 1-17                  |
| Y         | WO 2014113301 A1 (CISCO TECH INC.), 24 July 2014 (24.07.2014), description, paragraphs [0038]-[0053] and [0067]-[0077] | 1-17                  |
| A         | US 2014192808 A1 (CISCO TECH INC.), 10 July 2014 (10.07.2014), the whole document                                      | 1-17                  |
| A         | CN 104205764 A (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.), 10 December 2014 (10.12.2014), the whole document          | 1-17                  |

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

☒ See patent family annex.

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

|                                                                                                                                                                                                                    |                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Date of the actual completion of the international search<br>12 January 2016 (12.01.2016)                                                                                                                          | Date of mailing of the international search report<br><b>06 February 2016 (06.02.2016)</b> |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br><b>WANG, Guixia</b><br>Telephone No.: (86-10) <b>62411262</b>        |

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.

**PCT/CN2015/084384**

| Patent Documents referred<br>in the Report | Publication Date | Patent Family    | Publication Date  |
|--------------------------------------------|------------------|------------------|-------------------|
| CN 101193064 A                             | 04 June 2008     | CN 101193064 B   | 03 October 2012   |
|                                            |                  | KR 100910818 B1  | 04 August 2009    |
|                                            |                  | EP 1928127 B1    | 15 August 2012    |
|                                            |                  | TW 200840279 A   | 01 October 2008   |
|                                            |                  | US 7729276 B2    | 01 June 2010      |
|                                            |                  | HK 1121883 A1    | 28 June 2013      |
|                                            |                  | KR 20080048972 A | 03 June 2008      |
|                                            |                  | TW I410088 B     | 21 September 2013 |
|                                            |                  | EP 1928127 A1    | 04 June 2008      |
|                                            |                  | US 2008123652 A1 | 29 May 2008       |
| WO 2014113301 A1                           | 24 July 2014     | EP 2946534 A1    | 25 November 2015  |
|                                            |                  | CN 104969517 A   | 07 October 2015   |
|                                            |                  | US 2014201516 A1 | 17 July 2014      |
| US 2014192808 A1                           | 10 July 2014     | None             |                   |
| CN 104205764 A                             | 10 December 2014 | WO 2013147731 A1 | 03 October 2013   |
|                                            |                  | US 2015030029 A1 | 29 January 2015   |
|                                            |                  | EP 2832050 A1    | 04 February 2015  |
|                                            |                  | EP 2832050 A4    | 09 December 2015  |

|                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                        |                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------|
| A. 主题的分类                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                        |                      |
| H04L 12/70(2013.01)i; H04L 29/06(2006.01)i                                                                                                                                                                                                                                                                                                                                                       |                                                                                                        |                      |
| 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                        |                      |
| B. 检索领域                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                        |                      |
| 检索的最低限度文献(标明分类系统和分类号)                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                        |                      |
| H04L                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                        |                      |
| 包含在检索领域中的除最低限度文献以外的检索文献                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                        |                      |
| 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))                                                                                                                                                                                                                                                                                                                                                             |                                                                                                        |                      |
| VEN, CNTXT, USTXT, CPRSABS, CNKI: 报文, 帧, 数据包, 介质访问控制, 安全, 通道, 隧道, 信道, MACSEC, IPSEC, 自主, 自组织, 控制平面, ACP, 携带, 承载, package, message, frame, safe, key, tunnel, channel, link, autonomic, control, plane, CP, carri+,                                                                                                                                                                               |                                                                                                        |                      |
| C. 相关文件                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                        |                      |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                             | 引用文件, 必要时, 指明相关段落                                                                                      | 相关的权利要求              |
| Y                                                                                                                                                                                                                                                                                                                                                                                                | CN 101193064 A (美国博通公司) 2008年 6月 4日 (2008 - 06 - 04)<br>说明书第[0064]-[0088]段                             | 1-17                 |
| Y                                                                                                                                                                                                                                                                                                                                                                                                | WO 2014113301 A1 (CISCO TECH INC) 2014年 7月 24日 (2014 - 07 - 24)<br>说明书第[0038]-[0053]段, 第[0067]-[0077]段 | 1-17                 |
| A                                                                                                                                                                                                                                                                                                                                                                                                | US 2014192808 A1 (CISCO TECH INC) 2014年 7月 10日 (2014 - 07 - 10)<br>全文                                  | 1-17                 |
| A                                                                                                                                                                                                                                                                                                                                                                                                | CN 104205764 A (惠普发展公司, 有限合伙企业) 2014年 12月 10日 (2014 - 12 - 10)<br>全文                                   | 1-17                 |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                             |                                                                                                        |                      |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“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)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“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<br>“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<br>“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<br>“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<br>“&” 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 1月 12日                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                        | 2016年 2月 6日          |
| ISA/CN的名称和邮寄地址                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                        | 授权官员                 |
| 中华人民共和国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088                                                                                                                                                                                                                                                                                                                                               |                                                                                                        | 王桂霞                  |
| 传真号 (86-10)62019451                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                        | 电话号码 (86-10)62411262 |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2015/084384

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |             |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|-------------|----|----------------|
| CN          | 101193064  | A  | 2008年 6月 4日    | CN   | 101193064   | B  | 2012年 10月 3日   |
|             |            |    |                | KR   | 100910818   | B1 | 2009年 8月 4日    |
|             |            |    |                | EP   | 1928127     | B1 | 2012年 8月 15日   |
|             |            |    |                | TW   | 200840279   | A  | 2008年 10月 1日   |
|             |            |    |                | US   | 7729276     | B2 | 2010年 6月 1日    |
|             |            |    |                | HK   | 1121883     | A1 | 2013年 6月 28日   |
|             |            |    |                | KR   | 20080048972 | A  | 2008年 6月 3日    |
|             |            |    |                | TW   | I410088     | B  | 2013年 9月 21日   |
|             |            |    |                | EP   | 1928127     | A1 | 2008年 6月 4日    |
|             |            |    |                | US   | 2008123652  | A1 | 2008年 5月 29日   |
| WO          | 2014113301 | A1 | 2014年 7月 24日   | EP   | 2946534     | A1 | 2015年 11月 25日  |
|             |            |    |                | CN   | 104969517   | A  | 2015年 10月 7日   |
|             |            |    |                | US   | 2014201516  | A1 | 2014年 7月 17日   |
| US          | 2014192808 | A1 | 2014年 7月 10日   | 无    |             |    |                |
| CN          | 104205764  | A  | 2014年 12月 10日  | WO   | 2013147731  | A1 | 2013年 10月 3日   |
|             |            |    |                | US   | 2015030029  | A1 | 2015年 1月 29日   |
|             |            |    |                | EP   | 2832050     | A1 | 2015年 2月 4日    |
|             |            |    |                | EP   | 2832050     | A4 | 2015年 12月 9日   |

表 PCT/ISA/210 (同族专利附件) (2009年7月)