(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113543131 A
(43)申请公布日 2021.10.22

(21)申请号 202110780040.2

(22)申请日 2021.07.09

(71)申请人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 赵乾

(74)专利代理机构 深圳市隆天联鼎知识产权代理有限公司 44232
代理人 王鹏健

(51)Int.Cl.
*H04W 12/06*(2021.01)
*H04L 9/06*(2006.01)
*H04L 9/32*(2006.01)
*H04W 12/0431*(2021.01)
*H04W 12/069*(2021.01)
*H04W 76/10*(2018.01)

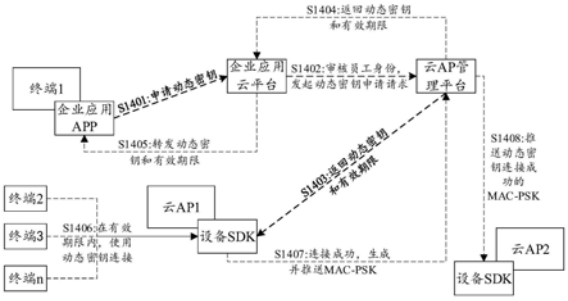
权利要求书3页 说明书17页 附图11页

(54)发明名称

网络连接管理方法、装置、计算机可读介质及电子设备

(57)摘要

本申请的实施例提供了一种网络连接管理方法、装置、计算机可读介质及电子设备。该网络连接管理方法包括:接收用于连接接入点设备的动态密钥;若接收到站点设备发送的包含有所述动态密钥的接入请求,则响应所述接入请求,与所述站点设备建立连接;在与所述站点设备成功建立连接之后,将所述站点设备的物理地址与所述动态密钥进行关联,生成物理地址与动态密钥之间的关联关系;将所述关联关系传递给其它接入点设备,以使所述其它接入点设备根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。本申请实施例的技术方案可以提高站点设备对接入点设备的接入效率。




CN 113543131 A

1.一种网络连接管理方法,其特征在于,包括:

接收用于连接接入点设备的动态密钥;

若接收到站点设备发送的包含有所述动态密钥的接入请求,则响应所述接入请求,与所述站点设备建立连接;

在与所述站点设备成功建立连接之后,将所述站点设备的物理地址与所述动态密钥进行关联,生成物理地址与动态密钥之间的关联关系;

将所述关联关系传递给其它接入点设备,以使所述其它接入点设备根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

2.根据权利要求1所述的网络连接管理方法,其特征在于,接收用于连接接入点设备的动态密钥,包括:

接收接入点管理平台发送的用于连接所述接入点设备的动态密钥;或

接收预配置的用于连接所述接入点设备的动态密钥。

3.根据权利要求1所述的网络连接管理方法,其特征在于,将所述关联关系传递给其它接入点设备,包括:

将所述关联关系发送给接入点管理平台,以使所述接入点管理平台将所述关联关系转发给所述其它接入点设备;或者

将所述关联关系通过与所述其它接入点设备之间的通信链路发送给所述其它接入点设备。

4.根据权利要求1至3中任一项所述的网络连接管理方法,其特征在于,所述网络连接管理方法还包括:接收所述动态密钥的有效期限;

响应所述接入请求,与所述站点设备建立连接,包括:根据所述有效期限确定所述接入请求中包含的动态密钥是否处于所述有效期限内,若确定所述动态密钥处于所述有效期限内,则与所述站点设备建立连接。

5.根据权利要求4所述的网络连接管理方法,其特征在于,所述网络连接管理方法还包括:

将所述动态密钥的有效期限传递给所述其它接入点设备,以使所述其它接入点设备在所述有效期限内根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

6.一种网络连接管理方法,其特征在于,包括:

响应于密钥申请请求,分配用于连接接入点设备的动态密钥;

将所述动态密钥发送给所述接入点设备和所述密钥申请请求的发起方,以使所述接入点设备基于所述动态密钥验证接收到的接入请求;

接收所述接入点设备发送的物理地址与所述动态密钥之间的关联关系,所述物理地址是基于所述动态密钥成功接入所述接入点设备的站点设备所拥有的地址;

将所述关联关系发送给其它接入点设备,以使所述其它接入点设备基于所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

7.根据权利要求6所述的网络连接管理方法,其特征在于,所述网络连接管理方法还包括:

生成所述动态密钥的有效期限;

将所述有效期限发送给所述接入点设备,以使所述接入点设备在所述有效期限内基于

所述动态密钥验证接收到的接入请求。

8.根据权利要求6或7所述的网络连接管理方法，其特征在于，在所述响应于密钥申请请求之前，所述网络连接管理方法还包括：

接收应用程序服务端发送的密钥申请请求，所述密钥申请请求是所述应用程序服务端对发起密钥申请的应用程序客户端的身份验证通过之后发送的。

9.一种网络连接管理方法，其特征在于，包括：

接收物理地址与动态密钥之间的关联关系，所述关联关系是其它接入点设备根据所述动态密钥，以及使用所述动态密钥、且与所述其它接入点成功建立连接的站点设备的物理地址生成的；

若接收到指定设备发送的接入请求，则获取所述指定设备的物理地址和所述接入请求中包含的接入密钥；

根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证。

10.根据权利要求9所述的网络连接管理方法，其特征在于，根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证，包括：

若根据所述关联关系确定所述指定设备的物理地址与所述接入请求中包含的接入密钥相关联，则确定对所述接入请求验证成功；

若所述指定设备的物理地址不存在于所述关联关系中，则拒绝所述接入请求。

11.根据权利要求9或10所述的网络连接管理方法，其特征在于，所述网络连接管理方法还包括：接收所述动态密钥的有效期限；

根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证，包括：在所述有效期限内，根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证。

12.一种网络连接管理装置，其特征在于，包括：

第一接收单元，配置为接收用于连接接入点设备的动态密钥；

第一处理单元，配置为若接收到站点设备发送的包含有所述动态密钥的接入请求，则响应所述接入请求，与所述站点设备建立连接；

第一生成单元，配置为在与所述站点设备成功建立连接之后，将所述站点设备的物理地址与所述动态密钥进行关联，生成物理地址与动态密钥之间的关联关系；

传输单元，配置为将所述关联关系传递给其它接入点设备，以使所述其它接入点设备根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

13.一种网络连接管理装置，其特征在于，包括：

分配单元，配置为响应于密钥申请请求，分配用于连接接入点设备的动态密钥；

第一发送单元，配置为将所述动态密钥发送给所述接入点设备和所述密钥申请请求的发起方，以使所述接入点设备基于所述动态密钥验证接收到的接入请求；

第二接收单元，配置为接收所述接入点设备发送的物理地址与所述动态密钥之间的关联关系，所述物理地址是基于所述动态密钥成功接入所述接入点设备的站点设备所拥有的地址；

第二发送单元，配置为将所述关联关系发送给其它接入点设备，以使所述其它接入点设备基于所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

14.一种计算机可读介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至11中任一项所述的网络连接管理方法。

15.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器实现如权利要求1至11中任一项所述的网络连接管理方法。

# 网络连接管理方法、装置、计算机可读介质及电子设备

## 技术领域

[0001] 本申请涉及计算机及通信技术领域，具体而言，涉及一种网络连接管理方法、装置、计算机可读介质及电子设备。

## 背景技术

[0002] 随着WLAN(Wireless Local Area Network，无线局域网)技术的发展，在一些应用场景中，需要有大量的站点设备(即Station，STA)来接入AP(Access Point，接入点)，比如企业级WLAN，在这种应用场景中，如何能够有效实现对站点设备的网络连接管理是亟待解决的技术问题。

## 发明内容

[0003] 本申请的实施例提供了一种网络连接管理方法、装置、计算机可读介质及电子设备，进而至少在一定程度上可以提高站点设备对接入点设备的接入效率。

[0004] 本申请的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本申请的实践而习得。

[0005] 根据本申请实施例的一个方面，提供了一种网络连接管理方法，包括：接收用于连接接入点设备的动态密钥；若接收到站点设备发送的包含有所述动态密钥的接入请求，则响应所述接入请求，与所述站点设备建立连接；在与所述站点设备成功建立连接之后，将所述站点设备的物理地址与所述动态密钥进行关联，生成物理地址与动态密钥之间的关联关系；将所述关联关系传递给其它接入点设备，以使所述其它接入点设备根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0006] 根据本申请实施例的一个方面，提供了一种网络连接管理方法，包括：响应于密钥申请请求，分配用于连接接入点设备的动态密钥；将所述动态密钥发送给所述接入点设备和所述密钥申请请求的发起方，以使所述接入点设备基于所述动态密钥验证接收到的接入请求；接收所述接入点设备发送的物理地址与所述动态密钥之间的关联关系，所述物理地址是基于所述动态密钥成功接入所述接入点设备的站点设备所拥有的地址；将所述关联关系发送给其它接入点设备，以使所述其它接入点设备基于所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0007] 根据本申请实施例的一个方面，提供了一种网络连接管理方法，包括：接收物理地址与动态密钥之间的关联关系，所述关联关系是其它接入点设备根据所述动态密钥，以及使用所述动态密钥、且与所述其它接入点成功建立连接的站点设备的物理地址生成的；若接收到指定设备发送的接入请求，则获取所述指定设备的物理地址和所述接入请求中包含的接入密钥；根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证。

[0008] 根据本申请实施例的一个方面，提供了一种网络连接管理装置，包括：第一接收单元，配置为接收用于连接接入点设备的动态密钥；第一处理单元，配置为若接收到站点设备

发送的包含有所述动态密钥的接入请求，则响应所述接入请求，与所述站点设备建立连接；第一生成单元，配置为在与所述站点设备成功建立连接之后，将所述站点设备的物理地址与所述动态密钥进行关联，生成物理地址与动态密钥之间的关联关系；传输单元，配置为将所述关联关系传递给其它接入点设备，以使所述其它接入点设备根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0009] 在本申请的一些实施例中，基于前述方案，所述第一接收单元配置为：接收接入点管理平台发送的用于连接所述接入点设备的动态密钥；或接收预配置的用于连接所述接入点设备的动态密钥。

[0010] 在本申请的一些实施例中，基于前述方案，所述传输单元配置为：将所述关联关系发送给接入点管理平台，以使所述接入点管理平台将所述关联关系转发给所述其它接入点设备；或者

[0011] 将所述关联关系通过与所述其它接入点设备之间的通信链路发送给所述其它接入点设备。

[0012] 在本申请的一些实施例中，基于前述方案，所述第一接收单元还配置为：接收所述动态密钥的有效期限；所述第一处理单元配置为：根据所述有效期限确定所述接入请求中包含的动态密钥是否处于所述有效期限内，若确定所述动态密钥处于所述有效期限内，则与所述站点设备建立连接。

[0013] 在本申请的一些实施例中，基于前述方案，所述传输单元还配置为：将所述动态密钥的有效期限传递给所述其它接入点设备，以使所述其它接入点设备在所述有效期限内根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0014] 根据本申请实施例的一个方面，提供了一种网络连接管理装置，包括：分配单元，配置为响应于密钥申请请求，分配用于连接接入点设备的动态密钥；第一发送单元，配置为将所述动态密钥发送给所述接入点设备和所述密钥申请请求的发起方，以使所述接入点设备基于所述动态密钥验证接收到的接入请求；第二接收单元，配置为接收所述接入点设备发送的物理地址与所述动态密钥之间的关联关系，所述物理地址是基于所述动态密钥成功接入所述接入点设备的站点设备所拥有的地址；第二发送单元，配置为将所述关联关系发送给其它接入点设备，以使所述其它接入点设备基于所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0015] 在本申请的一些实施例中，基于前述方案，所述网络连接管理装置还包括：第二生成单元，配置为生成所述动态密钥的有效期限；所述第一发送单元还配置为将所述有效期限发送给所述接入点设备，以使所述接入点设备在所述有效期限内基于所述动态密钥验证接收到的接入请求。

[0016] 在本申请的一些实施例中，基于前述方案，所述分配单元还配置为：在所述响应于密钥申请请求之前，接收应用程序服务端发送的密钥申请请求，所述密钥申请请求是所述应用程序服务端对发起密钥申请的应用程序客户端的身份验证通过之后发送的。

[0017] 根据本申请实施例的一个方面，提供了一种网络连接管理装置，包括：第三接收单元，配置为接收物理地址与动态密钥之间的关联关系，所述关联关系是其它接入点设备根据所述动态密钥，以及使用所述动态密钥、且与所述其它接入点成功建立连接的站点设备的物理地址生成的；获取单元，配置为若接收到指定设备发送的接入请求，则获取所述指定

设备的物理地址和所述接入请求中包含的接入密钥;验证单元,配置为根据所述关联关系、所述指定设备的物理地址,以及所述接入请求中包含的接入密钥,对所述接入请求进行验证。

[0018] 在本申请的一些实施例中,基于前述方案,所述验证单元配置为:若根据所述关联关系确定所述指定设备的物理地址与所述接入请求中包含的接入密钥相关联,则确定对所述接入请求验证成功;

[0019] 若所述指定设备的物理地址不存在于所述关联关系中,则拒绝所述接入请求。

[0020] 在本申请的一些实施例中,基于前述方案,所述第三接收单元还配置为:接收所述动态密钥的有效期限;所述验证单元配置为:在所述有效期限内,根据所述关联关系、所述指定设备的物理地址,以及所述接入请求中包含的接入密钥,对所述接入请求进行验证。

[0021] 根据本申请实施例的一个方面,提供了一种计算机可读介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现如上述实施例中所述的网络连接管理方法。

[0022] 根据本申请实施例的一个方面,提供了一种电子设备,包括:一个或多个处理器;存储装置,用于存储一个或多个程序,当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器实现如上述实施例中所述的网络连接管理方法。

[0023] 根据本申请实施例的一个方面,提供了一种计算机程序产品或计算机程序,该计算机程序产品或计算机程序包括计算机指令,该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令,处理器执行该计算机指令,使得该计算机设备执行上述各种可选实施例中提供的网络连接管理方法。

[0024] 在本申请的一些实施例所提供的技术方案中,接入点设备接收用于连接接入点设备的动态密钥,然后在接收到站点设备发送的包含有该动态密钥的接入请求时,响应该接入请求与站点设备建立连接,并在与站点设备成功建立连接之后,将站点设备的物理地址与动态密钥进行关联,生成物理地址与动态密钥之间的关联关系,然后将该关联关系传递给其它接入点设备,以使其它接入点设备根据该关联关系验证站点设备基于动态密钥发起的接入请求。可见,本申请实施例的技术方案使得在站点设备通过动态密钥接入接入点设备之后,接入点设备可以将站点设备的物理地址与该动态密钥进行关联,进而传递给其它接入点设备,以便于该站点设备方便快捷地接入其它接入点设备,提高了站点设备接入其它接入点设备的效率。

[0025] 应当理解的是,以上的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本申请。

## 附图说明

[0026] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本申请的实施例,并与说明书一起用于解释本申请的原理。显而易见地,下面描述中的附图仅仅是本申请的一些实施例,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。在附图中:

[0027] 图1示出了WPA/WPA2-PSK认证的示意图;

[0028] 图2示出了WPA/WPA2-PPSK认证的示意图;

[0029] 图3示出了STA与AP之间建立连接的流程图;

[0030] 图4示出了STA与AP之间的四次握手认证示意图；

[0031] 图5示出了STA与AP认证过程中的密钥生成示意图；

[0032] 图6示出了Portal认证的配置界面示意图；

[0033] 图7示出了根据本申请的一个实施例的网络连接管理方法的流程图；

[0034] 图8示出了根据本申请的一个实施例的网络连接管理方法的流程图；

[0035] 图9示出了根据本申请的一个实施例的网络连接管理方法的流程图；

[0036] 图10示出了根据本申请的一个实施例的云AP的场景示意图；

[0037] 图11示出了根据本申请的一个实施例的云AP场景的系统架构图；

[0038] 图12示出了根据本申请的一个实施例的网络连接管理方法的流程图；

[0039] 图13示出了根据本申请的一个实施例的一键联网的界面示意图；

[0040] 图14示出了根据本申请的一个实施例的网络连接管理方法的流程图；

[0041] 图15示出了根据本申请的一个实施例的功能选择界面示意图；

[0042] 图16示出了根据本申请的一个实施例的网络连接管理装置的框图；

[0043] 图17示出了根据本申请的一个实施例的网络连接管理装置的框图；

[0044] 图18示出了根据本申请的一个实施例的网络连接管理装置的框图；

[0045] 图19示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

## 具体实施方式

[0046] 现在参考附图以更全面的方式描述示例实施方式。然而，示例的实施方式能够以各种形式实施，且不应被理解为仅限于这些范例；相反，提供这些实施方式的目的是使得本申请更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。

[0047] 此外，本申请所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。在下面的描述中，有许多具体细节从而可以充分理解本申请的实施例。然而，本领域技术人员应意识到，在实施本申请的技术方案时可以不需用到实施例中的所有细节特征，可以省略一个或更多特定细节，或者可以采用其它的方法、元件、装置、步骤等。

[0048] 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0049] 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

[0050] 需要说明的是：在本文中提及的“多个”是指两个或两个以上。“和/或”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。字符“/”一般表示前后关联对象是一种“或”的关系。

[0051] WPA全名为Wi-Fi Protected Access(Wi-Fi网络安全接入)，有WPA、WPA2和WPA3三个标准，是一种保护无线网络安全的系统。WPA/WPA2-PSK(Pre-Shared Key，预共享密钥)是预分配共享密钥的认证方式，在加密方式和密钥的验证方式上的安全性更高。如图1所示，采用WPA/WPA2-PSK认证时，对于连接到接入点设备101的指定SSID(Service Set Identifier，服务集标识)的所有站点设备，接入密钥是相同的，比如站点设备102和站点设

备103的PSK都是“12345”。

[0052] WPA/WPA2-PPSK(Private PSK,私有的PSK)认证继承了WPA/WPA2-PSK认证的优点,部署简单,同时还可以实现对不同的站点设备提供不同的预共享密钥,有效提升了网络的安全性。在使用WPA/WPA2-PPSK认证时,连接到同一个SSID的站点设备可以有不同的接入密钥,根据不同的用户可以下发不同的授权,并且如果一个用户拥有多个站点设备,这些站点设备也可以通过同一个PPSK账号连接到网络。具体如图2所示,连接到接入点设备201的同一SSID的站点设备202与站点设备203可以使用相同的PSK,而站点设备204可以使用与站点设备202和站点设备203不相同的PSK。

[0053] 不管是WPA/WPA2-PSK方式,还是WPA/WPA2-PPSK方式,在STA与AP之间的连接过程以及秘钥协商流程是一致的。

[0054] 如图3所示,站点设备STA与接入点设备AP之间建立连接的过程主要包括:

[0055] 步骤S301,扫描阶段(SCAN)。

[0056] 具体地,STA使用Scanning来搜索AP,当STA漫游时寻找连接一个新的AP时,STA会在每个可用的信道上进行搜索。搜索方式有主动搜索(Active Scanning)和被动搜索(Passive Scanning)两种。

[0057] 主动搜索是STA依次在每个信道(1-13信道)发出Probe Request(探测请求)帧,寻找与STA所属有相同SSID的AP,若找不到相同SSID的AP,则一直扫描下去。主动搜索的特点是可以迅速搜索到AP。

[0058] 被动搜索是STA通过侦听AP定期发送的Beacon(信标)帧来发现网络,该帧提供了AP及所在BSS(Basic Service Set,基本服务集)的相关信息。被动搜索的方式虽然搜索到AP需要花费较多的时间,但是可以降低STA的功耗。

[0059] 步骤S302,认证阶段(Authentication)。

[0060] 具体地,当STA找到与其有相同SSID的AP之后,在SSID匹配的AP中,根据收到的AP信号强度,选择一个信号最强的AP,然后进入认证阶段,只有身份认证通过的STA才能进行无线接入访问。AP提供的认证方法包括:开放式认证(open-system authentication)、共享密钥认证(shared-key authentication)、预先身份认证(WPA PSK)等。

[0061] 其中,开放式认证的过程是STA发起认证请求,认证服务器收到后回应。共享密钥认证的过程是STA发起认证请求,认证服务器收到请求后回复质询文本,STA利用预置的key加密明文发送给认证服务器,认证服务器用预置的key解密并和之前的明文比较,如一致则认证通过。

[0062] 步骤S303,关联阶段(Association)。

[0063] 具体地,当AP向STA返回认证响应信息,STA身份认证获得通过后之后,进入关联阶段。在关联阶段中,STA向AP发送关联请求,AP向STA返回关联响应。当STA移动时就涉及到漫游问题,如果是在同一组网下漫游就无需重新认证而只需要重新关联。当AP与STA关联完成之后,STA的接入过程才完成,即STA与AP之间连接成功。

[0064] 在进行数据传输之前,STA与AP之间需要进行基于EAPOL(Extensible Authentication Protocol OVER LAN,基于局域网的扩展认证协议)的四次握手过程来产生所需要的密钥。具体过程如图4所示,STA作为请求方(Supplicant),AP作为认证方(Authenticator)来进行四次握手过程。

[0065] 在四次握手过程中，消息1是由认证方通过单播方式向请求方发送一个携带A-Nonce的EAPOL-Key帧。其中，A-Nonce是由认证方生成的一个随机数。

[0066] 请求方在接收到消息1之后，由于请求方已经获得的A-Nonce和AA(Authenticator MAC地址，即认证方的MAC地址)，同时请求方已经拥有了PMK(Pairwise Master Key，即成对主密钥，通常是一组随机数)和SPA(即请求方的MAC地址)，所以可以通过下面的函数计算出PTK(Pairwise Transient Key，成对临时密钥)：

[0067] PTK＝PRF(PMK+A-Nonce+S-Nonce+AA+SPA)

[0068] 其中，PRF表示pseudorandom function，即伪随机函数；S-Nonce是请求方生成的随机数；公式中的PMK是请求方自己设置的。生成的PTK包含3个部分：KCK(Key Confirmation Key，密钥确认密钥)、KEK(Key Encryption Key，密钥加密密钥)和TK(Temporal Key，临时密钥)。KCK用来计算密钥生成消息的完整性，KEK用来加密密钥生成消息，TK是真正用来进行数据加密的。

[0069] 在四次握手过程中，消息2是请求方在生成PTK之后，将S-Nonce、MIC(message integrity code，即消息完整性校验码，是针对一组需要保护的数据计算出的散列值，用来防止数据遭篡改)等信息通过第二个EAPOL-Key帧发送给认证方。其中，消息2中的MIC值会被KCK(Key Confirmation Key，密钥确认密钥)加密。

[0070] 认证方接收到消息2之后，取出消息2中的S-Nonce，也将进行和请求方中类似的计算来验证请求方返回的消息是否正确，具体是将收到的MIC和自己生成的MIC进行完整性校验。如果不正确，即对MIC完整性校验失败，则表明请求方PMK错误，于是整个握手工作就此停止。

[0071] 如果认证方验证请求方返回的消息正确，则认证方生成PTK和GTK(Group Temporal Key，组临时密钥)。GTK是用于加密组播和广播数据流的加密密钥。

[0072] 在四次握手过程中，消息3是认证方在生成PTK和GTK之后，向请求方发送第三个EAPOL-Key帧，其中携带有GTK和MIC。其中，GTK通过KEK进行加密，MIC通过KCK进行加密。

[0073] 请求方在接收到消息3之后，也将做一些计算以判断认证方的PMK是否正确。如果确认无误，则请求方通过消息4最后一次发送EAPOL-Key帧给认证方进行确认，如果认证成功，则请求方和认证方都安装(Install)密钥，安装(Install)的意思是指使用密钥来对数据进行加密。具体地，请求方安装PTK和GTK，认证方安装PTK。

[0074] 当请求方和认证方完成认证以后，认证方的控制端口将会被打开，这样802.11的数据帧将能够正常传输，而且所有的单播数据帧将会被PTK加密进行保护，所有的组播数据以及广播数据将会被GTK进行加密保护。

[0075] 在认证过程中的密钥生成过程如图5所示，PMK是由ESSID(Extended Service Set Identifier，服务区别号)和PSK生成的，比如通过SHA-1(Secure Hash Algorithm 1，安全散列算法1)算法来生成PMK。PTK是根据四次握手中获取的请求方MAC(即STA MAC)、认证方的MAC(可以通过BSSID来表示)、PMK、A-Nonce和S-Nonce来生成的。之后可以通过PTK来对密文和MIC进行加密。加密时可以采用AES(Advanced Encryption Standard，高级加密标准)或者TKIP(Temporal Key Integrity protocol，临时密钥完整性协议)的方式。

[0076] 在企业WLAN中，使用较多的是WPA/WPA2-PPSK认证，这样使得每个用户都可以有不同的密钥，并且配置和部署简单。但是这种方式需要将每个用户的密钥都保存在接入认证

设备上,即接入认证设备上需要单独存储密钥列表,如果密钥列表中的密钥数量较多,那么在校验用户输入的密钥时则会极大增加验证时间。同时,如果密钥数量较多,那么在有恶意设备故意输入错误密钥进行攻击时,会导致接入认证设备无法工作的问题,并且这种方式也难以避免密钥混用的现象。

[0077] 此外,在相关技术中,也有采用Portal认证的方式,Portal是作为网关服务于因特网的一种WEB站点,Wi-Fi提供方需要先对Portal认证进行配置,具体配置界面如图6所示,需要设置Portal URL(Uniform Resource Locator,统一资源定位器)、认证Key、认证Secret、认证URL、白名单、Check URL、网络类型等。在配置完成之后,用户可以连接上无密码的Wi-Fi,然后通过浏览器弹出portal认证界面,填入认证的用户名和密码之后,才能真正通过Wi-Fi网络进行上网。这种认证方案不仅操作繁琐,而且Portal认证还存在兼容性问题,有些终端(如某些厂商的手机)连接上Wi-Fi后,有可能无法弹出portal认证的页面,进而导致无法进行认证。

[0078] 基于上述问题,本申请实施例提供了一种新的网络连接管理方案,可以将待接入设备的接入密钥与物理地址进行关联,使得在接入点设备验证接入请求时,一方面可以验证待接入设备的物理地址是否存在于该关联关系中,避免了恶意设备频繁发起接入请求而影响接入点设备的性能,另一方面可以在待接入设备的物理地址存在于该关联关系中时,根据该物理地址对应的接入密钥快速验证接入请求中包含的接入密钥,提高了网络接入验证的效率,同时还可以避免接入密钥混用的问题。

[0079] 此外,在一些场景中,同一个用户可能具有多个站点设备,但是有些设备可能无法呈现便捷的、功能丰富的可视化界面来接入网络,比如打印机设备、扫描仪设备等。对于这种情况,如何能够保证这些设备便捷地接入网络是迫切的需求。本申请的实施例针对这种场景,提出了可以向这类站点设备分配动态密钥,待这类站点设备基于动态密钥接入网络之后,接入点设备可以将这类站点的物理地址与动态密钥进行关联,并发送给其它接入点设备,进而当这类站点设备移动到其它接入点设备所在的位置时,可以实现高效的网络接入。具体实现细节详细说明如下:

[0080] 图7示出了根据本申请的一个实施例的网络连接管理方法的流程图,该网络连接管理方法可以由接入点设备来执行。参照图7所示,该网络连接管理方法至少包括步骤S710至步骤S740,详细介绍如下:

[0081] 在步骤S710中,接收用于连接接入点设备的动态密钥。

[0082] 在本申请的一个实施例中,接入点设备可以接收接入点管理平台发送的用于连接接入点设备的动态密钥。在这种情况下,接入点管理平台可以针对用户发起的密钥申请请求来分配动态密钥,在分配动态密钥之后,可以将该动态密钥一方面返回给用户,另一方面返回给接入点设备。

[0083] 可选地,用户可以在应用程序客户端上发起密钥申请请求,进而应用程序客户端可以将该密钥申请请求发送给应用程序服务端,然后由应用程序服务端转发给接入点管理平台。在这种情况下,接入点管理平台在生成动态密钥之后,可以将动态密钥发送给应用程序服务端,然后由应用程序服务端反馈给应用程序客户端。

[0084] 在本申请的一个实施例中,接入点设备也可以接收预配置的用于连接接入点设备的动态密钥。在这种情况下,用户也需要获取到该预配置的动态密钥,以便于向接入点设备

发起连接。

[0085] 在本申请的一个实施例中，该动态密钥还可以具有有效期限，在这种情况下，接入点设备还需要接收该动态密钥的有效期限，以基于该有效期限进行接入管理。该实施例的技术方案也使得能够通过有效期限来对动态密钥进行管理，避免了动态密钥无期限使用而导致接入管理混乱的问题。

[0086] 在步骤S720中，若接收到站点设备发送的包含有动态密钥的接入请求，则响应该接入请求，与站点设备建立连接。

[0087] 在本申请的一个实施例中，用户在获取到动态密钥之后，对于将该动态密钥提供给站点设备，然后由站点设备发起接入请求。比如用户可以通过智能手机与该站点设备(如打印机设备、扫描仪设备等)建立蓝牙连接，然后将该动态密钥输入至智能手机提供的界面中，进而由该智能手机将该动态密钥传递给该站点设备。或者用户可以在站点设备提供的界面中来输入该动态密钥，进而由该站点设备基于该动态密钥发起接入请求。

[0088] 可选地，如果动态密钥具有有效期限，那么接入点设备需要根据该有效期限确定接入请求中包含的动态密钥是否处于有效期限内，如果处于有效期限内，且接入请求中包含的动态密钥与接入点设备事先接收到的动态密钥相匹配，那么接入点设备才会与站点设备建立连接。

[0089] 在步骤S730中，在与站点设备成功建立连接之后，将站点设备的物理地址与动态密钥进行关联，生成物理地址与动态密钥之间的关联关系。

[0090] 在本申请的一个实施例中，站点设备的物理地址可以是MAC(Media Access Control，媒体介入控制)地址。可选地，为了提高动态密钥的查询效率，可以根据动态密钥与物理地址之间的关联关系来生成哈希表，即可以通过哈希表的形式来体现物理地址与动态密钥之间的关联关系。

[0091] 在步骤S740中，将物理地址与动态密钥之间的关联关系传递给其它接入点设备，以使其它接入点设备根据该关联关系验证站点设备基于动态密钥发起的接入请求。

[0092] 在本申请的一个实施例中，接入点设备可以将关联关系发送给接入点管理平台，以使接入点管理平台将关联关系转发给其它接入点设备。

[0093] 在本申请的一个实施例中，接入点设备也可以将关联关系通过与其它接入点设备之间的通信链路发送给其它接入点设备。该实施例的技术方案适用于接入点设备之间建立有通信链路的应用场景。

[0094] 可选地，如果动态密钥具有有效期限，那么接入点设备需要将该动态密钥的有效期限传递给其它接入点设备，以使其它接入点设备在有效期限内根据关联关系验证站点设备基于动态密钥发起的接入请求。

[0095] 图7是从接入点设备的角度对本申请实施例的技术方案进行的阐述，以下从接入点管理平台的角度对本申请实施例的技术方案进行说明：

[0096] 图8示出了根据本申请的一个实施例的网络连接管理方法的流程图，该网络连接管理方法可以由接入点管理平台来执行，该接入点管理平台可以是用于进行接入管理的平台。参照图8所示，该网络连接管理方法至少包括步骤S810至步骤S840，详细介绍如下：

[0097] 在步骤S810中，响应于密钥申请请求，分配用于连接接入点设备的动态密钥。

[0098] 在本申请的一个实施例中，密钥申请请求可以是用户的终端设备发起的，比如用

户具有多个终端设备，但是有些终端设备无法便捷地接入网络，如打印机设备、扫描仪设备等，在这种情况下，用户可以使用智能手机来向接入点管理平台发起密钥申请请求，以基于接入点管理平台反馈的动态密钥来使其它终端设备接入网络。

[0099] 可选地，用户的终端设备可以直接与接入点管理平台建立连接，以发起密钥申请请求。或者用户的终端设备也可以通过指定的应用程序来向接入点管理平台发起密钥申请请求，比如用户可以在应用程序客户端上发起密钥申请请求，进而应用程序客户端可以将该密钥申请请求发送给应用程序服务端，然后由应用程序服务端转发给接入点管理平台。在这种情况下，接入点管理平台在生成动态密钥之后，可以将动态密钥发送给应用程序服务端，然后由应用程序服务端反馈给应用程序客户端。

[0100] 可选地，接入点管理平台还可以生成动态密钥的有效期限，然后将动态密钥的有效期限发送给接入点设备，以使接入点设备在有效期限内基于动态密钥验证接收到的接入请求。

[0101] 在步骤S820中，将动态密钥发送给接入点设备和密钥申请请求的发起方，以使接入点设备基于动态密钥验证接收到的接入请求。

[0102] 可选地，接入点设备在接收到接入点管理平台发送的动态密钥之后，如果接收到接入请求，则可以验证接入请求中的动态密钥与接入点设备从接入点管理平台获取到的动态密钥是否匹配，如果匹配，则可以确定对该接入请求验证通过。如果动态密钥具有有效期限，那么接入点设备还需要确定该动态密钥是否处于有效期限内，如果不在有效期限内，那么使用该动态密钥的接入请求将无法验证通过。

[0103] 在步骤S830中，接收接入点设备发送的物理地址与动态密钥之间的关联关系，该物理地址是基于动态密钥成功接入接入点设备的站点设备所拥有的地址。

[0104] 可选地，接入点设备生成动态密钥与物理地址之间的关联关系的过程可以参照前述实施例的技术方案，不再赘述。

[0105] 在步骤S840中，将物理地址与动态密钥之间的关联关系发送给其它接入点设备，以使其它接入点设备基于该关联关系验证站点设备基于动态密钥发起的接入请求。

[0106] 在本申请的实施例中，通过将物理地址与动态密钥之间的关联关系发送给其它接入点设备，使得站点设备在移动到其它接入点设备的覆盖区域内时，其它接入点设备可以基于该物理地址与动态密钥之间的关联关系快速实现对站点设备的接入验证，有效提高了接入网络的效率。

[0107] 以下从接收到物理地址与动态密钥之间的关联关系的接入点设备的角度来对本申请实施例的技术方案进行说明：

[0108] 图9示出了根据本申请的一个实施例的网络连接管理方法的流程图，该网络连接管理方法可以由接入点设备来执行。参照图9所示，该网络连接管理方法至少包括步骤S910至步骤S930，详细介绍如下：

[0109] 在步骤S910中，接收物理地址与动态密钥之间的关联关系，该关联关系是其它接入点设备根据动态密钥，以及使用动态密钥、且与其它接入点成功建立连接的站点设备的物理地址生成的。

[0110] 可选地，接入点设备生成物理地址与动态密钥之间的关联关系的过程可以参照前述实施例，不再赘述。

[0111] 在本申请的一个实施例中，接入点设备可以直接接收其它接入点设备发送过来的物理地址与动态密钥之间的关联关系，也可以接收接入点管理平台转发过来的物理地址与动态密钥之间的关联关系。

[0112] 在步骤S920中，若接收到指定设备发送的接入请求，则获取指定设备的物理地址和接入请求中包含的接入密钥。

[0113] 在本申请的实施例中，指定设备是需要接入接入点设备的站点设备。由于指定设备在向接入点设备发送接入请求之前已经与接入点设备进行通信，因此指定设备的物理地址可以是在指定设备发送接入请求就已经获取到的。当然，指定设备也可以在接入请求中再次携带其物理地址。

[0114] 在步骤S930中，根据物理地址与动态密钥之间的关联关系、指定设备的物理地址，以及接入请求中包含的接入密钥，对接入请求进行验证。

[0115] 在本申请的一个实施例中，如果根据物理地址与动态密钥之间的关联关系确定指定设备的物理地址与接入请求中包含的接入密钥相关联，则确定对接入请求验证成功。具体地验证过程可以是：接入点设备根据指定设备的物理地址在上述关联关系中查找到对应的动态密钥，然后将查找到的动态密钥与接入请求主动包含的接入密钥进行比对，若一致，则确定对接入请求验证成功。

[0116] 在本申请的一个实施例中，如果指定设备的物理地址不存在于上述的关联关系中，则拒绝该接入请求。该实施例的技术方案可以避免恶意设备频繁发起连接请求而导致接入点设备无法正常工作的情况发生。

[0117] 可选地，接入点设备还可以接收动态密钥的有效期限，进而可以在该有效期限内，根据关联关系、指定设备的物理地址，以及接入请求中包含的接入密钥，对接入请求进行验证。

[0118] 前述实施例中分别从接入点管理平台和接入点设备的角度对本申请实施例的技术方案进行了阐述，以下从各个设备之间进行交互的角度对本申请实施例的实现细节进行详细说明。

[0119] 在本申请的一个应用场景中，接入点设备可以是云AP，云AP是将本地AP的管理能力扩展到云端，通过云端(云AP管理平台，即前述实施例中的接入点管理平台)对多个云AP进行统一的管理，比如配置云AP的LAN、WAN(Wide Area Network，广域网)以及黑白名单等。云AP的场景如图10所示，云AP管理平台通过Internet或者WLAN直接与云AP进行通信，或者云AP管理平台通过Internet或者WLAN经过防火墙和交换机与云AP进行通信，云AP用于与无线终端进行通信交互。

[0120] 云AP的场景的系统架构如图11所示，主要包含三个部分：云AP硬件、云AP管理平台和应用程序。

[0121] 云AP硬件主要包含一个或多个云AP，云AP需要与云AP管理平台进行连接(具体可以通过多端口的转发器HUB来进行连接)，并且接收云AP管理平台发送的AP配置信息，同时接收PPSK的秘钥下发和管理，接收和管理终端(即站点设备)的连接信息。

[0122] 云AP管理平台包含了运营平台、HUB、设备管理、企业配置、通讯录、密钥管理、数据库等几部分。

[0123] 其中，运营平台用于管理云端任务调度、监控异常情况等；HUB负责与云AP硬件进

行连接,维持相关的心跳;设备管理主要用于管理连接的云AP的信息;企业配置主要用于管理每个企业相关的云AP配置;通信录主要用于记录企业员工的信息,包括手机号或者即时通信软件的账号信息等;秘钥管理用于生成、销毁和更新密钥,同时用于给企业分配MAC-PSK哈希表;应用服务用于给应用程序提供相应的API(Application Programming Interface,应用程序接口)接口信息等;数据库作为基础组件,用于对数据进行持久化存储。

[0124] 应用程序主要是指云AP对应的应用程序,包括前端的管理页面和应用信息,后端的平台和服务能力等。可选地,该应用程序可以是寄宿程序,寄宿程序是依赖于宿主环境而存在的程序,比如小程序、快应用等。

[0125] 基于图11所示的系统架构,在本申请的一个实施例中,可以通过图12所示的流程来实现网络接入管理,具体包括如下步骤:

[0126] 步骤S1201,企业应用APP推送终端MAC地址和当前企业信息至企业应用云平台。

[0127] 需要说明的是,企业应用APP可以是针对某个企业单独开发的APP,或者可以是面向所有企业的一个公共平台。如果企业应用APP是面向所有企业的公共平台,那么企业用户需要在该公共平台上创建企业信息,并将该企业的云AP与该企业信息进行绑定,同时在云AP上进行配置,比如配置SSID等。

[0128] 当企业员工的终端上安装了企业应用APP并进入自身所属的企业之后,企业应用APP可以收集终端的MAC地址,然后将这些信息推送给企业应用云平台。

[0129] 步骤S1202,企业应用云平台推送MAC地址和企业员工绑定关系至云AP管理平台。

[0130] 在本申请的一个实施例中,企业员工可以是企业员工的工号、姓名等信息,也可以是企业员工在企业应用APP中的账户名等信息。可选地,企业应用云平台也可以只将MAC地址推送给云AP管理平台,而将MAC地址与企业员工的绑定关系维护在本地。

[0131] 步骤S1203,云AP管理平台生成并推送MAC-PSK哈希表给AP的设备SDK。

[0132] 在本申请的一个实施例中,云AP管理平台可以根据企业应用云平台推送的MAC地址,生成一机一密的MAC-PSK哈希表,并将该MAC-PSK哈希表发送到云AP的设备SDK(Software Development Kit,软件开发工具包)中。

[0133] 步骤S1204,云AP管理平台生成并推送企业员工PSK至企业应用云平台。

[0134] 在本申请的一个实施例中,云AP可以将PSK与MAC地址之间的关联关系送给企业应用云平台,以便于企业应用云平台根据MAC地址进行PSK的分发。

[0135] 可选地,步骤S1204和步骤S1203之间没有严格的先后顺序,既可以先执行步骤S1203,再执行步骤S1204;也可以先执行步骤S1204,再执行步骤S1203;或者也可以同时执行步骤S1203和步骤S1204。

[0136] 步骤S1205,企业应用云平台转发企业员工PSK至企业应用APP。

[0137] 可选地,企业应用云平台根据企业应用APP上报的MAC地址,根据MAC地址与PSK的关联关系将PSK推送至相应的企业应用APP。需要说明的是:企业应用云平台在获取到MAC地址与PSK的关联关系之后,可以主动将PSK推送至相应的企业应用APP,还可以是在接收到企业应用APP发送的接入密钥获取请求时再发送给相应的企业应用APP。

[0138] 步骤S1206,用户在企业应用APP发起一键联网。

[0139] 可选地,如图13所示,在企业应用APP中可以显示“一键联网”的控件1301,当用户

选择了需要连接的企业网络之后，可以点击该“一键联网”的控件1301，进而终端上的企业应用APP会将PSK推送到云AP设备上，由于云AP设备在与企业应用APP通信的过程中也会获取到终端的MAC地址，进而云AP设备会根据MAC-PSK哈希表进行快速验证。

[0140] 具体地，可以根据终端的MAC地址在MAC-PSK哈希表中检索到对应的PSK，然后验证与企业应用APP推送的PSK是否一致，如果一致，则确定验证成功，这种方案相比于AP单独存储密钥列表，通过对密钥列表中的密钥进行检索来验证企业应用APP推送的PSK是否存在于该密钥列表中的方案，极大地减少了验证的时间。同时，由于AP需要验证MAC地址是否存在于MAC-PSK哈希表中，因此也可以直接拒绝非法MAC地址的设备发起的接入请求，避免了恶意设备频繁发起接入请求而影响接入点设备的性能，此外本申请实施例的技术方案还可以避免接入密钥混用的问题。

[0141] 图12所示实施例的技术方案是一机一密的应用场景，然而在一些场景下，有些终端设备是无法安装企业应用APP的，进而导致这些终端设备无法按照图12所示的流程来接入网络。对于这种情况，本申请实施例提出了采用动态密钥的方式来确保这些终端设备方便地接入网络，比如用户可以在能够安装企业应用APP的终端上来发起动态密钥的申请，当云AP管理平台生成对应的动态密钥之后，可以将该动态密钥返回给用户，进而用户可以基于该动态密钥来使终端设备发起接入请求，当连接成功之后，接入点设备可以将连接成功的终端设备的MAC地址和动态密钥加入MAC-PSK哈希表，进而可以实现图12所示的连接管理方案。同时，该动态密钥是有时间限制的，在这个时间内才能有效，进而也实现了对动态密钥的有效管理。具体流程可以如图14所示，包括如下步骤：

[0142] 步骤S1401，终端1上安装的企业应用APP向企业应用云平台申请动态密钥。

[0143] 需要说明的是，企业应用APP可以是针对某个企业单独开发的APP，或者可以是面向所有企业的一个公共平台。如果企业应用APP是面向所有企业的公共平台，那么企业用户需要在该公共平台上创建企业信息，并将该企业的云AP与该企业信息进行绑定，同时在云AP上进行配置，比如配置SSID等。

[0144] 步骤S1402，企业应用云平台审核员工身份，通过之后向云AP管理平台发起动态密钥申请请求。

[0145] 在本申请的一个实施例中，员工身份可以是员工的工号、姓名等信息，也可以是企业员工在企业应用APP中的账户名等信息。审核员工身份可以是审核员工是否是本企业的员工、审核员工是否有权限申请动态密钥等。

[0146] 步骤S1403，云AP管理平台生成动态密钥和动态密钥的有效期限，并将该动态密钥和有效期限返回给云AP1的设备SDK。

[0147] 步骤S1404，云AP管理平台将生成的动态密钥和有效期限返回给企业应用云平台。

[0148] 可选地，云AP管理平台也可以只把动态密钥返回给企业应用云平台，而动态密钥的有效期限可以不返回给企业应用云平台。

[0149] 需要说明的是：步骤S1404和步骤S1403之间没有严格的先后顺序，既可以先执行步骤S1403，再执行步骤S1404；也可以先执行步骤S1404，再执行步骤S1403；或者也可以同时执行步骤S1403和步骤S1404。

[0150] 步骤S1405，企业应用云平台转发动态密钥和有效期限至申请动态密钥的终端1的企业应用APP。

[0151] 可选地，企业应用云平台也可以只把动态密钥返回给企业应用APP，而动态密钥的有效期限可以不返回给企业应用APP。

[0152] 步骤S1406，终端1的企业应用APP获取到动态密钥和有效期限之后，用户可以在有效期限内，在其它终端(如终端2、终端3、终端n等)上输入该动态密钥，以向云AP1发起联网。

[0153] 需要说明的是，如果终端1的企业应用APP没有获取到有效期限，那么用户可以使用该动态密钥在其它终端上发起连接，然后由云AP1来确定动态密钥是否超过有效期限。

[0154] 步骤S1407，如果其它终端连接云AP1成功后，云AP1的设备SDK会根据该终端的MAC地址和动态密钥生成(或加入)MAC-PSK哈希表，并推送给云AP管理平台。

[0155] 步骤S1408，云AP管理平台将成功接入云AP1的终端设备的MAC-PSK哈希表推送给企业的其它AP(如图14中所示的的云AP2)，保证该终端设备在其它AP上也可以正常连接。

[0156] 需要说明的是，终端设备在连接其它AP时，由于其它AP已经具有该终端设备的MAC-PSK哈希表，因此可以按照图12中的验证流程来进行接入验证。

[0157] 基于图12和图14所示的技术方案，一个具体的应用场景是：员工A拥有多台设备，包括智能手机、打印机设备、扫描仪设备。员工A的智能手机可以采用图12所示的流程进行联网，在接入网络之后，员工A也希望打印机设备和扫描仪设备接入网络，但是由于打印机设备和扫描仪设备无法安装企业应用APP，那么员工A可以通过图14所示的方案来使用智能手机申请动态密钥。

[0158] 在申请到动态密钥之后，员工A使用该动态密钥将打印机设备和扫描仪设备接入AP1的网络，同时打印机设备和扫描仪设备也存储了该动态密钥。并且AP1可以将打印机设备和扫描仪设备的MAC地址与该动态密钥进行关联上传至云AP管理平台，然后由云AP管理平台发送给其它的AP，比如发送给AP2。

[0159] 如果员工A将打印机设备移动至另外一个区域，比如AP2的覆盖区域，那么打印机设备可以基于之前保存的动态密钥向AP2发起接入请求，由于AP2已经保存了打印机设备的MAC地址与该动态密钥的关联关系，那么可以快速地对打印机设备进行认证，以保证打印机设备迅速接入AP2的网络中。

[0160] 在本申请的一个实施例中，图12所示实施例的技术方案由于一个终端设备会分配一个接入密钥，可以将其理解为是“一机一密”的功能。图14所示实施例的技术方案由于一个动态密钥可以由多个终端设备使用，可以将其理解为是“一密多机”的功能。在本申请的一个实施例中，可以根据实际的应用场景和用户的需求，来选择开启“一机一密”的功能和“一密多机”的功能。比如如图15所示，在企业应用APP中可以显示“一机一密”功能和“一密多机”功能的开关控件，如果用户关闭了“一机一密”的功能，并开启了“一密多机”的功能，那么在选择网络之后，可以点击“一键申请”的控件1501，进而终端上的企业应用APP会向企业应用云平台发送动态密钥申请请求，以触发图14所示的流程。

[0161] 以下介绍本申请的装置实施例，可以用于执行本申请上述实施例中的网络连接管理方法。对于本申请装置实施例中未披露的细节，请参照本申请上述的网络连接管理方法的实施例。

[0162] 图16示出了根据本申请的一个实施例的网络连接管理装置的框图，该网络连接管理装置可以设置在接入点设备内。

[0163] 参照图16所示，根据本申请的一个实施例的网络连接管理装置1600，包括：第一接

收单元1602、第一处理单元1604、第一生成单元1606和传输单元1608。

[0164] 其中，第一接收单元1602配置为接收用于连接接入点设备的动态密钥；第一处理单元1604配置为若接收到站点设备发送的包含有所述动态密钥的接入请求，则响应所述接入请求，与所述站点设备建立连接；第一生成单元1606配置为在与所述站点设备成功建立连接之后，将所述站点设备的物理地址与所述动态密钥进行关联，生成物理地址与动态密钥之间的关联关系；传输单元1608配置为将所述关联关系传递给其它接入点设备，以使所述其它接入点设备根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0165] 在本申请的一些实施例中，基于前述方案，第一接收单元1602配置为：接收接入点管理平台发送的用于连接所述接入点设备的动态密钥；或接收预配置的用于连接所述接入点设备的动态密钥。

[0166] 在本申请的一些实施例中，基于前述方案，所述传输单元1608配置为：将所述关联关系发送给接入点管理平台，以使所述接入点管理平台将所述关联关系转发给所述其它接入点设备；或者

[0167] 将所述关联关系通过与所述其它接入点设备之间的通信链路发送给所述其它接入点设备。

[0168] 在本申请的一些实施例中，基于前述方案，所述第一接收单元1602还配置为：接收所述动态密钥的有效期限；所述第一处理单元配置为：根据所述有效期限确定所述接入请求中包含的动态密钥是否处于所述有效期限内，若确定所述动态密钥处于所述有效期限内，则与所述站点设备建立连接。

[0169] 在本申请的一些实施例中，基于前述方案，所述传输单元1608还配置为：将所述动态密钥的有效期限传递给所述其它接入点设备，以使所述其它接入点设备在所述有效期限内根据所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0170] 图17示出了根据本申请的一个实施例的网络连接管理装置的框图，该网络连接管理装置可以设置在接入点管理平台内。

[0171] 参照图17所示，根据本申请的一个实施例的网络连接管理装置1700，包括：分配单元1702、第一发送单元1704、第二接收单元1706和第二发送单元1708。

[0172] 其中，分配单元1702配置为响应于密钥申请请求，分配用于连接接入点设备的动态密钥；第一发送单元1704配置为将所述动态密钥发送给所述接入点设备和所述密钥申请请求的发起方，以使所述接入点设备基于所述动态密钥验证接收到的接入请求；第二接收单元1706配置为接收所述接入点设备发送的物理地址与所述动态密钥之间的关联关系，所述物理地址是基于所述动态密钥成功接入所述接入点设备的站点设备所拥有的地址；第二发送单元1708配置为将所述关联关系发送给其它接入点设备，以使所述其它接入点设备基于所述关联关系验证所述站点设备基于所述动态密钥发起的接入请求。

[0173] 在本申请的一些实施例中，基于前述方案，所述网络连接管理装置1700还包括：第二生成单元，配置为生成所述动态密钥的有效期限；所述第一发送单元还配置为将所述有效期限发送给所述接入点设备，以使所述接入点设备在所述有效期限内基于所述动态密钥验证接收到的接入请求。

[0174] 在本申请的一些实施例中，基于前述方案，所述分配单元1702还配置为：在所述响

应于密钥申请请求之前，接收应用程序服务端发送的密钥申请请求，所述密钥申请请求是所述应用程序服务端对发起密钥申请的应用程序客户端的身份验证通过之后发送的。

[0175] 图18示出了根据本申请的一个实施例的网络连接管理装置的框图，该网络连接管理装置可以设置在接入点设备内。

[0176] 参照图18所示，根据本申请的一个实施例的网络连接管理装置1800，包括：第三接收单元1802、获取单元1804和验证单元1806。

[0177] 其中，第三接收单元1802配置为接收物理地址与动态密钥之间的关联关系，所述关联关系是其它接入点设备根据所述动态密钥，以及使用所述动态密钥、且与所述其它接入点成功建立连接的站点设备的物理地址生成的；获取单元1804配置为若接收到指定设备发送的接入请求，则获取所述指定设备的物理地址和所述接入请求中包含的接入密钥；验证单元1806配置为根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证。

[0178] 在本申请的一些实施例中，基于前述方案，所述验证单元1806配置为：若根据所述关联关系确定所述指定设备的物理地址与所述接入请求中包含的接入密钥相关联，则确定对所述接入请求验证成功；

[0179] 若所述指定设备的物理地址不存在于所述关联关系中，则拒绝所述接入请求。

[0180] 在本申请的一些实施例中，基于前述方案，所述第三接收单元1802还配置为：接收所述动态密钥的有效期限；所述验证单元1806配置为：在所述有效期限内，根据所述关联关系、所述指定设备的物理地址，以及所述接入请求中包含的接入密钥，对所述接入请求进行验证。

[0181] 图19示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

[0182] 需要说明的是，图19示出的电子设备的计算机系统1900仅是一个示例，不应对本申请实施例的功能和使用范围带来任何限制。

[0183] 如图19所示，计算机系统1900包括中央处理单元(Central Processing Unit，CPU)1901，其可以根据存储在只读存储器(Read-Only Memory，ROM)1902中的程序或者从存储部分1908加载到随机访问存储器(Random Access Memory，RAM)1903中的程序而执行各种适当的动作和处理，例如执行上述实施例中所述的方法。在RAM 1903中，还存储有系统操作所需的各种程序和数据。CPU 1901、ROM 1902以及RAM 1903通过总线1904彼此相连。输入/输出(Input/Output，I/O)接口1905也连接至总线1904。

[0184] 以下部件连接至I/O接口1905：包括键盘、鼠标等的输入部分1906；包括诸如阴极射线管(Cathode Ray Tube，CRT)、液晶显示器(Liquid Crystal Display，LCD)等以及扬声器等的输出部分1907；包括硬盘等的存储部分1908；以及包括诸如LAN(Local Area Network，局域网)卡、调制解调器等的网络接口卡的通信部分1909。通信部分1909经由诸如因特网的网络执行通信处理。驱动器1910也根据需要连接至I/O接口1905。可拆卸介质1911，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器1910上，以便于从其上读出的计算机程序根据需要被安装入存储部分1908。

[0185] 特别地，根据本申请的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本申请的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的计算机程序。在这样的

实施例中，该计算机程序可以通过通信部分1909从网络上被下载和安装，和/或从可拆卸介质1911被安装。在该计算机程序被中央处理单元(CPU)1901执行时，执行本申请的系统中限定的各种功能。

[0186] 需要说明的是，本申请实施例所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(Erasable Programmable Read Only Memory，EPROM)、闪存、光纤、便携式紧凑磁盘只读存储器(Compact Disc Read-Only Memory，CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的计算机程序。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的计算机程序可以用任何适当的介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

[0187] 附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。其中，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0188] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现，所描述的单元也可以设置在处理器中。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定。

[0189] 作为另一方面，本申请还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该电子设备执行时，使得该电子设备实现上述实施例中所述的方法。

[0190] 应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本申请的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

[0191] 通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本申请实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM，U盘，移动硬盘等)中或网络上，包括若干指令以使得一台计算设备(可以是个人计算机、服务器、触控终端、或者网络设备等)执行根据本申请实施方式的方法。

[0192] 本领域技术人员在考虑说明书及实践这里公开的实施方式后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。

[0193] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

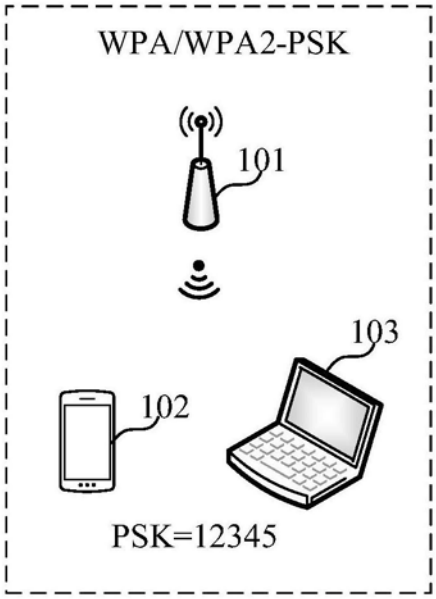

WPA/WPA2-PSK
101
103
102
PSK=12345

图1

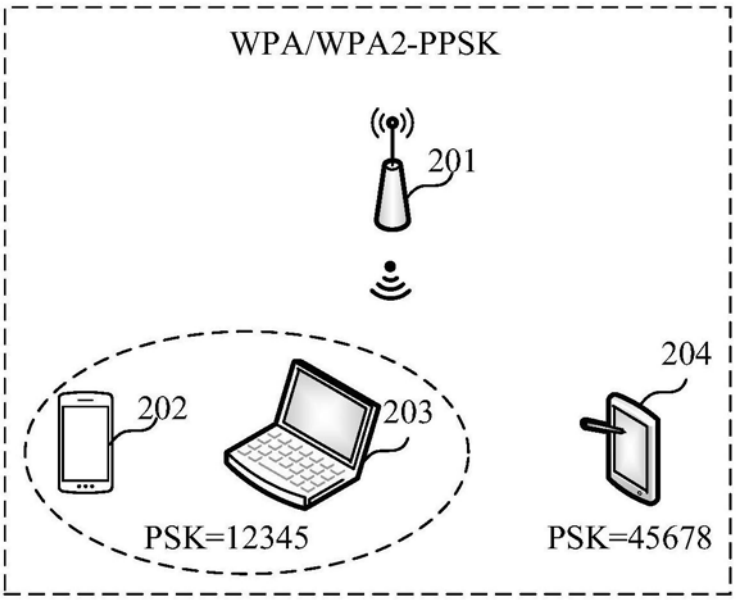

WPA/WPA2-PPSK
201
204
202
203
PSK=12345
PSK=45678

图2

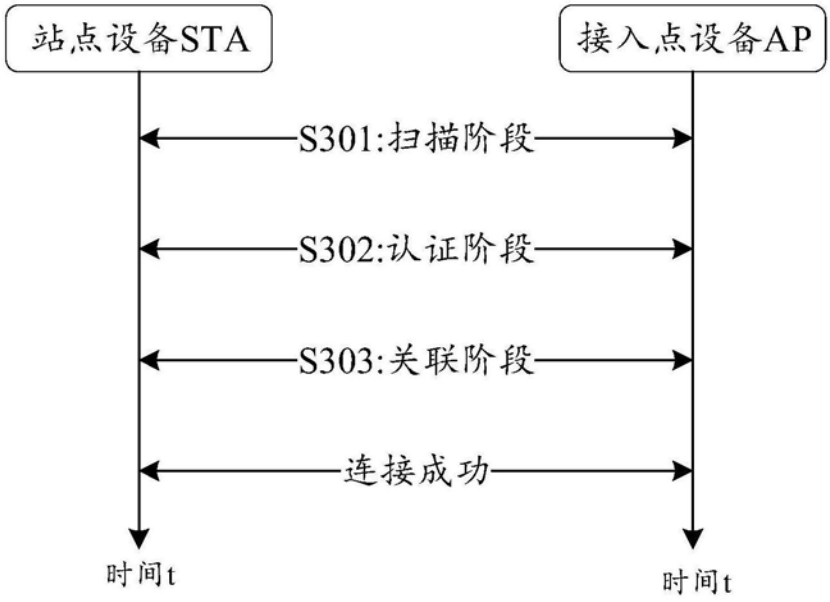



图3

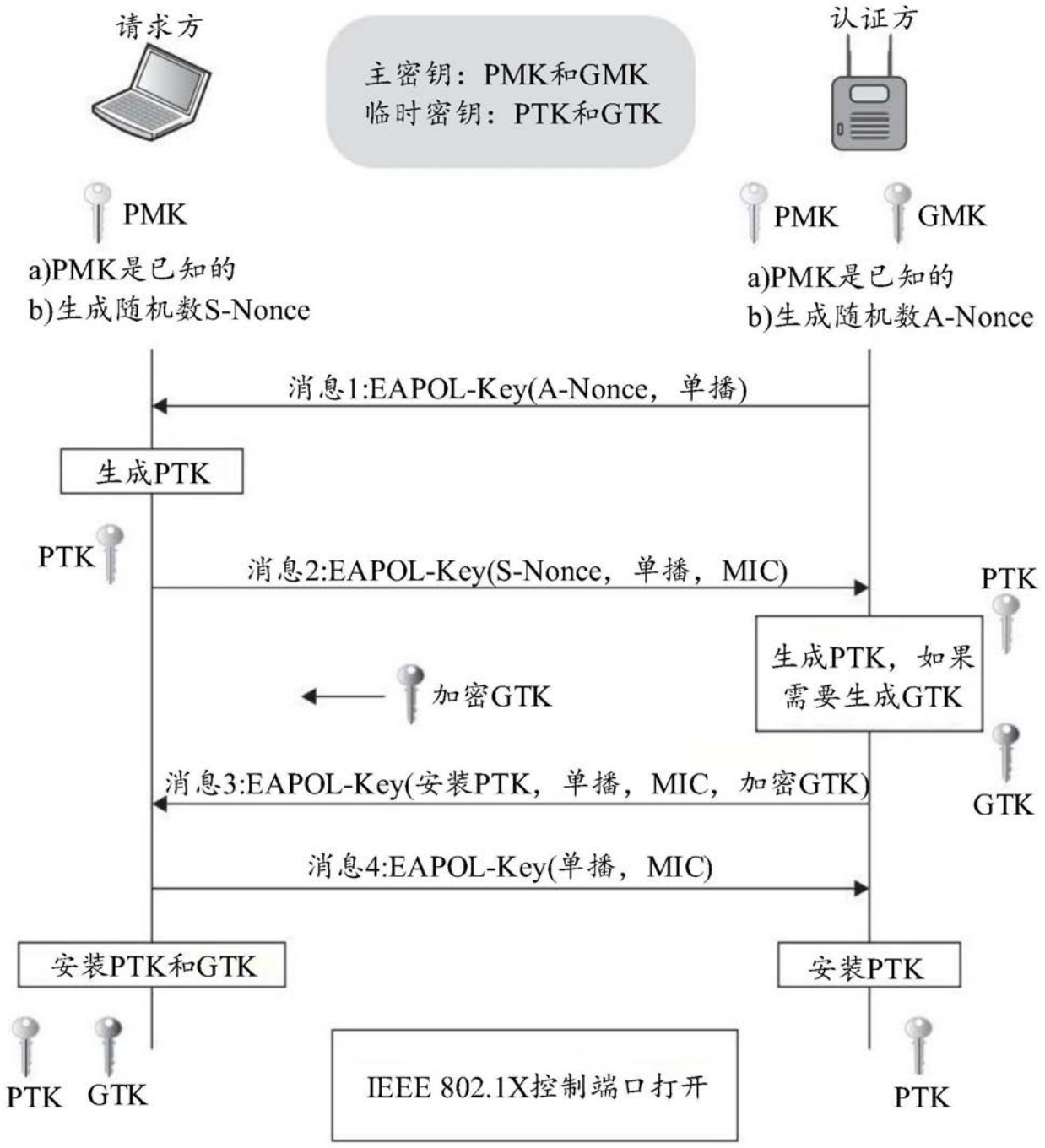

请求方
主密钥：PMK和GMK
临时密钥：PTK和GTK
认证方
PMK
a)PMK是已知的
b)生成随机数S-Nonce
PMK
GMK
a)PMK是已知的
b)生成随机数A-Nonce
消息1:EAPOL-Key(A-Nonce，单播)
生成PTK
PTK
消息2:EAPOL-Key(S-Nonce，单播，MIC)
PTK
生成PTK，如果需要生成GTK
加密GTK
GTK
消息3:EAPOL-Key(安装PTK，单播，MIC，加密GTK)
消息4:EAPOL-Key(单播，MIC)
安装PTK和GTK
安装PTK
PTK
GTK
IEEE 802.1X控制端口打开
PTK

图4

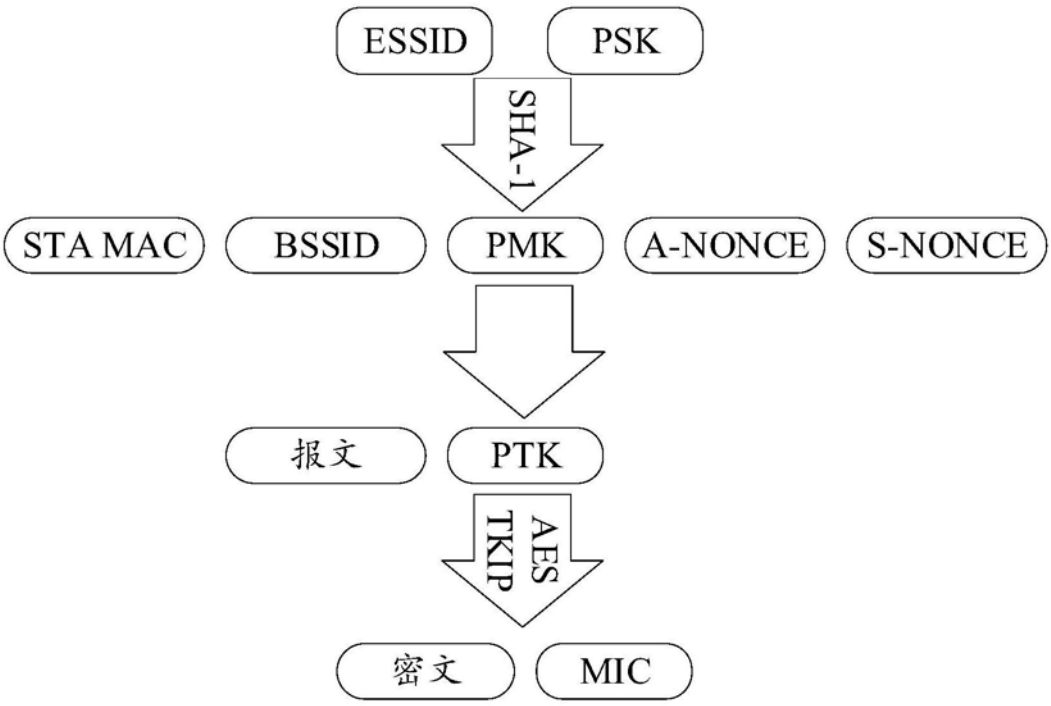

ESSID
PSK
SHA-1
STA MAC
BSSID
PMK
A-NONCE
S-NONCE
报文
PTK
AES
TKIP
密文
MIC

图5


Portal配置
确定
Portal状态
ON
*Portal URL
输入Portal URL
认证Key
输入认证Key
*认证Secret
输入认证Secret
认证URL
输入认证URL
白名单
输入白名单……
Check URL
Check URL
网络类型
LAN

图6

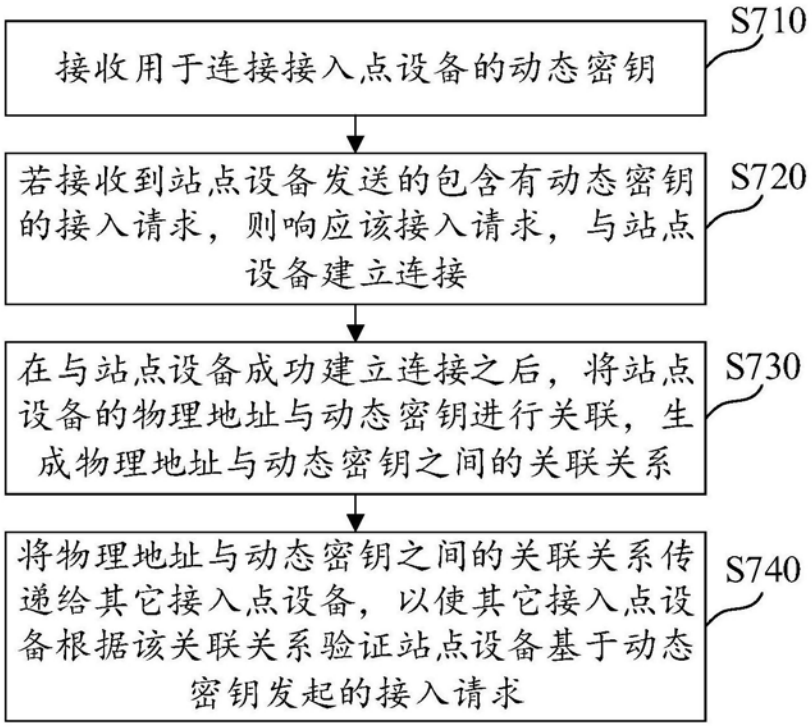

S710
接收用于连接接入点设备的动态密钥
S720
若接收到站点设备发送的包含有动态密钥的接入请求，则响应该接入请求，与站点设备建立连接
S730
在与站点设备成功建立连接之后，将站点设备的物理地址与动态密钥进行关联，生成物理地址与动态密钥之间的关联关系
S740
将物理地址与动态密钥之间的关联关系传递给其它接入点设备，以使其它接入点设备根据该关联关系验证站点设备基于动态密钥发起的接入请求

图7

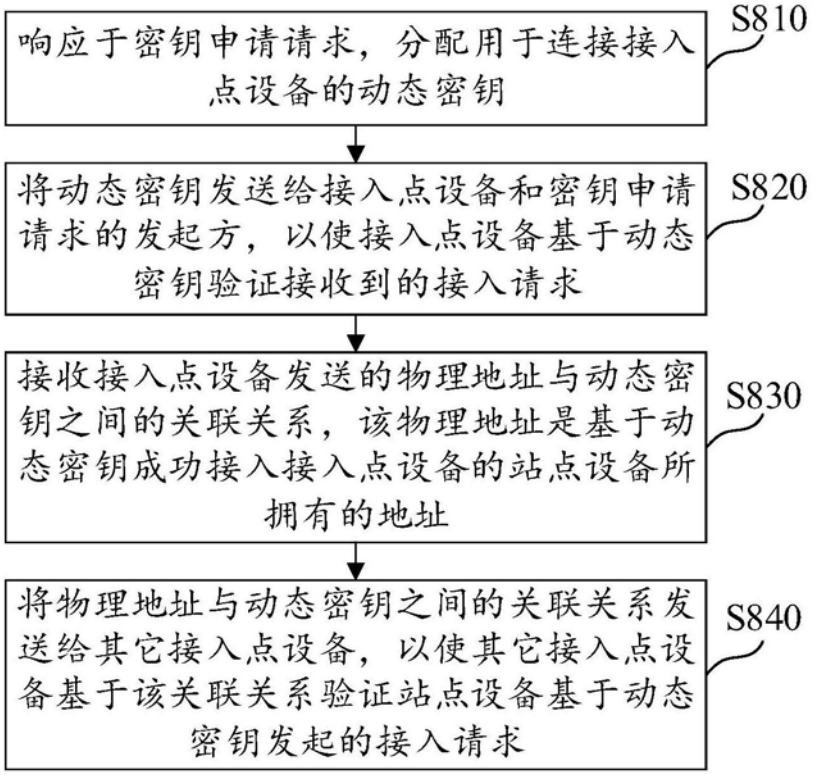

S810
响应于密钥申请请求，分配用于连接接入点设备的动态密钥
S820
将动态密钥发送给接入点设备和密钥申请请求的发起方，以使接入点设备基于动态密钥验证接收到的接入请求
S830
接收接入点设备发送的物理地址与动态密钥之间的关联关系，该物理地址是基于动态密钥成功接入接入点设备的站点设备所拥有的地址
S840
将物理地址与动态密钥之间的关联关系发送给其它接入点设备，以使其它接入点设备基于该关联关系验证站点设备基于动态密钥发起的接入请求

图8

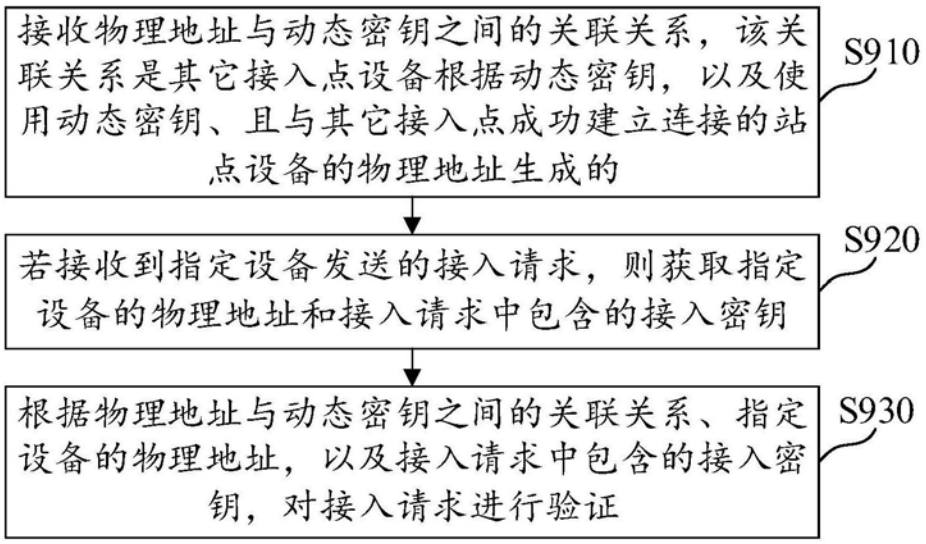

接收物理地址与动态密钥之间的关联关系，该关联关系是其它接入点设备根据动态密钥，以及使用动态密钥、且与其它接入点成功建立连接的站点设备的物理地址生成的
S910
若接收到指定设备发送的接入请求，则获取指定设备的物理地址和接入请求中包含的接入密钥
S920
根据物理地址与动态密钥之间的关联关系、指定设备的物理地址，以及接入请求中包含的接入密钥，对接入请求进行验证
S930

图9

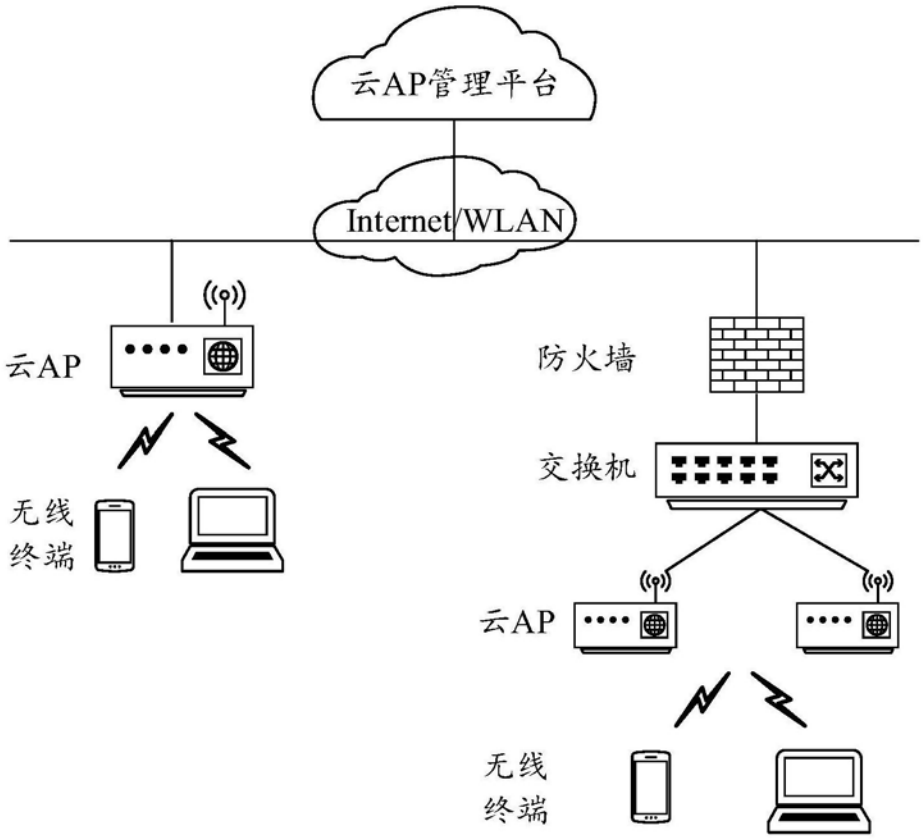

云AP管理平台
Internet/WLAN
云AP
无线终端
防火墙
交换机
云AP
无线终端

图10

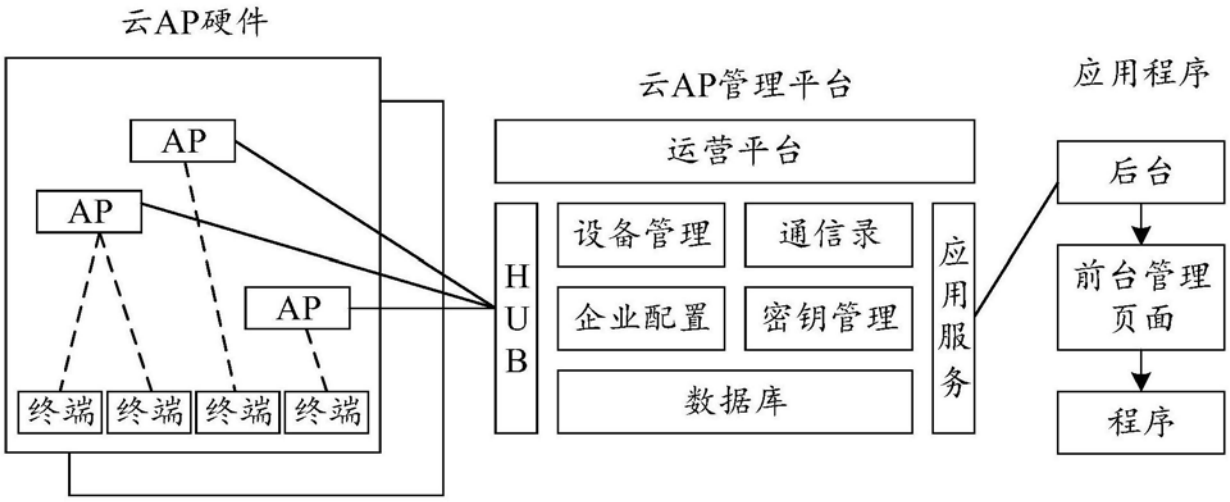

云AP硬件
AP
AP
AP
终端
终端
终端
终端
云AP管理平台
运营平台
HUB
设备管理
通信录
企业配置
密钥管理
数据库
应用服务
应用程序
后台
前台管理页面
程序

图11

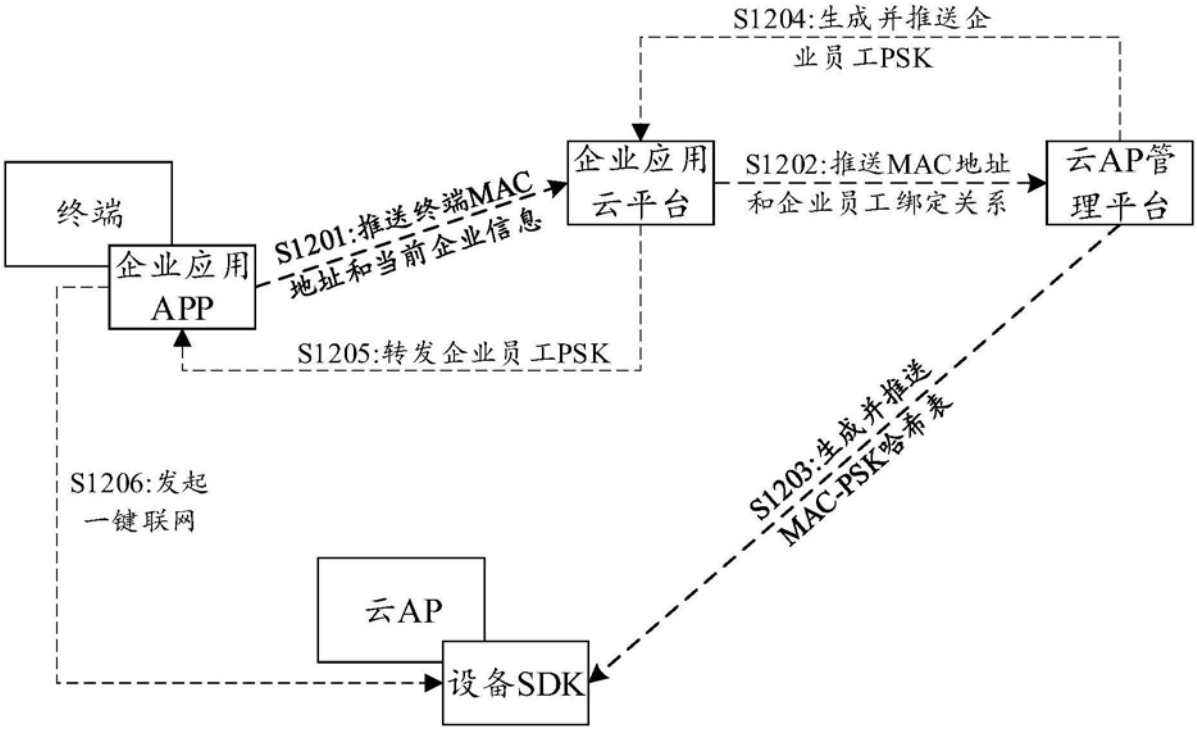

S1204:生成并推送企业员工PSK
终端
企业应用APP
S1201:推送终端MAC地址和当前企业信息
企业应用云平台
S1202:推送MAC地址和企业员工绑定关系
云AP管理平台
S1205:转发企业员工PSK
S1203:生成并推送MAC-PSK哈希表
S1206:发起一键联网
云AP
设备SDK

图12

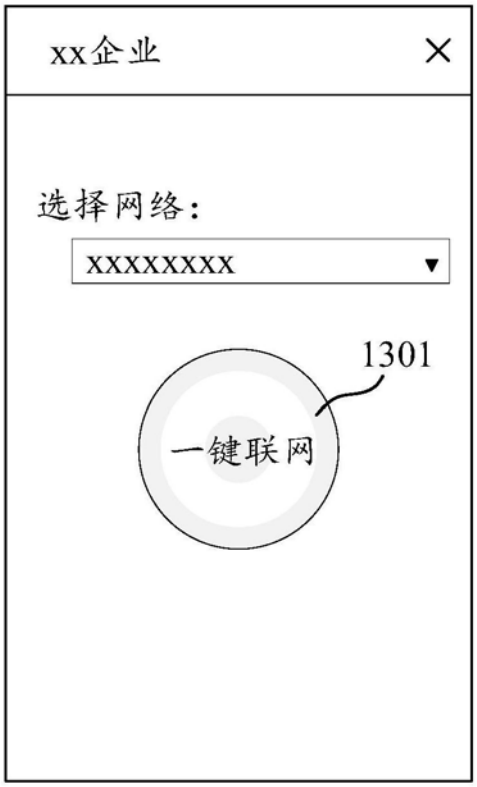

xx企业
选择网络:
xxxxxxxx
1301
一键联网

图13

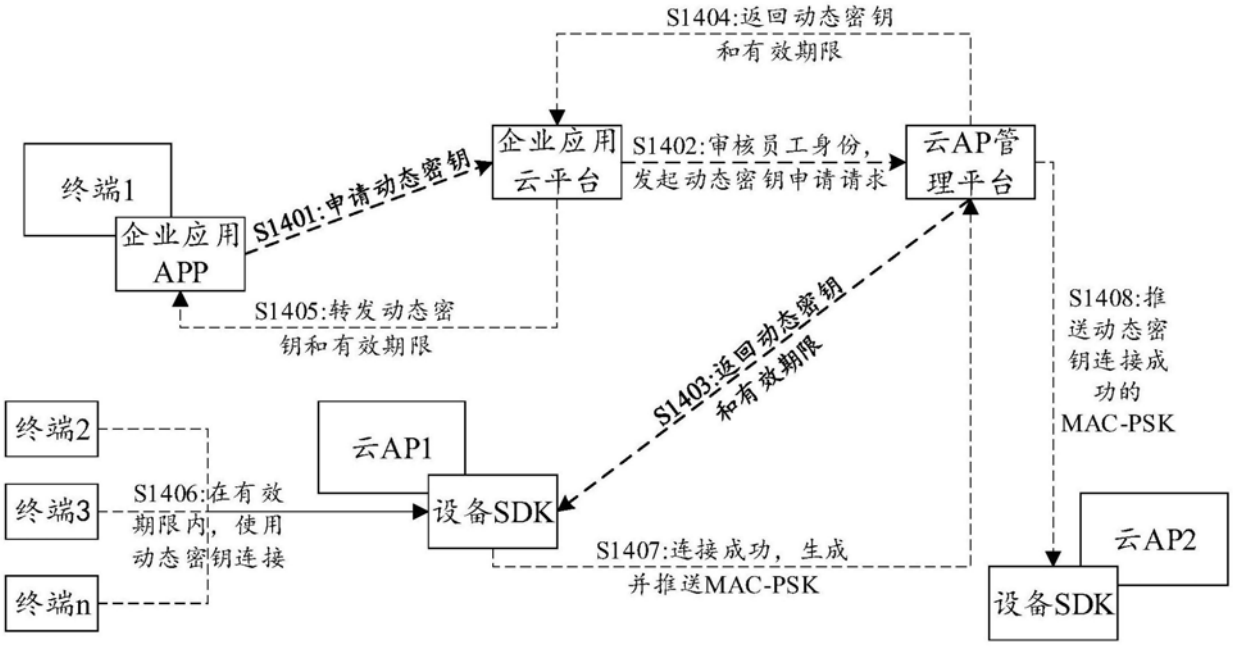

S1404:返回动态密钥和有效期限
企业应用云平台
S1402:审核员工身份，发起动态密钥申请请求
云AP管理平台
终端1
企业应用APP
S1401:申请动态密钥
S1405:转发动态密钥和有效期限
S1403:返回动态密钥和有效期限
S1408:推送动态密钥连接成功的MAC-PSK
终端2
终端3
终端n
S1406:在有效期限内，使用动态密钥连接
云AP1
设备SDK
S1407:连接成功，生成并推送MAC-PSK
云AP2
设备SDK

图14

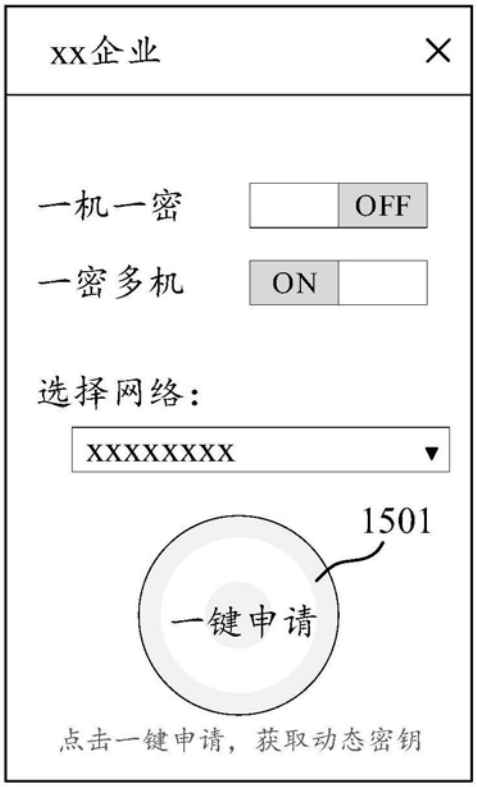

xx企业
一机一密
OFF
一密多机
ON
选择网络:
XXXXXXXX
1501
一键申请
点击一键申请，获取动态密钥

图15

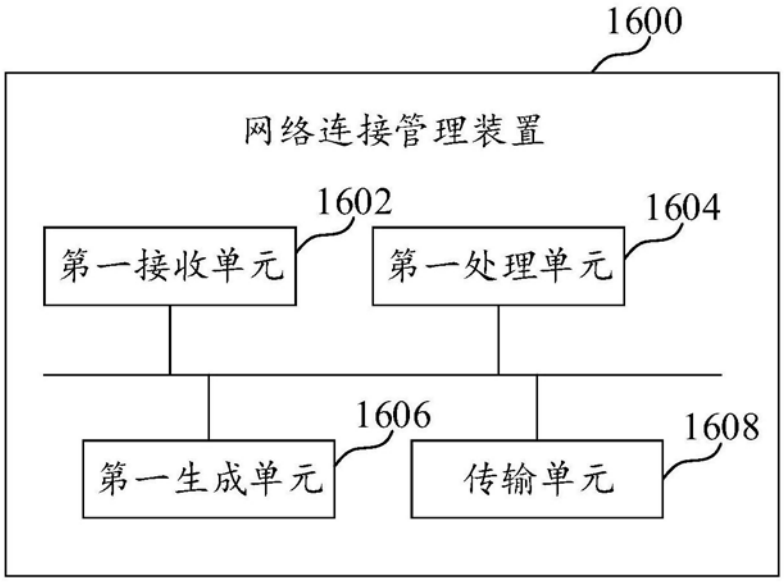

1600
网络连接管理装置
1602
第一接收单元
1604
第一处理单元
1606
第一生成单元
1608
传输单元

图16

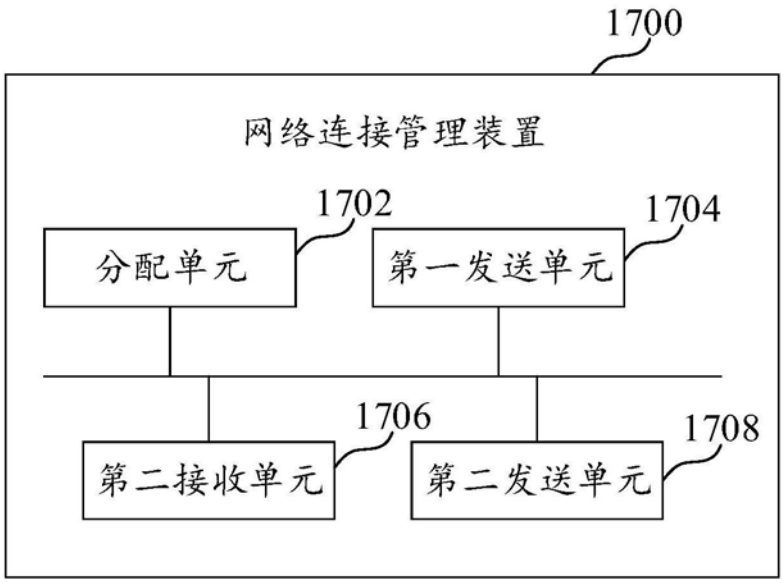

1700
网络连接管理装置
1702
分配单元
1704
第一发送单元
1706
第二接收单元
1708
第二发送单元

图17

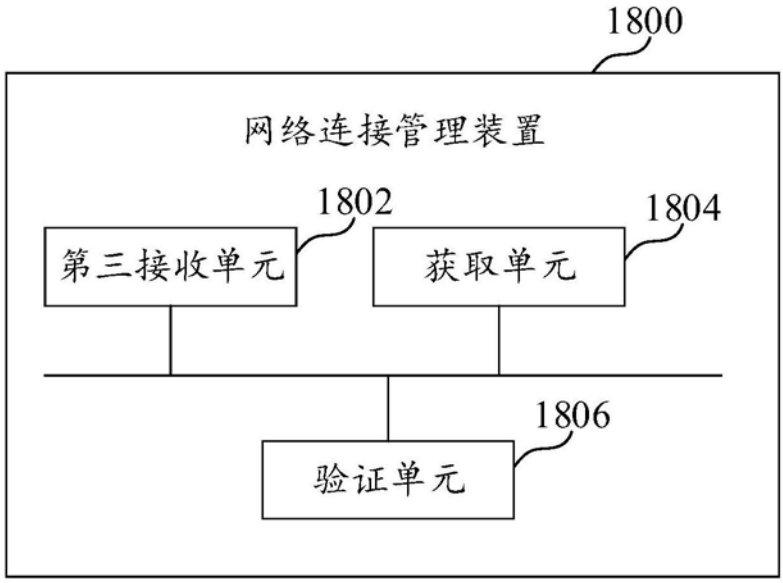

1800
网络连接管理装置
1802
第三接收单元
1804
获取单元
1806
验证单元

图18

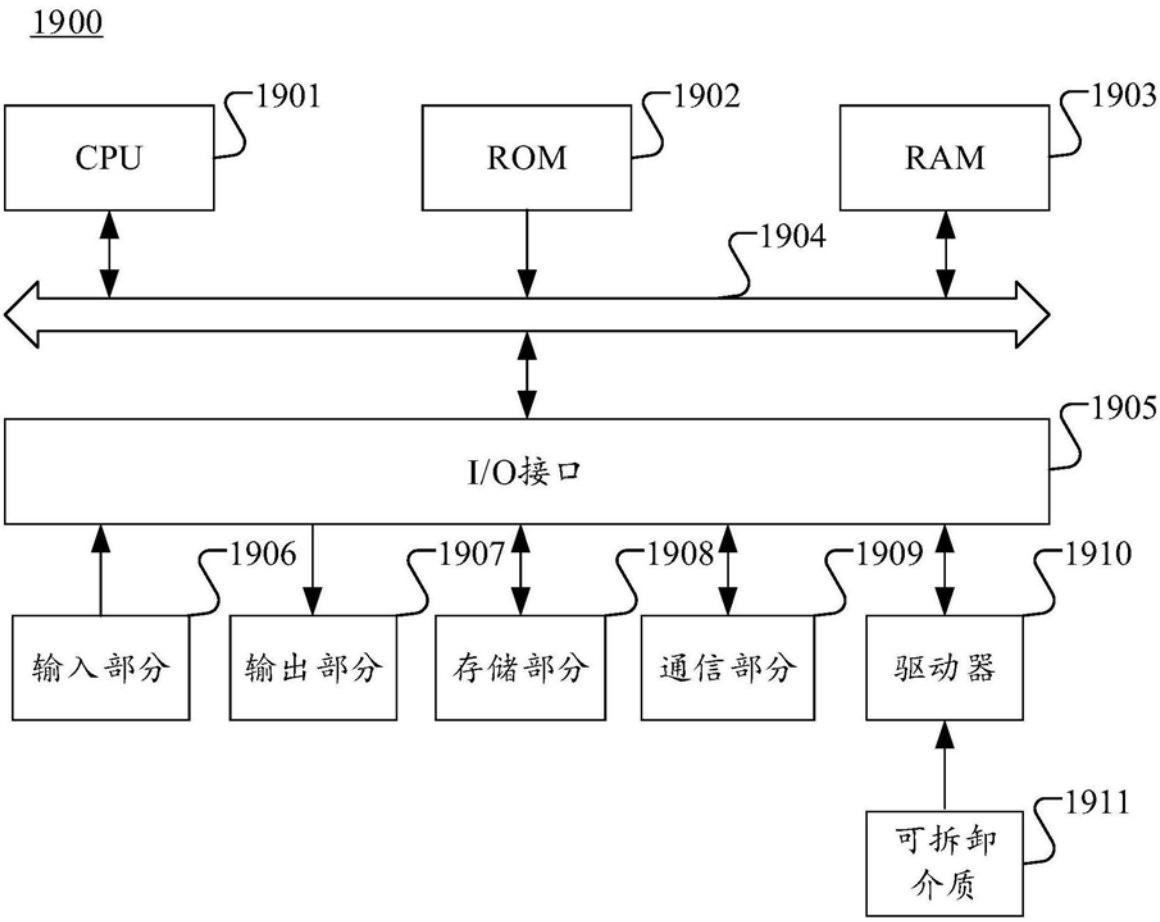

1900
CPU
1901
ROM
1902
RAM
1903
1904
I/O接口
1905
输入部分
1906
输出部分
1907
存储部分
1908
通信部分
1909
驱动器
1910
可拆卸介质
1911

图19