(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 114257567 A
(43)申请公布日 2022.03.29

(21)申请号 202111060318.5

(22)申请日 2021.09.10

(30)优先权数据
63/076,967 2020.09.11 US
17/446,838 2021.09.03 US

(71)申请人 黑莓有限公司
地址 加拿大安大略省

(72)发明人 M•P•蒙特莫罗 J•R•W•莱普 S•麦卡恩

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 罗利娜

(51)Int.Cl.
H04L 61/50(2022.01)
H04L 61/2503(2022.01)
H04W 8/26(2009.01)
H04W 88/08(2009.01)
H04L 61/103(2022.01)
H04L 9/08(2006.01)

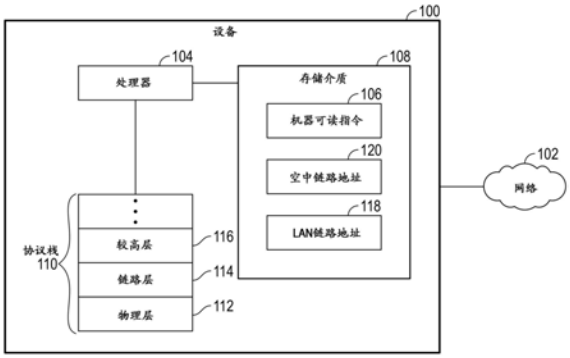
权利要求书2页 说明书12页 附图3页

(54)发明名称

用于设备的多个链路层地址

(57)摘要

本公开的实施例涉及用于设备的多个链路层地址。一种设备，包括链路层，其被配置为：使用第一链路层地址和第二链路层地址，在设备与无线网络关联的持续时间内维持第一链路层地址不变，并且在该持续时间期间将第二链路层地址从第一值改变为第二值。



CN 114257567 A

1.一种设备,包括:

链路层,所述链路层包括硬件处理电路并且被配置为:

使用第一链路层地址和第二链路层地址,

在所述设备与无线网络的关联的持续时间内维持所述第一链路层地址不变,以及

在所述持续时间期间将所述第二链路层地址从第一值改变为第二值。

2.根据权利要求1所述的设备,其中所述关联是与所述无线网络的接入点AP的关联,并且所述链路层被配置为:

与所述无线网络的各个AP建立多个链路,其中所述第二链路层地址用于所述多个链路中的第一链路,以及

维持用于所述多个链路中的第二链路的第三链路层地址,其中所述第三链路层地址在所述设备与另一AP的关联的持续时间期间是可改变的。

3.根据权利要求2所述的设备,其中所述第一链路层地址是多链路设备MLD地址,并且所述第二链路层地址和所述第三链路层地址是用于所述设备与所述无线网络的对应AP之间的所述多个链路的相应链路的多个链路层地址的一部分。

4.根据权利要求1所述的设备,其中所述第一链路层地址是第一媒体访问控制MAC地址,并且所述第二链路层地址是第二MAC地址。

5.根据权利要求1所述的设备,其中所述链路层被配置为将所述第一链路层地址包括在以有线网络为目的地的数据帧中。

6.根据权利要求1所述的设备,其中所述链路层被配置为将所述第一链路层地址包括在被传输给所述无线网络中的接入点AP的管理帧中。

7.根据权利要求1所述的设备,还包括:

处理器,所述处理器被配置为:

向所述无线网络中的接入点AP发送地址解析请求,以及

由所述设备响应于所述地址解析请求从所述AP接收所述第一链路层地址和所述第二链路层地址。

8.根据权利要求1所述的设备,其中所述第二链路层地址是随机化地址。

9.根据权利要求1所述的设备,其中所述第二链路层地址是在所述设备处以及在所述无线网络中的接入点AP处可独立得出的密码地址。

10.根据权利要求1所述的设备,其中所述链路层被配置为在包括包含所述第二链路层地址的报头的数据帧的有效负载中隧道传输包含所述第一链路层地址的局域网LAN报头。

11.根据权利要求1所述的设备,包括:

在所述链路层之上的另一层,所述另一层被配置为在所述第二链路层地址被改变时基于所述第一链路层地址来维持与局域网LAN的连接。

12.根据权利要求1所述的设备,包括:

安全层,所述安全层被配置为使用所述第二链路层地址来绑定所述设备和所述无线网络的接入点AP之间的安全关联。

13.根据权利要求12所述的设备,其中所述安全层被配置为使用所述第二链路层地址来得出成对主密钥PMK和成对临时密钥PTK,并且其中所述安全关联是PTK安全关联PTKSA。

14.根据权利要求13所述的设备,其中所述安全层被配置为响应于所述第二链路层地

址的所述改变来协商新的PTK。

15.根据权利要求1所述的设备,其中所述链路层被配置为在由所述无线网络中的接入点AP传输的信息中检测所述AP支持链路层地址保护特征,所述链路层地址保护特征提供用于供所述设备使用的不同链路层地址。

16.根据权利要求15所述的设备,其中所述链路层被配置为向所述AP发送以下指示:请求关于所述AP是否支持所述链路层地址保护特征的信息。

17.根据权利要求15所述的设备,其中所述链路层被配置为与对等设备执行隧道直接链路设置TDLS以在所述设备和所述对等设备之间建立直接无线链路,所述TDLS包括所述链路层向所述对等设备发送对所述链路层地址保护特征的支持的指示。

18.根据权利要求17所述的设备,其中所述链路层被配置为使用所述第二链路层地址向所述对等设备发送帧。

19.一种用于无线网络的接入点AP,包括:

链路层,所述链路层包括硬件处理电路并且被配置为:

通过所述无线网络向设备传输对提供多个链路层地址的链路层地址保护特征的支持的指示,所述多个链路层地址包括在所述设备和所述AP之间的关联的持续时间内将被维持不变的第一链路层地址,以及在所述持续时间期间将被变化为不同值的第二链路层地址。

20.根据权利要求19所述的AP,其中所述链路层被配置为:

通过所述无线网络从所述设备接收地址解析请求,以及

响应于所述地址解析请求,向所述设备发送所述第一链路层地址和所述第二链路层地址。

21.根据权利要求19所述的AP,其中所述链路层被配置为:

通过有线局域网LAN从第二设备接收第二地址解析请求,以及

响应于所述第二地址解析请求,向所述第二设备发送在所述第二设备和所述AP之间的关联的持续时间内被维持不变的第三链路层地址。

22.根据权利要求19所述的AP,其中所述链路层被配置为维持将所述第一链路层地址映射到所述第二链路层地址的映射。

23.根据权利要求22所述的AP,其中所述链路层被配置为:

从所述设备接收以目的地设备为目标的帧,

将所述帧中的所述第二链路层地址变换为所述第一链路层地址,以及

将所述第一链路层地址包括在被发送到所述目的地设备的所述帧中。

24.根据权利要求22所述的AP,其中所述链路层被配置为:

从源设备接收以所述设备为目标的帧,

将所述帧中的所述第一链路层地址变换为所述第二链路层地址,以及

将所述第二链路层地址包括在被发送到所述设备的所述帧中。

25.一种包括指令的非瞬态机器可读存储介质,所述指令在执行时使设备:

在所述设备的链路层处,使用第一链路层地址和第二链路层地址,

在所述设备与无线网络的关联的持续时间内维持所述第一链路层地址不变,以及

在所述持续时间期间将所述第二链路层地址从第一值改变为第二值。

用于设备的多个链路层地址

技术领域

[0001] 本公开的实施例涉及用于设备的多个链路层地址。

背景技术

[0002] 电子设备可以通过有线或无线网络进行通信。网络的一个示例包括局域网(LAN)，它是一种允许特定区域(物理区域或逻辑区域)中的设备彼此通信的网络。没有适当凭证或权限的设备将无法连接到LAN。

[0003] LAN可以包括有线LAN或无线LAN。无线LAN(WLAN)包括设备能够无线连接到的无线接入点(AP)。

发明内容

[0004] 根据一些实现，公开了一种设备，包括：链路层，链路层包括硬件处理电路并且被配置为：使用第一链路层地址和第二链路层地址，在设备与无线网络的关联的持续时间内维持第一链路层地址不变，以及在持续时间期间将第二链路层地址从第一值改变为第二值。

[0005] 根据一些实现，公开了一种用于无线网络的接入点AP，包括：链路层，链路层包括硬件处理电路并且被配置为：通过无线网络向设备传输对提供多个链路层地址的链路层地址保护特征的支持的指示，多个链路层地址包括在设备和AP之间的关联的持续时间内将被维持不变的第一链路层地址，以及在持续时间期间将被变化为不同值的第二链路层地址。

[0006] 根据一些实现，公开了一种包括指令的非瞬态机器可读存储介质，指令在执行时使设备：在设备的链路层处，使用第一链路层地址和第二链路层地址，在设备与无线网络的关联的持续时间内维持第一链路层地址不变，以及在持续时间期间将第二链路层地址从第一值改变为第二值。

附图说明

[0007] 关于以下附图来描述本公开的一些实现。

[0008] 图1是根据本公开的一些实现的设备的框图。

[0009] 图2是根据本公开的一些实现的包括接入点(AP)和站(STA)的示例布置的框图。

[0010] 图3是根据本公开的一些实现的STA和AP之间的过程的消息流图。

[0011] 在整个附图中，相同的附图标号指明相似但不一定相同的元件。附图不一定按比例绘制，并且某些部件的尺寸可能被夸大以更清楚地说明所示示例。此外，附图提供了与描述相一致的示例和/或实现；然而，描述不限于附图中所提供的示例和/或实现。

具体实施方式

[0012] 在本公开中，除非上下文另有明确指示，否则术语“一”、“一个”或“该”的使用也旨在包括复数形式。此外，当在本公开中使用时，术语“包括(includes)”“包括(including)”、

“包括(comprises)”、“包括(comprising)”、“具有(have)”或“具有(having)”指定所述元件的存在,但是不排除其他元件的存在或添加。

[0013] 1.背景、缩略词和缩写

[0014] 下面的表1列出了各种缩略词和缩写

[0015] 表1

[0016]

缩略词/缩写	完整文本	简要描述
AP	接入点	基础设施 IEEE 802.11（WLAN）无线设备，其终止空中接口，允许业务流入和流出基础设施。

[0017]

缩略词/缩写	完整文本	简要描述
IP	互联网协议	
LAN	局域网	
MAC	媒体访问控制	OSI 栈的层 2。也用于 MAC 地址，其在 802.3 和 802.11 网络中是 48 位标识符
STA	站	IEEE 802.11（WLAN）无线设备。这可以是移动设备或接入点。
WLAN	无线局域网	
EHT	超高吞吐量	IEEE 802.11be 修正案的名称
PHY	物理层	OSI 栈的层 1
MLD	多链路设备	802.11be 中定义的设备类型，其支持多于一个同步无线电链路。逻辑上它是在其中具有多于一个 STA 的设备。
RCM	随机和变化的 MAC 地址	IEEE 802.11 中的研究组名称
ESS	扩展服务集	包括多于一个 AP 的 WLAN。此配置允许 AP 之间的移动性，同时保持连接到网络
DHCP	动态主机配置协议	LAN 上的分配层 3 IP 地址的方法
ARP	地址解析协议	层 2 地址（MAC 地址）与层 2 地址（IPv4 地址）之间的绑定
PMK	成对主密钥	如 IEEE 802.11 中所定义
PTK	成对临时密钥	如 IEEE 802.11 中所定义
PTKSA	成对临时密钥安全关联	如 IEEE 802.11 中所定义
RSNA	健壮安全网络	如 IEEE 802.11 中所定义

[0018]

缩略词/缩写	完整文本	简要描述
	关联	
SAE	对等同时认证	如 IEEE 802.11 中所定义
FT	快速基本服务集（BSS）转变	如 IEEE 802.11 中所定义
FILS	快速初始链路设置	如 IEEE 802.11 中所定义
KDE	密钥数据封装	如 IEEE 802.11 中所定义
TDLS	隧道直接链路设置	如 IEEE 802.11 中所定义

[0019] 下面的表2列出了所使用的各种术语以及这些术语的对应简要描述。

[0020] 表2

[0021]

术语	简要描述
IP 地址	通过互联网协议（IP）分配给网络实体的唯一标识符。这对于网络分段来说通常是唯一的。
MAC 地址	分配给网络实体用于网络通信的唯一标识符。这通常是全球唯一的。
LAN MAC	在寻址 LAN 和/或 WLAN 上的站或设备时使用的 MAC 地址
AIR MAC	源地址（SA）或目的地地址（DA）中使用的 MAC 地址
链路地址	IEEE 802.11be 提议的地址，用于标识多链路设备中的个体链路。
MLD 地址	IEEE 802.11be 提议的地址，用于标识多链路设备中的整个设备
LAN MAC	用于本文所提议的术语。替代名称可以是 MAC

[0022]

术语	简要描述
保护	地址隐私、LAN MAC 隐私、临时 MAC 寻址等。
代理 ARP	代理 ARP 服务使得 AP 能够代表关联的非 AP STA 来响应 ARP 和邻居发现帧
SA 查询帧	安全关联查询帧

[0023] 2.问题

[0024] 2.1总则

[0025] 在局域网(LAN)中操作的设备使用其媒体访问控制(MAC)地址作为在LAN上传输和接收的帧的源地址。LAN使用设备的MAC地址将LAN业务路由到LAN上的正确设备。此外，设备的MAC地址被用来维持其他状态信息，诸如IP地址。如果设备改变其MAC地址，则LAN和IP通信都被中断。设备必须剥离并重新附接到LAN以重新建立状态信息，这可能会中断任何应用级通信。

[0026] 2.2用户隐私

[0027] 在LAN上操作的设备可以被分配全球唯一的MAC地址。传统上，设备在LAN中操作时使用全球唯一的MAC地址作为其地址。随着用户隐私变得越来越重要，一些设备现在将其MAC地址分配给本地管理的地址空间中随机衍生的地址以进行通信。在执行发现过程以及在LAN上进行连接和操作时，随机衍生的地址被用来与其他设备进行通信。

[0028] 在LAN通信和隐私的保护之间存在对设备的相互冲突的行为要求。相互冲突的行为要求的一个示例包括使用MAC地址用于在与LAN关联的持续时间内运行的安全密钥算法(其基于MAC地址生成安全密钥)，以及基于经常改变MAC地址以阻止被动观察者的跟踪的隐私增强。应当开发解决方案来解决相互冲突的行为要求。

[0029] 3.示例实现

[0030] 图1示出了能够通过诸如有线LAN或无线LAN(WLAN)之类的网络102进行通信的设备100。设备的示例可以包括以下任意或某种组合：台式计算机、笔记本计算机、平板计算机、智能电话、物联网(IOT)设备、交通工具、交通工具中的控制器、游戏电器、家用电器等。

[0031] 设备100包括能够执行存储在非瞬态机器可读或计算机可读存储介质108中的机器可读指令106的一个或多个硬件处理器104。硬件处理器可以包括微处理器、多核微处理器的核心、微控制器、可编程集成电路、可编程门阵列或其他硬件处理电路。

[0032] 存储介质108可以使用一个或多个存储设备来实现。存储设备可以包括易失性存储器设备或非易失性存储器设备。存储设备的另一个示例可以包括永久性存储设备，诸如基于磁盘的存储设备、固态驱动器等。

[0033] 设备100还包括协议栈110，其包括允许设备100和网络102之间的通信的各种层。

[0034] 在一些示例中，网络102是无线网络，诸如WLAN、蜂窝网络等等。在其他示例中，网络102(或另一网络)可以包括有线网络，诸如LAN。尽管仅描绘了一个网络102，但是应注意，可以存在设备100可与之通信的多个网络，其中网络可以包括无线网络和有线网络。例如，设备100可以与WLAN以及与有线LAN进行通信。

[0035] 协议栈110的层包括物理层112,其包括物理电路(包括收发器)以通过网络102传输和接收信号。协议栈110还包括在物理层112之上的链路层114。在一些示例中,链路层114包括媒体访问控制(MAC)层。

[0036] 协议栈110还包括在链路层114之上的一个或多个较高层116。较高层116的示例可以包括以下中的任意或某个组合:IP层、安全协议层等等。

[0037] 注意,(多个)较高层116和可能的链路层114可以被实现为可由一个或多个硬件处理器104执行的机器可读指令。在另外的示例中,链路层114(和可能的一个或多个较高层116)可以使用硬件处理电路来实现。

[0038] 根据本公开的一些实现,链路层114能够使用多个链路层地址(例如,多个MAC地址)用于去往或来自设备100的通信。多个链路层地址包括在设备100与无线网络关联的持续时间内维持不变的第一链路层地址。多个链路层地址还包括第二链路层地址,其在设备100与无线网络关联的持续时间期间从第一值改变为第二值(并且可能改变为其他值)。

[0039] 在一些示例中,在与无线网络关联的持续时间内不变的第一链路层地址被称为LAN链路地址118。在设备100与无线网络关联的持续时间期间可以改变的第二链路层地址被称为空中链路地址120。LAN链路地址118和空中链路地址120可以被存储在存储介质108(例如,存储器)中以用于在设备的通信100中使用。

[0040] 3.1实现1:LAN MAC保护

[0041] 根据一些实现,支持使用多个链路层地址用于特定设备(例如,100)的通信的特征被称为LAN MAC保护特征。在其他示例中,此特征也可以被称为LAN MAC隐私、MAC地址轮换、AIR MAC改变协议等。

[0042] 更一般地,该特征被称为链路层地址保护特征。

[0043] 图2示出了包括接入点(AP)202-1和202-2的示例布置,其是WLAN中的无线接入网络节点,无线设备(被称为站或STA)可以与其建立无线连接。AP也可以被称为STA。不是AP的无线设备被称为非AP STA。

[0044] 图2示出了能够与AP 202-1和202-2通信的多个STA(A、B、C、D和E)。STA A、B、C和E是能够与WLAN 204中的AP 202-1和202-2无线通信的无线设备。STA D是通过有线LAN 206连接到AP 202-1和202-2的有线设备。

[0045] WLAN 204被认为是空中侧,其中STA通过空中(无线)来与AP 202-1或202-2通信。有线LAN 206是LAN侧的一部分,其中STA通过有线通信介质来与AP 202-1或202-2通信。

[0046] 在图2的示例中,STA A、B和C支持LAN MAC保护特征,STA E是不支持LAN MAC保护特征的传统设备。在随后的讨论中,支持LAN MAC保护特征的STA可以被称为“LAN MAC保护的STA”。

[0047] LAN MAC保护的STA(STA A、B和C中的任何一个)可以使用LAN MAC保护特征来与使用单个静态MAC地址(例如,图1的LAN链路地址118)的传统设备(例如,STA E)进行互操作。

[0048] WLAN 204中的AP 202-1或202-2使用由AP传输的消息或信息元素来通告对LAN MAC保护特征的支持,诸如在信标、探测响应帧等等中。例如,可以通过在空中通信的帧的扩展能力元素中的LAN MAC保护元素(例如,LAN MAC保护位)中进行通告来指定对LAN MAC保护特征的支持。更一般地,AP可以包括链路层(在一些示例中包括硬件处理电路或在其他示例中包括机器可读指令),其被配置为通过无线网络(例如,WLAN 204)向设备(STA A、B或C

中的任何一个)传输支持提供多个链路层地址的链路层地址保护特征的指示,该多个链路层地址包括在设备和AP之间的关联的持续时间内维持不变的第一链路层地址,以及在持续时间期间将变化为不同值的第二链路层地址。

[0049] 设备100的链路层114被配置为在由WLAN 204中的AP传输的信息(例如,消息或信息元素)中检测AP支持链路层地址保护特征,该特征提供设备100使用不同的链路层地址。链路层114被配置为向AP发送指示以请求关于AP是否支持链路层地址保护特征的信息。

[0050] 在一些示例中,LAN MAC保护的STA可以通过包括LAN MAC保护元素或通过在(重新)关联请求帧中设置LAN MAC地址隐私指示符来请求LAN MAC保护特征的使用。

[0051] LAN MAC保护的STA A、B和C维持两个MAC地址:在相应的STA与AP关联的持续时间内不改变的LAN MAC地址,以及在持续时间期间可以改变的AIR MAC地址。AIR MAC地址被使用在LAN MAC保护的STA和AP之间传输的帧中。LAN MAC地址被用来转发以有线LAN 206为目的地的帧。每个LAN MAC保护的STA A、B或C在STA与ESS中的AP关联的持续时间内维持其相应的LAN MAC地址。每个LAN MAC保护的STA A、B或C根据STA的MAC地址轮换/改变策略来维持其AIR MAC地址。

[0052] AP(202-1或202-2)管理用于LAN MAC保护的STA(其中LAN MAC保护已被启用)的地址解析。每个LAN MAC保护的STA A、B或C都可以使用代理ARP进行地址解析。有线LAN 206上的STA D也可以使用代理ARP进行地址解析。

[0053] AP(202-1或202-2)用STA D的LAN MAC地址来响应来自LAN侧上的STA(STA D)的ARP请求。AP(202-1或202-2)进一步使用STA A、B或C的AIR MAC地址来响应来自空中侧LAN MAC保护的STA A、B或C的ARP请求(即,AP用STA的LAN MAC地址和AIR MAC地址两者来响应来自空中侧LAN MAC保护的STA的ARP请求)。

[0054] 如图2进一步所示,每个AP 202-1或202-2分别包括相应的LAN MAC-AIR MAC映射表(或另一种格式的映射信息)208-1或208-2。每个LAN MAC-AIR MAC映射表208-1或208-2包括多个条目,其中多个条目中的每个条目将对应STA的LAN MAC地址映射到对应STA的AIR MAC地址。例如,LAN MAC-AIR MAC映射表208-1或208-2的每个条目可以是包括两个元素的双元组:LAN MAC地址和映射到LAN MAC地址的对应AIR MAC地址。

[0055] 在一些示例中,相应AP 202-1和202-2中的LAN MAC-AIR MAC映射表208-1和208-2彼此同步(210),即,LAN MAC-AIR MAC映射表208-1和208-2之一的任何改变被传播到LAN MAC-AIR MAC映射表208-1和208-2中的另一个。

[0056] 注意,每个LAN MAC保护的STA(A、B或C)还可以维持相应的LAN MAC-AIR MAC双元组,其包括AP的LAN MAC地址和映射到LAN MAC地址的对应AIR MAC地址。

[0057] 下面描述其中使用LAN MAC保护特征的数据路由的示例。

[0058] 1.LAN MAC保护的STA在到WLAN 204的空中链路上使用随机化MAC地址(AIR MAC地址)来发现并建立LAN接入。当LAN MAC保护的STA与LAN 206建立状态时,LAN MAC保护的STA使用数据帧的IEEE 802.11报头中的随机化MAC地址来寻址通过空中链路发送的帧。

[0059] 2.LAN MAC保护的STA使用不同的MAC地址(LAN MAC地址),例如其全球唯一的MAC地址或本地管理的(例如,IEEE 802.1CQ分配的)MAC地址,以通过LAN(有线局域网206)进行通信。

[0060] 3.对于单播业务(其是由传输设备传输到个体目标设备的业务),AP 202-1或202-

2维持用于使用双元组进行单播通信的关联STA(其与AP关联)的映射,其每个都包括对应AIR MAC地址和对应LAN MAC地址。双元组是上面指出的LAN MAC-AIR MAC映射表208-1或208-2的一部分。LAN MAC保护的STA和AP之间的管理业务使用AIR MAC地址作为源或目标MAC地址进行寻址。在一些示例中,存在用于处理LAN中的MAC寻址的两种机制:

[0061] (a)LAN报头在空中链路上被隧道传输。LAN MAC保护的STA的IP栈被绑定到LAN MAC地址。AP和LAN MAC保护的STA之间的单播业务使用AIR MAC地址。

[0062] (b)LAN MAC保护的STA和AP使用AIR MAC地址通过空中链路进行通信。当AP从LAN MAC保护的STA或以LAN MAC保护的STA为目的地的那些接收帧时,AP将帧中的AIR MAC地址替换为LAN MAC地址,反之亦然。

[0063] 注意:对于上面的机制(a),AIR MAC地址的存在对于LAN MAC保护的STA或AP的操作系统(OS)和(多个)上层(例如,IP栈)是完全透明的。此外,LAN MAC地址和AIR MAC地址(在双元组中)之间的转换由LAN MAC保护的STA或AP的WLAN驱动程序负责。LAN MAC保护的STA和AP之间建立隧道。

[0064] 对于上面的机制(b),双元组对于LAN MAC保护的STA或AP的OS而言是已知的,并且OS在传输帧时使用正确的地址(AIR MAC地址或LAN MAC地址)。

[0065] 4.对于广播/多播业务(其是由源设备使用群组地址向多个目标设备传输的业务),上行链路业务(从LAN MAC保护的STA到AP)以上面讨论的方式被视为单播业务。下行链路广播/多播业务不使用LAN MAC保护的STA的MAC地址,因此下行链路广播/多播业务以传统设备使用的方式来发送(利用报头字段中的群组地址)。

[0066] 5.在LAN MAC保护的STA与AP的关联的生命周期期间,AIR MAC地址可以改变,而LAN MAC地址保持不变。这允许与LAN 206的无缝连接,同时减轻观察者长时间跟踪LAN MAC保护的STA。

[0067] 在LAN MAC保护的STA和AP之间使用AIR MAC地址来交换管理帧,因此无线通信不使用LAN MAC地址。具体而言,802.11报头中的3个或4个地址中的任何一个的值都不被设置为去往AP或来自AP的任何通信中的LAN MAC地址。LAN MAC地址仅在加密帧(数据帧或管理帧)内使用隧道传输在AP和STA之间进行交换。

[0068] 在一些示例中,AP的链路层从STA接收以目的地设备为目标的帧,将接收到的帧中的AIR MAC地址变换(使用AP中的LAN MAC-AIR MAC映射表)为对应的LAN MAC地址,并且将对应的LAN MAC地址包括在发送给目的地设备的帧中。

[0069] 在进一步的示例中,AP的链路层从源设备接收以STA为目标的帧,(使用AP中的LAN MAC-AIR MAC映射表)将帧中的LAN MAC地址变换为对应的AIR MAC地址,并且将对应的AIR MAC地址包括在发送给STA的帧中。

[0070] 当LAN MAC保护特征被启用时,用于STA和AP的安全关联被绑定到AIR MAC地址。例如,设备100包括作为协议栈110一部分的安全层,其中安全层被配置为使用AIR MAC地址来绑定设备100和WLAN 204的AP之间的安全关联。

[0071] 这与传统STA行为一致。从安全角度来看,LAN MAC地址保护特征的工作如下,如图3中所示。

[0072] 基于管理帧(在302)从STA 300(LAN MAC保护的STA)到AP 202(AP 202-1或202-2之一)的传输,PMK(成对主密钥)和PTK(成对临时密钥)衍生被绑定到AIR MAC地址,该地址

被用于初始关联到WLAN 204中的AP。安全层被配置为使用AIR MAC地址来得出PMK和PTK。设备100的安全层与AP绑定的安全关联是PTKSA(PTK安全关联)。

[0073] 由于在STA 300处的AIR MAC地址的改变,管理帧包括新的AIR MAC地址。注意,即使AIR MAC地址的改变导致新的关联(在链路层114),(多个)较高层(116)的连接或其他关联不变。链路层114之上的较高层被配置为在AIR MAC层地址改变时基于LAN MAC地址来维持与LAN 206的连接。

[0074] 响应于管理帧,STA 300关闭(在304处)STA 300处的802.1x端口,并且AP 202关闭(在306处)AP 202处的802.1x端口。关闭802.1x端口是指IEEE 802.1X中指定的虚拟端口的删除。

[0075] 在STA 300和AP 202之间执行(在308处)4向握手以建立STA 300和AP 202之间的关联。在4向握手的消息4中,STA 300加密并在密钥描述符元素(KDE)中将其LAN MAC地址发送到AP 202。

[0076] 当STA 300轮换(改变)其AIR MAC地址时,STA 300向AP 200发送信号以协商新的PTK。该过程工作如下。

[0077] (A)STA 300轮换其AIR MAC地址并且通过用信号发送LAN MAC地址隐私指示符来(重新)关联到AP 202。STA 300和AP 202使用RSNA(稳健安全网络关联、SAE(对等同时认证)、FT(快速基本服务集(BSS)转变)或FILS(快速初始链路设置)协议中的任何一个来协商新的PTKSA(成对临时密钥安全关联)。在4向握手、FT或FILS交换的最后一条消息期间,STA 300在KDE(密钥数据封装)中将LAN MAC地址发送到AP 202。

[0078] (B)STA 300可以使用替代管理帧来用信号发送新的PTKSA的协商。例如,可以修改SA(安全关联)查询帧以触发AP 202发起4向握手以得出新的PTKSA。

[0079] 当4向握手完成时(如从AP 202向STA 300发送(在310处)的成功指示所指示的),IEEE 802.1X控制端口被STA 300和AP 202打开(分别在312和314处)并且STA 300和AP 202各自存储(分别在316和318处)包含映射的AIR MAC地址和LAN MAC地址的双元组。

[0080] 为了保护隐私,可以与AIR MAC地址的改变同步地改变附加的标识符。这包括MAC帧序列计数器、PHY OFDM(正交频分多址)数据加扰器和/或其他标识符。

[0081] 轮换MAC地址意味着改变MAC地址。MAC地址的改变可以采用随机地址或伪随机地址的选择,或者使用其他算法选择的地址。改变后的MAC地址不必是循环的。MAC地址改变可以在改变发生时进行协商,或者MAC地址可以通过AP和STA都可以独立计算下一个AIR MAC地址的方式来确定。

[0082] 在一些示例中,LAN MAC保护的STA使用扩展能力位或其他指示符来通告其对LAN MAC保护特征的支持。

[0083] 在一些示例中,AP使用扩展能力位或其他指示符来通告其对LAN MAC保护特征的支持。

[0084] 在一些示例中,LAN MAC保护的STA可以基于AP的LAN MAC保护能力来决定是否关联到AP。LAN MAC保护的STA可以以多种不同的方式进行配置。如果AP不支持LAN MAC保护特征,则LAN MAC保护的STA可以以旧有模式进行关联。如果AP支持LAN MAC保护特征,则LAN MAC保护的STA可以避免以旧有模式进行关联。LAN MAC保护的可以在以旧有模式进行关联之前提示用户。

[0085] 任何前述内容的使用可以基于相关于隐私的不同用户偏好,以及使用旧有模式引起的隐私损失。还可以在LAN MAC保护的STA中存储允许用于旧有模式的网络列表或者不使用白名单或黑名单机制。

[0086] 类似地,AP可以具有允许或禁止STA以旧有模式进行连接的策略。

[0087] STA的扫描算法可以考虑LAN MAC保护特征并且以比不支持它的那些更高的优先级连接到支持该特征的AP。

[0088] 3.2实现2:TDLS

[0089] 对等设备将包括它们的LAN MAC保护元素或扩展能力位作为TDLS(隧道直接链路设置)链路设置和TDLS发现帧的一部分。

[0090] TDLS允许在同一WLAN中操作的STA之间的直接通信。在没有TDLS的情况下,所有帧都必须从源STA传输到AP,然后从AP传输到目的地STA。TDLS技术通过使得源STA能够直接向目的地STA传输数据,从而允许无线介质的使用减少近一半。TDLS技术已在IEEE 802.11z修正案中被标准化,并且自2012年起在Wi-Fi联盟认证计划中进行测试。它被广泛部署在消费类和企业WLAN装备中。

[0091] 根据本公开的一些实现,如果发起TDLS STA已关联到启用了LAN MAC地址隐私的AP,则发起TDLS STA在TDLS链路设置帧中包括设置为指定值(以指示对LAN MAC保护特征的支持)的LAN MAC隐私元素或能力位。如果响应方STA已关联到具有LAN MAC保护的AP并接收到包括设置为指定值的LAN MAC隐私元素或能力位的TDLS链路设置帧,则响应方STA通过在响应中包括LAN MAC保护元素或扩展能力来进行响应。此信息允许任一TDLS对等体优雅地处理TDLS链路的拆除——如果另一个对等体改变其MAC地址的话。

[0092] 一旦TDLS链路设置成功完成,则两个对等设备将使用它们的AIR MAC地址来交换帧。如果其中一个对等设备改变其AIR MAC地址,则TDLS链接将被断开。在改变之后随后用新地址重新建立TDLS链路。

[0093] 3.3实现3:加密MAC地址

[0094] 前述是指轮换AIR MAC地址,改变AIR MAC地址,或者挑选随机AIR MAC地址。这样做的一种机制是从本地地址空间(诸如46位数字空间)中挑选随机MAC地址。这与也随机挑选地址的其他设备发生冲突的概率非常小但非零。一些标准进一步将本地地址空间划分为四个象限,每个象限为44位。在设备挑选新地址之后,设备将新地址通知AP。这可能涉及管理帧的交换。从长远来看,还有其他挑选使用较少管理帧的新MAC地址的替代方法。

[0095] 加密MAC地址的使用可以减少与协商或通知AP或STA新的AIR MAC地址在改变之后将是什么相关联的通信。只有AP和STA知道序列和/或种子的加密序列允许两个设备独立地得出序列中的下一个AIR MAC地址。这可以通过确定性伪随机数生成器来实现。该算法的密码属性使得间歇性被动观察者无法将旧地址和新地址相关,而每个知道这些值的AP和STA都可以计算出序列中的相同的下一个地址。

[0096] 3.4实现4:802.11be多链路地址

[0097] 该实现依附于当前任务组IEEE 802.11be正在为多链路设备所做的事情。

[0098] 在日期为2020年1月的IEEE 802.11-19/1899r7“MLAMAC Addresses Considerations”中描述的IEEE 802.11be提出了用于下一代WLAN的技术或机制。IEEE 802.11be修正案将定义能够支持最大吞吐量至少30Gbps的超高吞吐量(EHT)PHY和MAC层。

IEEE 802.11be修正案正在研究一种被称为多链路设备(MLD)的多链路聚合技术。

[0099] IEEE 802.11be引入了“MLD地址”,当使用多个链路时,该MLD地址在LAN上被使用。设备(诸如设备100)的多个链路用于设备与无线网络(诸如图2的WLAN 204)的各个AP的关联。

[0100] 多链路设备概念引入了个体LINK MAC地址到MLD(设备)地址的映射。在IEEE 802.11be中,个体LINK MAC地址将被视为AIR MAC地址,它可以被映射到不通过空中传输的LAN MAC地址(MLD地址)。

[0101] 根据本公开的一些实现,认证和PTK生成是基于MLD MAC地址(LAN MAC地址)的,而只有(多个)LINK MAC地址((多个)AIR MAC地址)被用于SA/TA/RA/DA地址字段中。

[0102] 本公开的实现引入了对MLD提议的改变,以使得长期存在的MLD MAC地址免受窃听。为此,只有LINK MAC地址对空中观察者可见。本公开的实现还使用与以上3.1节中讨论的那些技术类似的技术来添加协议以使得LINK MAC地址能够在关联期间进行改变而不丢弃。

[0103] 使用具有LINK MAC地址(AIR MAC地址)和MLD地址(LAN MAC地址)的这种方案,即使当STA仅通过单个链路进行连接时也是提供以上3.1节中的LAN MAC保护特征的示例实现。

[0104] 更一般地,设备可以建立与多个AP的关联以用于与AP的多个链路。设备的链路层被配置为为多个链路维持相应不同的空中链路地址,其中空中链路地址在关联的持续时间期间每个都是可变的。

[0105] 4.示例益处

[0106] 本公开的实现允许保护用户隐私,该用户隐私基于第二链路层地址的使用来保护第一链路层地址(其在无线设备与AP的关联期间保持不变),该第二链路层地址可以在关联期间改变一次或多次。以这种方式,第一链路层地址不必以未加密的形式在空中被传输,诸如在IEEE 802.11 MAC报头中。相反,未加密的IEEE 802.11 MAC报头包含第二链路层地址,而第一链路层地址可以作为包括IEEE 802.11 MAC报头的帧中的有效负载进行隧道传输(并加密)。

[0107] 例如,在本地地址空间中使用MAC地址而不使用用于所有WLAN业务的全局分配的MAC地址的益处是:它防止了长时间的跟踪。在跟踪对手是被动观察者的情况下,它防止了跨不同位置的跟踪,因为大多数实现将扫描操作中使用的地址随机化,并在与网络进行关联时为每个SSID使用不同的地址。在一些情况下,MAC地址改变实现还提供来自网络提供商的隐私。

[0108] 存储介质(例如,图1中的108)可以包括以下中的任意或某种组合:半导体存储器设备,诸如动态或静态随机存取存储器(DRAM或SRAM)、可擦除和可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)和闪存或其他类型的非易失性存储器设备;磁盘,诸如固定磁盘、软磁盘和可移除磁盘;其他类型的磁介质,包括磁带;诸如压缩盘(CD)或数字视盘(DVD)之类的光学介质;或其他类型的存储设备。注意,可以在一个计算机可读或机器可读存储介质上提供上面讨论的指令,或者可替代地,可以在分布在可能具有多个节点的大型系统中的多个计算机可读或机器可读存储介质上提供上面讨论的指令。一个或多个这种计算机可读或机器可读存储介质被认为是物品(或制品)的一部分。物品或制品可

以指的是任何制造的单个组件或多个组件。存储介质可以位于运行机器可读指令的机器中，或者位于可以通过网络从其下载机器可读指令以执行的远程站点处。

[0109] 在前述描述中，阐述了许多细节以提供对本文所公开的主题的理解。然而，可以在没有这些细节中的一些细节的情况下实践各种实现。其他实现可以包括对上述细节的修改和变化。所附权利要求旨在涵盖此类修改和变化。

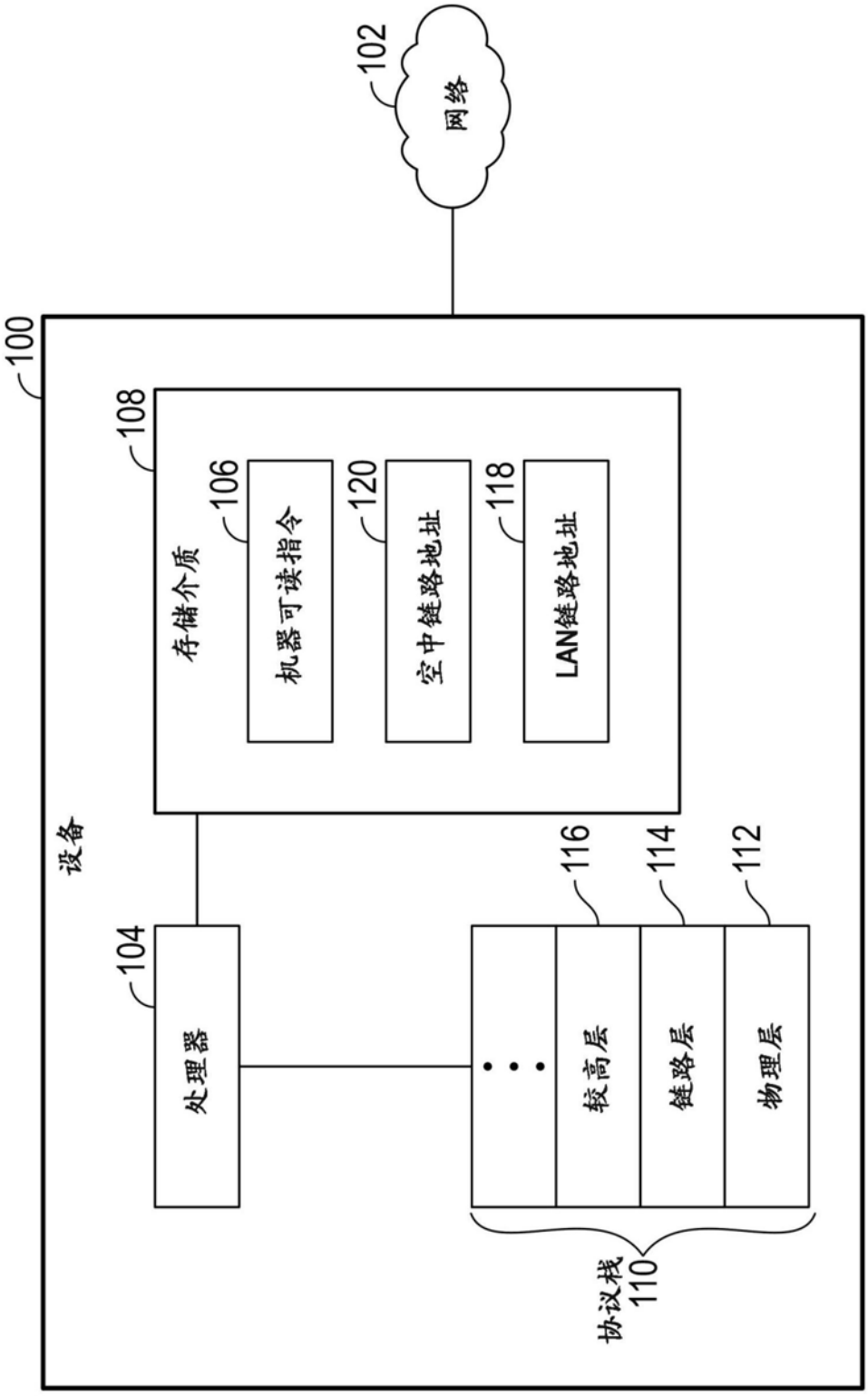

102
网络
100
设备
108
存储介质
106
机器可读指令
120
空中链路地址
118
LAN链路地址
104
处理器
116
较高层
114
链路层
112
物理层
协议栈
110

图1

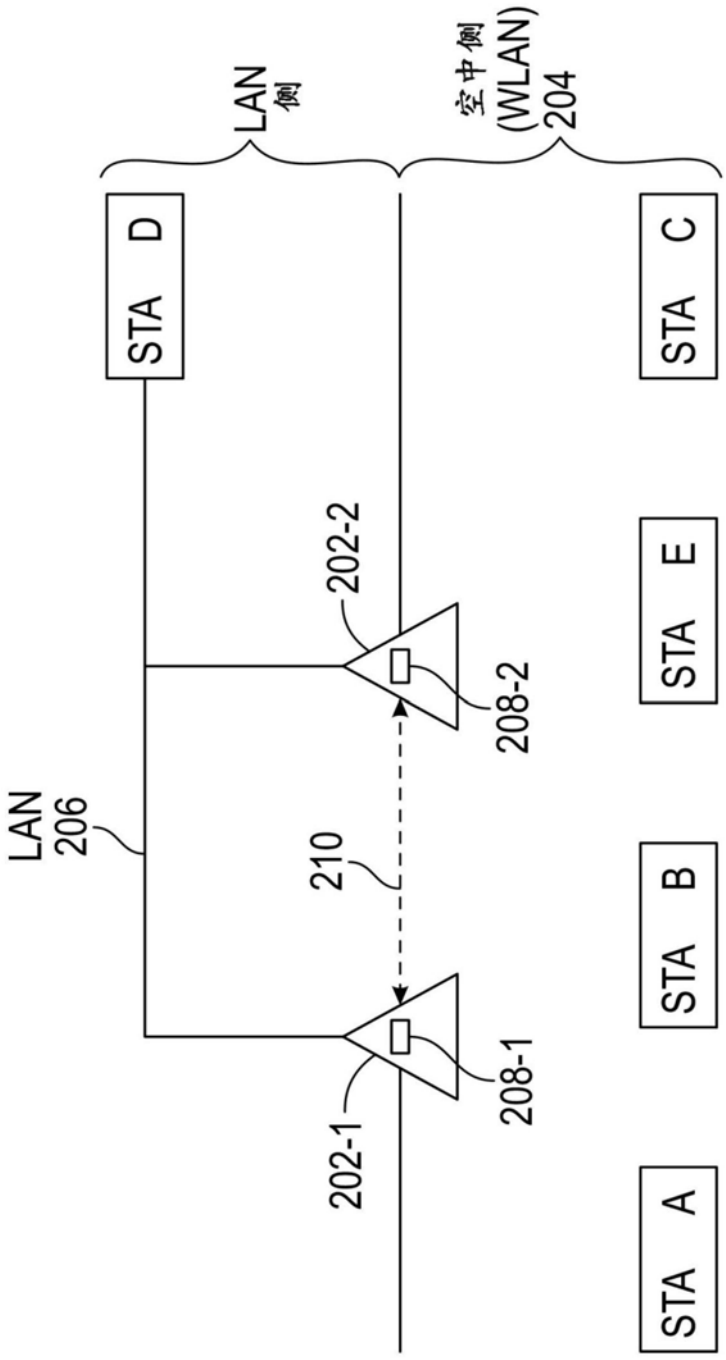

LAN
侧
空中侧
(WLAN)
204
STA D
STA C
202-2
208-2
STA E
LAN
206
210
STA B
208-1
202-1
STA A

图2

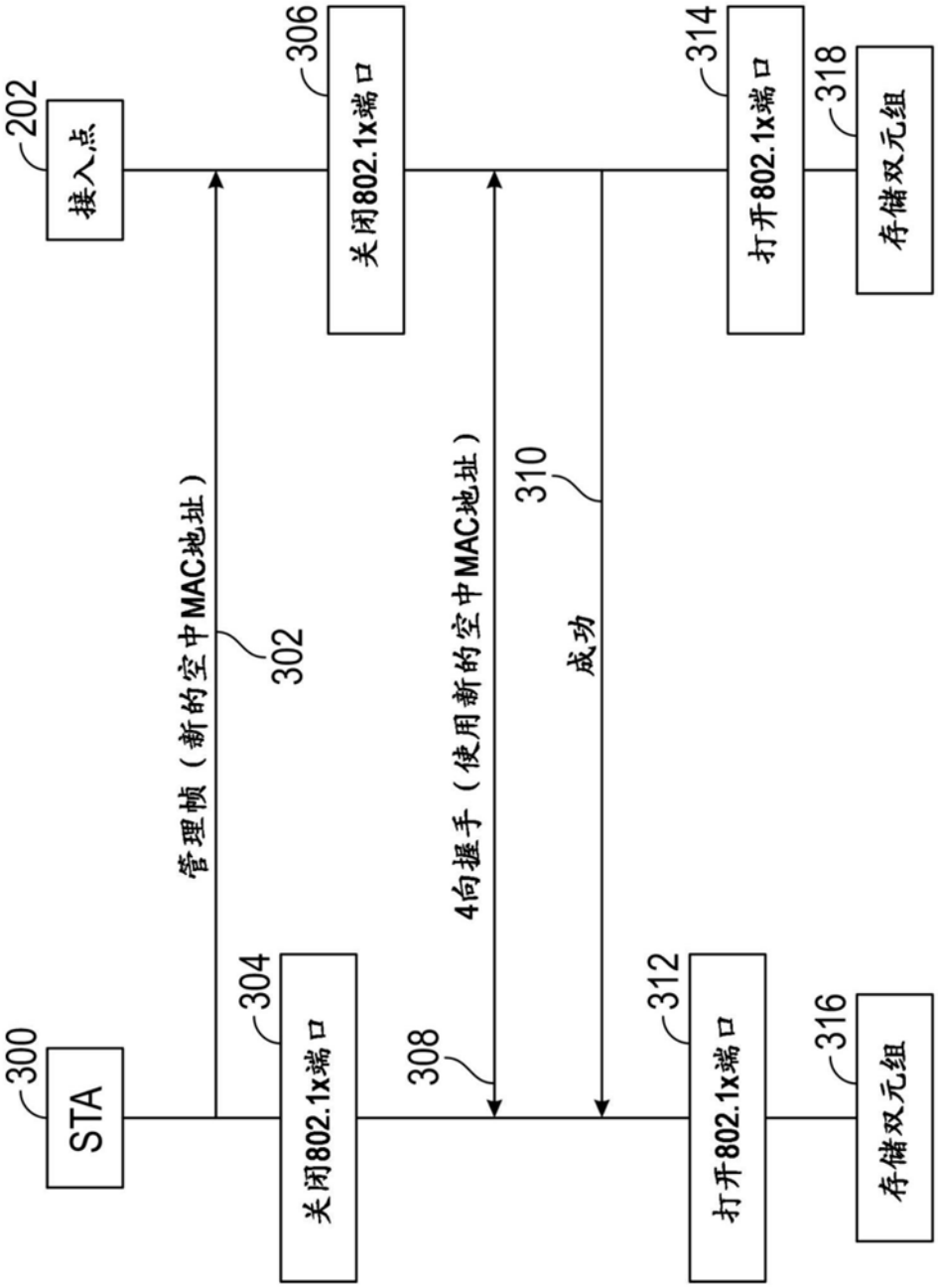

202
接入点
306
关闭802.1x端口
314
打开802.1x端口
318
存储双元组
管理帧（新的空中MAC地址）
302
4向握手（使用新的空中MAC地址）
310
成功
300
STA
304
关闭802.1x端口
308
312
打开802.1x端口
316
存储双元组

图3