(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 104685934 A
(43)申请公布日 2015.06.03

(21)申请号 201380035100.1
(22)申请日 2013.07.02
(30)优先权数据
61/667,600 2012.07.03 US
61/695,177 2012.08.30 US
(85)PCT国际申请进入国家阶段日
2014.12.30
(86)PCT国际申请的申请数据
PCT/US2013/049034 2013.07.02
(87)PCT国际申请的公布数据
WO2014/008238 EN 2014.01.09
(71)申请人 交互数字专利控股公司
地址 美国特拉华州
(72)发明人 L·王 R·G·穆里亚斯 Y·塔加利 张国栋 R·L·奥勒森
(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 陈潇潇 刘国平
(51)Int.Cl.
H04W 48/12(2006.01)
H04W 48/18(2006.01)
H04W 36/00(2006.01)

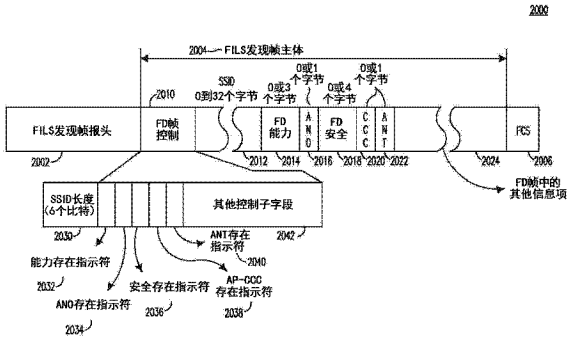
权利要求书2页 说明书24页 附图23页

(54)发明名称

快速初始链路建立发现帧

(57)摘要

一种用于在无线站中的方法，该方法包括从接入点(AP)接收全信标帧的实例之间的快速初始链路建立发现(FD)帧，并基于接收到的FD帧确定是否与AP相关联。FD帧包括FD帧内容和FD帧控制字段。FD帧控制字段包括服务集标识符(SSID)长度字段，其对应于FD帧内容中可变长度SSID字段的长度；以及以下任意一者或多者：能力存在指示符、接入网络选项存在指示符、安全存在指示符、AP配置改变计数存在指示符、或AP下一个目标信标传输时间存在指示符。这些存在指示符的每一者用于指示FD帧内容中是否存在相应字段。



CN 104685934 A

1. 一种用于在无线站中的方法，该方法包括：

从接入点 (AP) 接收全信标帧的实例之间的快速初始链路建立发现 (FD) 帧，其中所述 FD 帧包括：

FD 帧内容；和

FD 帧控制字段，该 FD 帧控制字段包括：

服务集标识符 (SSID) 长度字段，该 SSID 长度字段对应于所述 FD 帧内容中的可变长度 SSID 字段的长度；及

以下中的任意一者或多者：

能力存在指示符，指示在所述 FD 帧内容中是否存在相应的能力字段；

接入网选项存在指示符，指示在所述 FD 帧内容中是否存在相应的接入网选项字段；

安全存在指示符，指示在所述 FD 帧内容中是否存在相应的安全字段；

AP 配置改变计数存在指示符，指示在所述 FD 帧内容中是否存在相应的 AP 配置改变计数字段；或

AP 下一个目标信标传输时间存在指示符，指示在所述 FD 帧内容中是否存在相应的 AP 下一个目标信标传输时间字段；以及

基于接收到的 FD 帧确定是否与所述 AP 相关联。

2. 根据权利要求 1 所述的方法，其中所述能力字段包括所述 AP 的能力信息。

3. 根据权利要求 1 所述的方法，其中所述接入网选项字段指示所述 AP 提供的接入服务。

4. 根据权利要求 1 所述的方法，其中所述安全字段指示所述 AP 使用的一种或多种类型的安全性。

5. 根据权利要求 1 所述的方法，其中所述 AP 配置改变计数字段指示 AP 配置参数集已发生改变的次数。

6. 根据权利要求 1 所述的方法，其中所述 AP 下一个目标信标传输时间字段指示来自所述 AP 的下一个全信标帧的传输时间。

7. 根据权利要求 6 所述的方法，其中所述 AP 下一个目标信标传输时间被表达为相对于 FD 帧传输时间的偏移值。

8. 根据权利要求 7 所述的方法，其中所述偏移值被表达为时间单元的数量。

9. 根据权利要求 1 所述的方法，其中所述 FD 帧控制字段还包括：

邻居 AP 信息存在指示符，指示在所述 FD 帧内容中是否存在相应邻居 AP 信息字段。

10. 根据权利要求 9 所述的方法，其中所述邻居 AP 信息字段包括操作种类字段、信道数量字段以及针对所述邻居 AP 信息字段中的每个邻居 AP 的下一个目标信标传输时间字段。

11. 根据权利要求 10 所述的方法，其中每个下一个目标信标传输时间字段指示来自相应邻居 AP 的下一个全信标帧的传输时间。

12. 根据权利要求 11 所述的方法，其中所述下一个目标信标传输时间被表达为相对于 FD 帧传输时间的偏移值。

13. 根据权利要求 12 所述的方法，其中所述偏移值被表达为时间单元的数量。

14. 根据权利要求 1 所述的方法，其中所述 FD 帧内容还包括可选字段或可选信息元素。

15. 根据权利要求 14 所述的方法，其中在所述 FD 帧内容包括任意可选字段的情况下，

对应于所述可选字段的存在指示符被包含在所述 FD 帧控制字段中。

16. 根据权利要求 1 所述的方法，该方法还包括：

在基于接收到的 FD 帧确定与所述 AP 相关联的情况下，向所述 AP 传送关联请求帧。

快速初始链路建立发现帧

背景技术

[0001] 基础设施基础服务集 (BSS) 模式中的无线局域网 (WLAN) 具有用于 BSS 的接入点 (AP) 以及与 AP 相关联的一个或多个站 (STA)。AP 典型地具有对分布系统 (DS) 或另一种类型的有线 / 无线网络 (其将业务量带入和带出 BSS) 的接入或与之对接。源自 BSS 外部至 STA 的业务量经过 AP 并被递送到 STA。源自 STA 至 BSS 外部的目的地的业务量被发送给 AP 以被递送给各自的目的地。BSS 内的 STA 之间的业务量还可以通过 AP 发送，其中源 STA 发送业务量至 AP，以及 AP 递送该业务量至目的地 STA。BSS 内的 STA 之间的业务量是真正的端到端业务量。该端到端业务量还可以使用直接链路建立 (DLS) 或隧道 DLS(TDLS) 直接在源和目的地 STA 之间被发送。独立 BSS 模式 (IBSS) 中的 WLAN 没有 AP 以及彼此直接通信的 STA。

[0002] 在基础设施 BSS 中，STA 执行扫描过程以发现合适的 AP/ 网络来通常经由关联过程建立 WLAN 链路。存在两种基础扫描模式 :被动扫描和主动扫描。

[0003] 使用被动扫描模式，AP 定期传送信标帧以向 STA 提供 AP/ 网络信息。信标通过提供 AP 通告来支持系统中各种功能，该 AP 通告具有 BSS 标识符 (BSSID)、BSS 中 STA 的同步、能力信息、BSS 操作信息、媒介接入的系统参数、发射功率限制等。此外，信标可以携带多种可选信息元素。

[0004] 使用主动扫描模式，STA 主动生成探测请求帧并将其传送给 AP，从 AP 接收探测响应帧，并处理该探测响应帧以获取 AP/ 网络信息。

[0005] 图 1 示出了信标帧 100 的一般帧格式，该信标帧 100 包括媒介接入控制 (MAC) 报头 102、帧主体 104 以及帧校验序列 (FCS) 字段 106。MAC 报头 102 包括帧控制字段 110、持续时间字段 112、多个地址字段 114-118、序列控制字段 120 以及高吞吐量 (HT) 控制字段 122。

[0006] 帧主体 104 包括强制字段和信息元素 (IE)，包括但不限于 (图 1 中未示出) 时间戳字段、信标间隔字段、能力字段、服务集标识符 (SSID) 字段、支持的速率字段以及一个或多个可选 IE，例如 BSS 负载信息。BSS 负载信息指示 BSS 处的业务量加载水平，并可以包括 5 个相关 IE :BSS 负载，包括 STA 计数、信道利用和准许能力 ;BSS 可用准许容量 ;服务质量 (QoS) 业务量能力 ;BSS 平均接入延迟 ;以及 BSS 接入类别 (AC) 接入延迟。对于强制和典型的可选 IE，信标帧的长度可以超过 100 字节。在典型的企业环境中，信标长度大约是 230 字节。

[0007] 快速初始链路建立 (FILS) 的目标是支持 100ms 内的用于 STA 的初始链路建立时间以及支持至少 100 个同时进入 BSS 的非 AP STA 以及 1 秒内的快速链路建立。由于信标可以用于在初始链路建立过程开始时向 STA 提供关于 AP 的信息，信标可以包括用于促进快速链路建立以满足指定功能需求的信息。

[0008] FILS 过程包括 5 个阶段 :(1)AP 发现 ;(2) 网络发现 ;(3) 附加定时同步功能 (TSF) ;(4) 认证和关联 ;(5) 较高层 IP 建立。

发明内容

[0009] 一种用于在无线站中的方法，该方法包括从接入点 (AP) 接收全信标帧的实例之间的快速初始链路建立发现 (FD) 帧，并基于接收到的 FD 帧确定是否与 AP 相关联。FD 帧包括 FD 帧内容和 FD 帧控制字段。FD 帧控制字段包括服务集标识符 (SSID) 长度字段，其对应于 FD 帧内容中可变长度 SSID 字段的长度；以及以下任意一者或多者：能力存在指示符、接入网络选项存在指示符、安全存在指示符、AP 配置改变计数存在指示符、或 AP 下一个目标信标传输时间存在指示符。这些存在指示符的每一者用于指示 FD 帧内容中是否存在相应字段。

附图说明

[0010] 从以下通过示例方式给出并结合附图的描述中可以得到更详细的理解，其中：

[0011] 图 1 是信标帧格式的图；

[0012] 图 2A 是可以在其中实施一个或多个公开的实施方式的示例通系统的系统图；

[0013] 图 2B 是可以在图 2A 中示出的通信系统中使用的示例无线发射 / 接收单元 (WTRU) 的系统图；

[0014] 图 2C 是可以在图 2A 中示出的通信系统中使用的示例无线电接入网和示例核心网的系统图；

[0015] 图 3 是测量导频帧格式的图；

[0016] 图 4 是短信标帧格式的图；

[0017] 图 5 是用于 FD 帧中的接入网选项信息元素格式的图；

[0018] 图 6 是用于 FD 帧中的邻居 AP 信息元素格式的图；

[0019] 图 7 是用于 FD 帧中的鲁棒安全网络元素 (RSNE) 的图；

[0020] 图 8 是用于 FD 帧中的固定长度的优化的 RSNE 的图；

[0021] 图 9 是用于 FD 帧中的可变长度的优化的 RSNE 的图；

[0022] 图 10 是用于 FD 帧中的优化的 RSNE 的固定长度位图编码的图；

[0023] 图 11 是用于 FD 帧中的固定长度的两个八位位组的优化的 RSNE 的图；

[0024] 图 12 是用于 FD 帧中的具有 RSN 能力的两个八位位组的优化的 RSNE 的图；

[0025] 图 13 是用于 FD 帧中的 HT 物理层特定信息元素的图；

[0026] 图 14 是用于 FD 帧中的极高吞吐量 (VHT) 物理层特定信息元素的图；

[0027] 图 15 是 FD 帧控制字段格式的图；

[0028] 图 16A-16B 是示意性 FD 帧 SSID 设计的图；

[0029] 图 17 是 FD 帧能力信息项格式的图；

[0030] 图 18 是 FD 帧安全信息项格式的图；

[0031] 图 19 是可变长度的 FD 帧安全信息项格式的图；

[0032] 图 20 是 FD 帧 AP 的下一个 TBTT 信息项格式的图；

[0033] 图 21 是 FD 帧邻居 AP 信息项格式的图；

[0034] 图 22 是示意性 FD 帧主体格式的图；

[0035] 图 23 是可扩展 FD 帧主体格式的图；

[0036] 图 24 是公共动作帧格式中的 FD 帧的图；

[0037] 图 25 是具有单独帧控制字段的 FD 扩展帧格式的图；以及

[0038] 图 26 是具有组合帧控制字段的 FD 扩展帧格式的图。

具体实施方式

[0039] 图 2A 是在其中一个或多个公开的实施方式可得以实施的示例通信系统 200 的图。通信系统 200 可以是向多个无线用户提供诸如语音、数据、视频、消息、广播等这样的内容的多接入系统。通信系统 200 可使多个无线用户能够通过共享包括无线带宽的系统资源来访问这样的内容。例如，通信系统 200 可采用一个或多个信道接入方法，例如码分多址 (CDMA)、时分多址 (TDMA)、频分多址 (FDMA)、正交 FDMA(OFDMA)、单载波 FDMA(SC-FDMA) 等。

[0040] 如图 2A 所示，通信系统 200 可包括无线发射 / 接收单元 (WTRU)202a、202b、202c、202d、无线电接入网 (RAN)204、核心网 206、公共交换电话网 (PSTN)208、因特网 210 和其它网络 212，但是将理解公开的实施方式设想任意数目的 WTRU、基站、网络和 / 或网络元件。WTRU 202a、202b、202c、202d 的每一个可以是任意类型的、被配置为在无线环境中运行和 / 或通信的装置。以示例的方式，WTRU 202a、202b、202c、202d 可被配置为发送和 / 或接收无线信号，并且可包括用户设备 (UE)、移动站、固定或移动用户单元、寻呼机、蜂窝电话、个人数字助手 (PDA)、智能电话、膝上型计算机、上网本、个人计算机、无线传感器、消费电子产品等。

[0041] 通信系统 200 还可包括基站 214a 和基站 214b。基站 214a、214b 的每一个可以是任意类型的、被配置为与 WTRU 202a、202b、202c、202d 的至少一个无线接口以便于接入一个或多个诸如核心网 206、因特网 210 和 / 或其他网络 212 这样的通信网络的装置。以示例的方式，基站 214a、214b 可以是基地收发信机站 (BTS)、节点 B、e 节点 B、家用节点 B、家用 e 节点 B、站点控制器、接入点 (AP)、无线路由器等。虽然基站 214a、214b 每一个被图示为单一元件，应理解基站 214a、214b 可包括任意数目的互连基站和 / 或网络元件。

[0042] 基站 214a 可以是 RAN 204 的一部分，RAN 204 还可包括其它基站和 / 或网络元件 (未示出)，例如基站控制器 (BSC)、无线电网络控制器 (RNC)、中继节点等。基站 214a 和 / 或基站 214b 可被配置为在可被称为小区 (未示出) 的特定地理区域内发送和 / 或接收无线信号。小区可进一步被划分为小区扇区。例如，与基站 214a 相关联的小区可被划分为 3 个扇区。因此，在一个实施方式中，基站 214a 可包括 3 个收发信机，即小区的每个扇区一个。在另一个实施方式中，基站 214a 可采用多输入多输出 (MIMO) 技术，因此可针对小区的每个扇区使用多个收发信机。

[0043] 基站 214a、214b 可通过空中接口 216 与 WTRU 202a、202b、202c、202d 的一个或多个通信，空中接口 216 可以是任意适当的无线通信链路 (例如射频 (RF)、微波、红外 (IR)、紫外 (UV)、可视光等)。空中接口 216 可使用任意适当的无线电接入技术 (RAT) 来建立。

[0044] 更具体地，如上所述，通信系统 200 可以是多接入系统，并且可采用一个或多个信道接入方案，例如 CDMA、TDMA、FDMA、OFDMA、SC-FDMA 等。例如，RAN 204 中的基站 214a 和 WTRU 202a、202b、202c 可实现诸如通用移动电信系统 (UMTS) 陆地无线电接入 (UTRA) 这样的无线电技术，其可使用宽带 CDMA(WCDMA) 来建立空中接口 216。WCDMA 可包括诸如高速分组接入 (HSPA) 和 / 或演进型 HSPA(HSPA+) 这样的通信协议。HSPA 可包括高速下行链路分组接入 (HSDPA) 和 / 或高速上行链路分组接入 (HSUPA)。

[0045] 在另一个实施方式中，基站 214a 和 WTRU 202a、202b、202c 可实现诸如演进型

UMTS 陆地无线电接入 (E-UTRA) 这样的无线电技术，其可使用长期演进 (LTE) 和 / 或高级 LTE(LTE-A) 来建立空中接口 216。

[0046] 在其它实施方式中，基站 214a 和 WTRU 202a、202b、202c 可实现诸如 IEEE 802.16(即微波接入全球互通 (WiMAX))、CDMA2000、CDMA20001X、CDMA2000 EV-DO、临时标准 2000(IS-2000)、临时标准 95(IS-95)、临时标准 856(IS-856)、全球移动通信系统 (GSM)、增强型数据速率 GSM 演进技术 (EDGE)、GSM EDGE(GERAN) 等这样的无线电技术。

[0047] 图 2A 中的基站 214b 可以是例如无线路由器、家用节点 B、家用 e 节点 B 或接入点，并且可使用任意适当的 RAT 以便局部区域中的无线连接性，例如商业地点、家庭、车辆、校园等。在一个实施方式中，基站 214b 和 WTRU202c、202d 可实现诸如 IEEE 802.11 这样的无线电技术，以建立无线局域网 (WLAN)。在另一个实施方式中，基站 214b 和 WTRU 202c、202d 可实现诸如 IEEE 802.15 这样的无线电技术，以建立无线个域网 (WPAN)。仍然在另一个实施方式中，基站 214b 和 WTRU 202c、202d 可使用基于蜂窝的 RAT(例如 WCDMA、CDMA2000、GSM、LTE、LTE-A 等) 来建立微微小区 (picocell) 或毫微微小区 (femtocell)。如图 2A 所示，基站 214b 可与因特网 210 有直接连接。因此，基站 214b 不需要通过核心网 206 接入因特网 210。

[0048] RAN 204 可与核心网 206 通信，核心网 206 可以是任意类型的、被配置为向 WTRU 202a、202b、202c、202d 的一个或多个提供语音、数据、应用和 / 或通过网际协议的语音 (VoIP) 服务的网络。例如，核心网 206 可提供呼叫控制、计费服务、基于移动位置的服务、预付费呼叫、因特网连接、视频发布等，和 / 或执行诸如用户认证这样的高级安全功能。虽然未在图 2A 中示出，应理解 RAN 204 和 / 或核心网 206 可与采用与 RAN 204 相同 RAT 或不同 RAT 的其它 RAN 直接或间接通信。例如，除了与可采用 E-UTRA 无线电技术的 RAN 204 连接之外，核心网 206 还可与采用 GSM 无线电技术的另一个 RAN(未示出) 通信。

[0049] 核心网 206 还可作为网关，用于 WTRU 202a、202b、202c、202d 接入 PSTN 208、因特网 210 和 / 或其它网络 212。PSTN 208 可包括提供传统旧电话业务 (POTS) 的电路交换电话网络。因特网 210 可包括使用通用通信协议的互连计算机网络和装置的全球系统，例如传输控制协议 (TCP)/ 网际协议 (IP) 因特网协议系列中的 TCP、用户数据报协议 (UDP) 和 IP。网络 212 可包括由其它服务供应商所有和 / 或运营的有线或无线通信网络。例如，网络 212 可包括与可采用与 RAN 204 相同 RAT 或不同 RAT 的一个或多个 RAN 相连接的另一个核心网。

[0050] 在通信系统 200 中的 WTRU 202a、202b、202c、202d 的一些或所有可包括多模能力，例如 WTRU 202a、202b、202c、202d 可包括用于通过不同无线链路与不同无线网络通信的多个收发信机。例如，图 2A 中示出的 WTRU202c 可被配置为与可采用基于蜂窝的无线电技术的基站 214a 和与可采用 IEEE 802 无线电技术的基站 214b 通信。

[0051] 图 2B 是示例 WTRU 202 的系统图。如图 2B 所示，WTRU 202 可包括处理器 218、收发信机 220、发射 / 接收元件 222、扬声器 / 麦克风 224、键盘 226、显示器 / 触摸板 228、不可移除存储器 230、可移除存储器 232、电源 234、全球定位系统 (GPS) 芯片组 236 和其它外围设备 238。应理解，WTRU 202 可包括前述元件的任意子组合，而与实施方式保持一致。

[0052] 处理器 218 可以是通用处理器、专用处理器、传统处理器、数字信号处理器 (DSP)、多个微处理器、与 DSP 核相关联的一个或多个微处理器、控制器、微控制器、专用集成电路

(ASIC)、现场可编程门阵列 (FPGA) 电路、任意其它类型的集成电路 (IC)、状态机等。处理器 218 可执行信号编码、数据处理、功率控制、输入 / 输出处理和 / 或使 WTRU 202 能够在无线环境中运行的任意其它功能。处理器 218 可与收发信机 220 相耦合，收发信机 220 可与发射 / 接收元件 222 相耦合。虽然图 2B 将处理器 218 和收发信机 220 图示为分离的部件，将理解处理器 218 和收发信机 220 可在电子封装或芯片中集成在一起。

[0053] 发射 / 接收元件 222 可被配置为通过空中接口 216 向基站 (例如基站 214a) 发送或从基站 (例如基站 214a) 接收信号。例如，在一个实施方式中，发射 / 接收元件 222 可以是被配置为发送和 / 或接收 RF 信号的天线。在另一个实施方式中，发射 / 接收元件 222 可以是被配置为例如发送和 / 或接收 IR、UV 或可视光信号的发射器 / 检测器。在另一个其它实施方式中，发射 / 接收元件 222 可以被配置为发送和接收 RF 和光信号两者。将理解，发射 / 接收元件 222 可被配置为发送和 / 或接收无线信号的任意组合。

[0054] 此外，虽然发射 / 接收元件 222 在图 2B 中被图示为单一元件，WTRU 202 可包括任意数目的发射 / 接收元件 222。更具体地，WTRU 202 可采用 MIMO 技术。因此，在一个实施方式中，WTRU 202 可包括两个或更多个用于通过空中接口 216 发送和接收无线信号的发射 / 接收元件 222(例如多个天线)。

[0055] 收发信机 220 可被配置为调制即将由发射 / 接收元件 222 发送的信号并解调由发射 / 接收元件 222 接收的信号。如上所述，WTRU 202 可具有多模能力。因此，收发信机 220 可包括例如用于使 WTRU 202 能够通过诸如 UTRA 和 IEEE 802.11 这样的多个 RAT 通信的多个收发信机。

[0056] WTRU 202 的处理器 218 可与扬声器 / 麦克风 224、键盘 226 和 / 或显示器 / 触摸板 228(例如液晶显示 (LCD) 显示单元或有机发光二极管 (OLED) 显示单元) 相耦合，并可从它们接收用户输入数据。处理器 218 还可以向扬声器 / 麦克风 224、键盘 226 和 / 或显示器 / 触摸板 228 输出用户数据。此外，处理器 218 可从诸如不可移除存储器 230 和 / 或可移除存储器 232 这样的任意类型的适当存储器访问信息，并将数据存储在其中。不可移除存储器 230 可包括随机存取存储器 (RAM)、只读存储器 (ROM)、硬盘或任意其它类型的存储器存储设备。可移除存储器 232 可包括用户身份模块 (SIM) 卡、记忆棒、安全数字 (SD) 存储卡等。在其它实施方式中，处理器 218 可从物理上不位于 WTRU 202 上 (例如在服务器或家用计算机 (未示出) 上) 的存储器访问信息，并将数据存储在其中。

[0057] 处理器 218 可从电源 234 接收功率，并可被配置为分配和 / 或控制给 WTRU 202 中其它组件的功率。电源 234 可以是任意适当的用于向 WTRU202 供电的设备。例如，电源 234 可包括一个或多个干电池 (例如镍镉 (NiCd)、镍锌 (NiZn)、镍金属氢化物 (NiMH)、锂离子 (Li-ion) 等)、太阳能电池、燃料电池等。

[0058] 处理器 218 还可以与可被配置为提供关于 WTRU 202 当前位置的位置信息 (例如经度和纬度) 的 GPS 芯片组 236 相耦合。附加于或替代来自 GPS 芯片组 236 的信息，WTRU 202 可通过空中接口 216 从基站 (例如基站 214a、214b) 接收位置信息，和 / 或基于从两个或更多个附近基站接收的信号的定时来确定它的位置。将理解，WTRU 202 可借助任何适当的位置确定方法来获取位置信息而与实施方式保持一致。

[0059] 处理器 218 可进一步与其它外围设备 238 相耦合，其它外围设备 238 可包括提供附加特征、功能和 / 或有线或无线连接的一个或多个软件和 / 或硬件模块。例如，外围设备

238 可包括加速计、电子罗盘、卫星收发信机、数字照相机（用于相片或视频）、通用串行总线 (USB) 端口、振动设备、电视收发信机、免提耳机、蓝牙®模块、调频 (FM) 无线电单元、数字音乐播放器、媒体播放器、视频游戏机模块、因特网浏览器等。

[0060] 图 2C 是根据一种实施方式的 RAN 204 和核心网 206 的系统图例。RAN204 可以是使用 IEEE 802.16 无线电技术通过空中接口 216 与 WTRU 202a、202b、202c 进行通信的接入服务网络 (ASN)。正如下文将继续讨论的，WTRU202a、202b、202c、RAN 204 的不同功能实体和核心网 206 之间的通信链路可以被定义为参考点。

[0061] 如图 2C 所示，RAN 204 可以包括基站 240a、240b、240c 和 ASN 网关 242，尽管应该理解的是 RAN 204 可以包含任意数量的基站和 ASN 网关而仍然与实施方式保持一致。基站 240a、240b、240c 分别与 RAN 204 中的特定小区（未示出）相关联，并且可以分别包括一个或多个收发信机，该收发信机通过空中接口 216 来与 WTRU 202a、202b、202c 通信。在一种实施方式中，基站 240a、240b、240c 可以使用 MIMO 技术。由此，例如基站 240a 可以使用多个天线来传送无线信号至 WTRU 202a 并且从 WTRU 202a 中接收无线信号。基站 240a、240b、240c 还可以提供移动性管理功能，例如切换触发、隧道建立、无线电资源管理、业务分类、服务质量 (QoS) 策略执行，等等。ASN 网关 282 可以作为业务汇聚点且可以负责寻呼、用户简档的缓存、路由到核心网 206，等等。

[0062] WTRU 202a、202b、202c 与 RAN 204 之间的空中接口 216 可以被定义为执行 IEEE 802.16 规范的 R1 参考点。另外，WTRU 202a、202b、202c 中的每个可以建立与核心网 206 间的逻辑接口（未示出）。WTRU 202a、202b、202c 与核心网 206 间的逻辑接口可以被定义为 R2 参考点，可以被用来认证、授权、IP 主机配置管理、和 / 或移动管理。

[0063] 基站 240a、240b、240c 中的每个之间的通信链路可以被定义为包括用于便于 WTRU 切换和基站之间的数据传输的协议的 R8 参考点。基站 240a、240b、240c 和 ASN 网关 242 之间的通信链路可以被定义为 R6 参考点。R6 参考点可以包括用于便于基于与每个 WTRU 202a、202b、202c 相关联的移动事件的移动管理的协议。

[0064] 如图 2C 所示，RAN 204 可以被连接到核心网 206。RAN 204 和核心网 206 之间的通信链路可以被定义为例如包括用于便于数据传输和移动管理能力的协议的 R3 参考点。核心网 206 可以包括移动 IP 本地代理 (MIP-HA)244，认证、授权、记账 (AAA) 服务器 246 和网关 248。尽管每个上述元件被描述为核心网 206 的一部分，但是应该理解的是这些元件中的任意一个可以被除了核心网运营商以外的实体拥有和 / 或运营。

[0065] MIP-HA 可负责 IP 地址管理，并可以使得 WTRU 202a、202b、202c 在不同 ASN 和 / 或不同核心网之间漫游。MIP-HA 244 可以向 WTRU 202a、202b、202c 提供对例如因特网 210 的分组交换网络的接入，以促进 WTRU 202a、202b、202c 与 IP 使能设备之间的通信。AAA 服务器 246 可以负责用户认证并用于支持用户服务。网关 248 可以促进与其他网络的互通。例如，网关 248 可以向 WTRU 202a、202b、202c 提供对例如 PSTN 208 的电路交换网络的接入，以促进 WTRU 202a、202b、202c 与传统路线通信设备之间的通信。此外，网关 248 可以向 WTRU 202a、202b、202c 提供对网络 212 的接入，该网络 212 可以包括其他服务提供商拥有和 / 或运营的其他有线或无线网络。

[0066] 虽然在图 2C 中没有示出，但是应当理解 RAN 204 可以连接到其他 ASN 且核心网 206 可以连接到其他核心网。RAN 204 与其他 ASN 之间的通信链路可以定义为 R4 参考点，

其可以包括用于协调 WTRU 202a、202b、202c 在 RAN 204 与其他 ASN 之间的移动性的协议。核心网 206 与其他核心网之间的通信链路可以定义为 R5 参考，其可以包括用于促进本地核心网与受访核心网之间的互通的协议。

[0067] 其他网络 212 也可连接到基于 IEEE 802.11 的无线局域网 (WLAN)260。WLAN 260 可以包括接入路由器 265。接入路由器可以包含网关功能。接入路由器 265 可以与多个接入点 (AP)270a、270b 通信。接入路由器 265 与 AP 270a、270b 之间的通信可以经由有线以太网 (IEEE 802.3 标准)，或任意类型的无线通信协议。AP 270a 通过空中接口与 WTRU 202d 进行无线通信。

[0068] 期望改进被动扫描机制以促进 FILS 和 / 或减少用于扫描的 MAC 帧的广播时间 (airtime) 占用。AP 可以传送在全信标实例之间的 MAC 帧 (这里称为“FILS 发现 (FD) 帧”) 以支持用于快速初始链路建立的快速 AP/ 网络发现。FD 帧可以周期性和 / 或非周期性被传送。如果周期性传送，则可以改变 FD 帧的周期。FD 帧是公共动作帧，其可以是以下中的一者 :修改的测量导频帧、修改的短信标帧或新设计的 MAC 公共动作帧。

[0069] FD 帧可以在 5GHz 频带的 20、40、80 和 160MHz (给定发射机的动态频率选择 (DFS) 所有权) 的 20MHz 处作为非 HT 双重物理层会聚过程 (PLCP) 协议数据单元 (PPDU) 被传送。FD 帧可以包括以下信息项 :SSID、能力、接入网选项、安全性、AP 配置改变计数 (CCC)、AP 的下一个目标信标传输时间 (TBTT)、以及邻居 AP 的下一个 TBTT。

[0070] 一种用于改进被动扫描性能的方式用于 STA 获取 AP/ 网络信息而不用发送探测请求帧。示例包括使用测量导频 (MP) 帧或短信标帧。

[0071] MP 帧是由 AP 以相对于信标间隔较短的间隔伪周期传送的紧凑公共动作帧。MP 帧提供比信标帧更少的信息以考虑所需要的短间隔。MP 帧用于帮助 STA 经由被动扫描快速发现 BSS 的存在，以允许 STA 经由被动扫描快速收集邻居 AP 信号强度测量，以及使得 STA 能够传送探测请求。

[0072] MP 帧的配置参数包括针对 MP 和 MP 帧间隔的支持等级。图 3 示出了 MP 帧 300 的示例格式，其包括 MAC 报头 302、帧主体 304 以及 FCS 字段 306。MAC 报头 302 包括帧控制字段 310、持续时间字段 312、目的地地址字段 314、源地址字段 316、BSSID 字段 318、序列控制字段 320 以及 HT 控制字段 322。

[0073] 帧控制字段 310 包括协议版本子字段 330、类型子字段 332、子类型子字段 334、至分布系统 (DS) 子字段 336、来自 DS 子字段 338、多片段子字段 340、重试子字段 342、功率管理子字段 344、多数据子字段 346、受保护帧子字段 348、以及命令子字段 350。

[0074] 帧主体 304 包括动作帧部分 360、一个或多个卖方 (vendor) 特定 IE 362、以及可选管理消息完整码 (MIC) 元素 364。动作帧部分 360 包括类别字段 370、公共动作字段 372、能力信息字段 374、精简国家字符串字段 376、操作种类字段 378、信道字段 380、MP 间隔字段 382、以及一个或多个可选子元素 384。能力信息字段 374 包括频谱管理子字段 390、短时隙时间子字段 392、以及预留子字段 394。

[0075] AP 广播 MP 帧，且该传输是伪随机的。基础 MP 间隔小于信标间隔。在每个满足距离 TBTT 的最小间隔的目标测量导频传输时间 (TMPTT)，AP 将 MP 帧调度为用于传输的下一个帧，其在使用接入类别语音 (AC_VO) 增强分布信道接入 (EDCA) 参数的其他排队帧的前面。TMPTT 与 TBTT 之间的最小间隙是 MP 间隔的一半。在 TMPTT，如果介质不可用于 AP 传

送 MP 帧，则 AP 推迟 MP 传输一个 MP 间隔的最大时段，并在下一个 TMPTT 丢弃该延迟的 MP 帧传输。

[0076] 虽然 MP 帧可以用作 FD 帧，但是其不合适，因为在 FD 帧中需要携带比在当前 MP 帧设计中存在的更多的能力信息。该附加的能力信息可以包括例如：用于指向全 / 常规 TBTT 的时间指针字段；用于链路建立的所有必要信息，由此扫描 STA 不需要等待常规信标或探测请求 / 响应；关于邻居 BSS 的信息，使得能够发现运行参数的邻居 BSS；以及其他 BSS 的 FILS 信标传输时间的信息。

[0077] 短信标帧被设计成减少信标传输的介质占用，特别是在具有小信道带宽的系统中，例如 1MHz、2MHz 等，由此导致功耗减少 (AP 传输时间减少和 STA 接收时间减少)。该短信标帧用于允许长信标间隔 (例如 500ms)(是通常使用的 100ms 的信标间隔的 5 倍长)，但是仍然实现处于长休眠周期且可以在随机时间醒来的 STA 的同步，例如机器至机器应用中的计量器 / 传感器。

[0078] 对于全信标的相同开销，短信标帧格式允许信标被更频繁地传送，这改进了随机时间醒来且可以快速同步的不同步 STA 的同步时间。短信标帧仅携带用于信标主要功能的必要信息，包括：通告 AP 存在；STA 的同步；共享允许 STA 传送所需的最小信息；以及功率节省指示，例如业务量指示图 (TIM)。在关联过程期间可以从全信标或使用探测请求 / 响应机制取得其他非必要信息。

[0079] 图 4 示出了示例短信标帧 400 格式，包括帧控制字段 402、源地址 (SA) 字段 404、时间戳字段 406、改变序列字段 408、下一个全信标时间字段 410、压缩 SSID 字段 412、接入网选项字段 414、一个或多个可选 IE 416 以及 FCS 字段 418。

[0080] 帧控制字段 402 包括版本子字段 420、类型子字段 422、子类型子字段 424、下一个全信标时间存在子字段 426、SSID 存在子字段 428、互通存在子字段 430、BSS 带宽子字段 432、安全子字段 434 以及预留子字段 436。子字段 426-430 用于指示在短信标帧 400 中是否存在相应的字段 410-414(如图 4 中虚线箭头示出的)。

[0081] 短信标帧的需求包括 17 字节的最小帧大小，具有以下信息字段：BSS 带宽、SA、时间戳、以及改变序列值。短信标帧还可以包括可选信息字段，例如用于指示下一个全信标时间、压缩 SSID 以及接入网选项的帧控制 (FC) 字段的三比特指示符；以及具有可变大小的可选 IE。

[0082] 短信标帧格式可能不适合用于 FD 帧，因为设计短信标帧所处的使用情况与 FD 帧使用情况不同。短信标帧使用情况包括非关联的 STA(例如，具有长休眠周期的计量器和传感器) 和关联的 STA，且不必支持传统 STA。由于较小信道大小和较长信标间隔的较低传输速率 (低到 100kbps)，期望极高的无线媒介占用。此外，FD 帧使用情况主要包括非关联的 STA，需要与传统 STA 的兼容性，且以更常规的信道大小工作。此外，不同的使用情况支持不同的帧内容。对于短信标帧，重要的是包括“改变序列”信息且其需要关联的 STA 的 TIM，而 FD 帧使用情况不需要“改变序列”值或支持 TIM。

[0083] 由于最小化 FD 帧大小以及在基于具有 FILS 能力的 AP 的 WLAN 系统中允许传统非 AP STA 与具有 FILS 能力的非 AP STA 共存的目标，当前 MAC 帧格式在设计 FILS 发现 (FD) 帧时提出了挑战。

[0084] FD 帧设计目标之一是减少无线媒介占用，这需要 FD 帧具有小尺寸，优选地小于信

标帧。例如，基于 WLAN 系统业务量测量研究，典型的信标帧主体大小大约是 130 字节，因此 FD 帧主体期望是小于 50 字节。这提出了两个设计挑战：在 FD 帧中识别每个内容项的必需信息以及在 FD 帧中有效支持可变长度信息项和可选信息项。

[0085] 目前，信息元素 (IE) 是最常使用的用于编码可变长度信息项和可选信息项的格式。针对每个 IE 有两字节的开销：元素 ID 字段（一个字节）和长度字段（一个字节）。IE 还包括信息主体字段，其大小由长度字段指定。至于 FILS 发现强制和可选的内容项，需要 7 个 IE(14 字节的编码开销)，包括 SSID(可变长度信息项）和 6 个其他可选信息项。因此，在 FD 帧中需要可替换的编码方案来支持可变长度信息项和可选信息项。

[0086] 在 FD 帧中可包含以下信息以促进快速 AP/ 网络选择：下一个 TBTT 的时间、能力信息、BSS 负载信息、安全信息、接入网选项以及邻居 AP 信息。

[0087] TBTT 信息当前被提供作为基于 AP 与 STA 之间同步的公共时钟的时间值。例如，下一个 TBTT 可以从常规信标帧中的两个参数中导出：8 字节时间戳和 2 字节信标间隔字段。下一个 TBTT 所需的时间戳信息由三字节的下一个 TBTT 时间信息字段提供，其使用 AP 时间戳的三个最低有效字节。当使用基于公共同步时钟的时间值时，在 AP 和 STA 之间需要同步以供 STA 正确解译下一个 TBTT 时间信息。由于 FD 帧本意是在初始链路建立期间 STA 接收的第一个帧，基于时间戳的参数不适用于指示 FD 帧中的下一个 TBTT 信息。需要可替换的方法来解决这些不足。

[0088] 下一个 TBTT 的时间的指示指示来自当前 FD 帧的传送 AP 的下一个常规全信标帧的到达时间。该指示使用一个字节，以时间单元 (time unit, TU) 的个数为单位，即 1024μs。从当前 FD 帧传输时间引入偏移值。

[0089] 能力信息帮助 STA 进行快速 AP/ 网络发现，且包括但不限于 PHY 能力指示，例如短前导码或分组二进制卷积码 (PBCC)；安全能力信息；ESS 指示符；短时隙；频谱管理信息；以及 IPv4/IPv6 指示。

[0090] BSS 可不需要大多数已有 BSS 负载信息。因此，可使用 AP/BSS 负载的简单指示。例如 AP/BSS 的当前负载可以被压缩成短至 1 字节长的字段并包括信道利用、平均接入延迟和 / 或其他准确反映当前 AP 负载的测量。一个或两个参数足以用信号发送该 BSS 负载。在一个实施中，针对平均接入延迟或信道利用可使用一字节字段。在另一实施中，针对平均接入延迟和信道利用两者，可使用一字节字段，5 比特用于平均接入延迟，3 比特用于信道利用。

[0091] 安全信息可以包括鲁棒安全网络元素 (RSNE)(其可以由两个至四个八位位组来表示）以及隐私能力指示。

[0092] 通过包括附加 FILS 字段可以解决其他安全信息的顾虑。例如，AP 可以通告其支持优化的 FILS 认证过程，例如 FILS 可扩展认证协议 (EAP) 和 / 或 FILS 非 EAP 认证。AP 的 FILS 认证过程的支持可以使用 RSNE 能力字段中的比特来标志。在这种情况中，附加字段可以被添加到 RSNE 以携带特定 FILS 认证过程的附加属性（例如，FILS 标识、密码套件等。）

[0093] 接入网选项指示 AP/ 网络提供的接入服务（包括接入网类型）。图 5 示出了可以用于在 FD 帧中用信号发送信息的接入网选项 (ANO)IE 500 格式。接入网选项 IE 500 包括接入网类型字段 502、因特网字段 504、接入所需附加步骤 (ASRA) 字段 506、紧急服务可达 (ESR) 字段 508、以及未认证紧急服务可接入 (UESA) 字段 510。

[0094] 邻居 AP 当前使用其 BSSID(6 字节）或 SSID(典型地 6 至 8 字节，但是可以大至 32

字节）来标识。当有多个邻居 AP 时，邻居 AP 信息项需要在 FD 帧中被组织，由此在 FD 帧中包括邻居 AP 信息的有效性可以包含最小必需信息就能实现。

[0095] 邻居 AP 信息提供关于邻居 AP/ 信道的信息，并可以包括信道种类、信道数、下一个 TBTT 以及可能地 BSSID 或 SSID。图 6 示出了用于 FD 帧中的邻居 AP IE 600 的示例。邻居 AP IE 600 包括元素 ID 字段 602、长度字段 604、每个邻居 AP 的信息 606。每个邻居 AP 的信息 606 包括操作种类字段 610、操作信道字段 612 以及下一个 TBTT 的时间字段 614。

[0096] 在 FD 帧中可以包括以下信息以通告 AP 存在 :BSSID、压缩的 SSID 以及信道描述符。BSSID 唯一地标识每个 BSS 并且是 6 字节的基础设施 BSS 的 AP 的 MAC 地址。BSSID 中的信息可以被携带在 FD 帧的 MAC 报头中的 SA（源地址）字段或地址 3 字段中。

[0097] 压缩的 SSID 包括扩展的服务集 (ESS) 或独立的基本服务集 (IBSS) 的标识。知道全 SSID 的设备可以通过解码压缩的 SSID 而发现 BSS 的存在。可以对 SSID 执行标准的散列函数以创建压缩的 SSID。在一个实施中，压缩的 SSID 字段的长度是 4 字节。

[0098] 信道描述符包括操作信道的信道频率和间隔，由国家、操作种类以及操作信道来规定。国家字符串标识 STA 操作所在的国家，精简的国家字符串（例如，国家字符串中的前两个字节）可以用于 FD 帧。操作种类标识操作信道的操作种类。操作信道标识操作种类中的操作信道。

[0099] 用于短信标帧的缩短的时间戳（在 AP 的时间戳的四个最低有效比特）可以重新用于 FD 帧。

[0100] 图 7-12 中描述了优化鲁棒安全网络元素 (RSNE) 的不同版本。这些实施方式中的任何一个均可与以下公开的实施方式相结合，并且尤其与图 15-26 中任意图中公开的 FD 帧结构结合。图 7 示出了 RSNE 700 格式，包括元素 ID 字段 702 ;长度字段 704 ;版本字段 706 ;群组数据密码套件字段 708 ;成对密码套件计数字段 710 ;成对密码套件列表字段 712，其中 m 表示成对密码套件计数 ;认证和密钥管理 (AKM) 套件计数字段 714 ;AKM 套件列表字段 716，其中 n 表示 AKM 套件计数 ;RSN 能力字段 718 ;成对主密钥 (PMK) 标示符 (PMKID) 计数字段 720 ;PMKID 列表字段 722，其中 s 表示 PMKID 计数 ;以及群组管理密码套件字段 724。RSNE 的长度可以多达 255 个八位位组，且对于 RSNE 被包含在 FD 帧中需要 RSNE 优化。也就是说，参考关于图 7-12 的详细描述，安全字段指示由 AP 使用的一种或多种类型的安全性。

[0101] 图 8 示出了用于 FD 帧中的使用固定长度的四个八位位组编码的优化的 RSNE 800。RSNE 800 包括群组数据密码套件字段 802，其可以是 4 比特长 ;成对密码套件列表字段 804，其可以是 8 比特长，允许多达两个成对套件 ;AKM 套件列表字段 806，其可以是 8 比特长，允许多达两个 AKM 套件 ;优化的 RSN 能力字段 808，其可以是 8 比特长 ;以及群组管理密码套件字段 810，其可以是 4 比特长。RSN 能力字段 808 可以包括一比特预认证子字段和一比特管理帧保护所需子字段。RSN 能力字段 808 中其余 6 个比特可以携带其他信息，包括 AP 支持 FILS 认证过程的标志 ;例如，一比特 FILS EAP 认证字段和一比特 FILS 非 EAP 认证字段。

[0102] 图 9 示出了用于 FD 帧中的使用多达 4 个八位位组的可变长度编码的优化 RSNE 900。RSNE 900 包括群组数据密码套件字段 902，其可以是 4 比特长 ;成对密码套件计数字段 904，其可以是 2 比特长 ;成对密码套件列表字段 906，其依据成对密码套件计数字段 904 的值可以为 0，4 或 8 比特长 ;AKM 套件计数字段 908，其可以是 2 比特长 ;AKM 套件列表字段

910，其依据 AKM 套件计数字段 908 的值可以是 0、4 或 8 比特长；优化的 RSN 能力字段 912，其可以是 4 比特长；以及群组管理套件字段，其可以是 4 比特长。RSN 能力字段 912 可包括一比特预认证子字段、一比特管理帧保护所需子字段、一比特 FILS EAP 认证子字段以及一比特 FILS 非 EAP 认证子字段。

[0103] 图 10 示出了用于 FD 帧中的使用四个八位位组的固定长度位图编码的优化 RSNE 1000。RSNE 1000 包括群组数据密码套件字段 1002，其可以是 4 比特长；成对密码套件列表字段 1004，其可以是 8 比特长，允许多达 8 种成对套件选择；AKM 套件列表字段 1006，其可以是 8 比特长，允许多达 8 种 AKM 套件选择；优化的 RSN 能力字段 1008，其可以是 8 比特长；以及群组管理套件字段，其可以是 4 比特长。RSN 能力字段 1008 可以包括一比特预认证子字段和一比特管理帧保护所需子字段。RSN 能力字段 1008 中剩余的 6 比特可以携带其他信息，反映 AP 支持 FILS 认证过程。

[0104] 图 11 示出了用于 FD 帧中的使用固定长度的两个八位位组编码的优化 RSNE 1100。RSNE 1100 包括组合的群组和成对密码套件字段 1102，其可为 4 比特长；AKM 套件列表字段 1104，其可为 4 比特长；优化 RSN 能力字段 1106，其可为 4 比特长；以及群组管理套件字段 1108，其可以是 4 比长。成对密码套件字段 1102 表示被选择用于保护群组数据和成对数据的密码套件。RSN 能力字段 1106 可以包括一比特预认证子字段、一比特管理帧保护所需子字段、一比特 FILS EAP 认证子字段以及一比特 FILS 非 EAP 认证子字段。

[0105] 图 12 示出了用于 FD 帧中的使用固定长度的两个八位位组编码的可替换的优化 RSNE 1200。RSNE 1200 包括群组密码套件字段 1202，其可以是 4 比特长；成对密码套件列表字段 1204，其可以是 4 比特长；AKM 套件列表字段 1206，其可以是 4 比特长；以及群组管理密码套件字段 1208，其可以是 4 比特长。在 RSNE 1200 中，RSN 能力字段没有被包含在 FD 帧中。

[0106] 在 RSNE 700-1200 中，密码套件可以由四比特来表示，如表 1 中所示。

[0107] 表 1

[0108]

密码套件的 4 比特表示	OUI（组织上唯一的标识符）	套件类型	含义
0000	00-0F-AC	0	使用群组密码套件
0001	00-0F-AC	1	WEP-40
0010	00-0F-AC	2	TKIP
0011	00-0F-AC	3	预留
0100	00-0F-AC	4	CCMP - RSNA 中数据帧的默认的成对密码套件和默认的群组密码套件
0101	00-0F-AC	5	WEP-104
0110	00-0F-AC	6	BIP -启用管理帧保护的 RSNA 中默认的群组管理密码套件
0111	00-0F-AC	7	不允许群组地址业务量
	00-0F-AC	8–255	预留
	卖方 OUI	其他	卖方特定
	其他	任意	预留

[0109] 在 RSNE 700-1200 中，AKM 套件可以由四比特来表示，如表 2 所示。

[0110] 表 2

[0111]

AKM套件列表比特	OUI	套件类型	含义		
			认证类型	密钥管理类型	密钥导出类型
0000	00-0F-AC	0	预留	预留	预留
0001	00-0F-AC	1	通过IEEE 802.1X协商的认证或使用11.5.9.3中定义的PMKSA缓存 – RSNA默认	11.6中定义的RSNA密钥管理或使用11.5.9.3中定义的PMKSA缓存 – RSNA默认	11.6.1.2中定义的
0010	00-0F-AC	2	PSK	11.6中定义的RSNA密钥管理，使用PSK	11.6.1.2中定义的
0011	00-0F-AC	3	通过IEEE 802.1X协商的FT认证	11.6.1.7中定义的FT密钥管理	11.6.1.7.2中定义的
0100	00-0F-AC	4	使用PSK的FT认证	11.6.1.7中定义的FT密钥管理	11.6.1.7.2中定义的
0101	00-0F-AC	5	通过IEEE 802.1X协商的认证或使用具有SHA256密钥导出的11.5.9.3中定义的PMKSA缓存	8.5 中定义的 RSAN 密钥管理或使用 11.5.9.3 中定义的 PMKSA 缓存，具有 SHA256 密钥导出	11.6.1.7.2中定义的
0110	00-0F-AC	6	具有SHA256密钥导出的PSK	11.6中定义的RSNA密钥管理，使用具有SHA256密钥导出的PSK	11.6.1.7.2中定义的
0111	00-0F-AC	7	TDLS	TPK握手	11.6.1.7.2中定义的
1000	00-0F-AC	8	具有SHA-256的SAE认证或使用具有SHA256密钥导出的11.5.9.3中定义的PMKSA缓存	11.6中定义的RSNA密钥管理，具有SHA256密钥导出的11.5.9.3中定义的PMKSA缓存或13.5中定义的认证的网格对等交换	11.6.1.7.2中定义的
1001	00-0F-AC	9	通过SAE的FT认证，具有SHA256	11.6.1.7中定义的FT密钥管理	11.6.1.7.2中定义的
	00-0F-AC	10–255	预留	预留	预留
	卖方OUI	任意	卖方特定	卖方特定	卖方特定
	其他	任意	预留	预留	预留

[0113] 可以在 FD 帧中包含以下信息以使得 STA 能够进行传送，包括 PHY 特定信息和功率

约束。PHY 特定信息包括 802.11g、802.11n 和 802.11ac PHY 特定信息。802.11g PHY 特定信息包括来自扩展的速率 PHY(ERP)IE 的三个比特 (NonERP_Present(非 ERP_ 存在)、Use_Protection(用户 _ 保护)和 Barker_Preamble_Mode(Barker_ 前导码 _ 模式))。5 个预留比特可以用于用信号发送能力字段中的其他信息。

[0114] 802.11n PHY 特定信息可以包括缩短的 HT 能力元素,其可以被压缩成 1 字节信息主体,如表 3 所示。

[0115] 表 3

[0116]

HT 能力项	大小(比特)

[0117]

支持的信道带宽集	1
HT-Greenfield(HT- 绿色字段)	1
发射 STBC	1
接收 STBC	2
预留	2
40MHz 不容忍	1

[0118] 802.11n PHY 特定信息还可以包括缩短的 HT 操作元素,其可以被压缩成 1 字节信息主体,仅使用主信道字段。可选地,可以包括 1 字节 STA 信道宽子字段,以及表 3 中一个预留比特可以被再利用以节省开销。

[0119] 图 13 示出了用于 FD 帧中的 HT PHY 特定 IE 1300 的示例。HT PHY 特定 IE 1300 包括支持的信道宽集字段 1302,用于指示 STA 支持的信道宽 ;HT-Greenfield(HT- 绿色字段)字段 1304,用于指示对接收 HT-Greenfield 格式的 PPDU 的支持 ;发射空时块编码 (STBC) 字段 1306,用于指示对使用 STBC 的 PPDU 传输的支持 ;接收 STBC 字段 1308,用于指示对使用 STBC 接收 PPDU 的支持 ;预留部分 1310 ;40MHz 不容忍字段 1312,用于指示是否禁止 40MHz 传输 ;以及主信道字段 1314,用于指示主操作信道。

[0120] 802.11ac PHY 特定信息可以包括缩短的 VHT 能力元素,其可以被压缩成 1 字节信息主体,如表 4 所示。

[0121] 表 4

[0122]

VHT/HT 能力和操作项	大小(比特)
支持的信道宽集(来自 VHT 能力元素)	2
发射 STBC(来自 VHT 能力元素)	1

接收 STBC（来自 VHT 能力元素）	3
STA 信道宽（来自 HV 操作元素）	1
预留	1

[0123] 802.11ac PHY 特定信息还可以包括缩短的 VHT 操作元素，以及 HT 操作元素，其可以被压缩成 4 字节信息主体。

[0124] BSS 操作信道宽可以由 HT 操作元素 HT 操作信息字段中的 STA 信道宽子字段和 VHT 操作元素 VHT 操作信息字段中的信道宽子字段的组合来表示。STA 信道宽子字段可以在 1 字节信息主体中与其他项打包，如上表 4 所示。

[0125] 可以通过使用 HT 操作元素主信道字段中的信息与 VHT 操作元素 VHT 操作信息字段信道中心频率段 0 和信道中心频率段 1 子字段的组合来指示信道化。

[0126] 图 14 示出了用于 FD 帧中的使用的 VHT PHY 特定 IE 1400 的示例。VHT PHY 特定 IE 1400 包括第一部分 1402，其元素从 VHT 能力元素中压缩，第二部分 1404，其元素从 HT 操作元素中压缩，以及第三部分 1406，其元素从 VHT 操作元素中压缩。第一部分 1402 包括支持的信道宽集字段 1410、发射 STBC 字段 1412 以及接收 STBC 字段 1414。第二部分 1404 包括 STA 信道宽字段 1416、预留部分 1418 以及主信道字段 1420。第三部分 1406 包括信道宽字段 1422、信道中心频率段 0 字段 1424 以及信道中心频率段 1 字段 1426。

[0127] 功率约束信息包括允许 STA 确定当前信道中局部最大发射功率所需的信息。信标或探测响应帧中的 1 字节功率约束 IE 可以被再使用以用信号发送 FD 帧中的该信息。

[0128] 如上所提及的，AP 可以在全信标实例之间传送 FD 帧以支持用于快速初始链路建立的快速 AP/ 网络发现。与此对应的，实施方式涉及一种用于在无线站中的方法，该方法包括从 AP 接收全信标帧的实例之间的 FD 帧，并基于接收到的 FD 帧确定是否与 AP 相关联。FD 帧和在其中使用 FD 帧的方法的进一步细节将在下文中参考附图（尤其参考图 15-26）而被公开，图 15-26 公开了涉及上文公开的实施方式的特征以及本发明概念内可实行的特定实施方式的特征的不同结合。根据与上文实施方式及下文公开的其它特定实施方式可结合的特定实施方式，控制字段，称为 FD 帧控制字段，被引入到 FD 帧中以支持 FD 帧主体中的内容项的有效编码。图 15 示出了 FD 帧 1500 的示例，包括 FD 帧报头 1502、FD 帧主体 1504、以及 FCS 字段 1506。依据使用的帧格式，FD 帧报头 1502 可以包括 MAC 管理帧报头和其他帧字段。FD 帧主体 1504 包括 FD 帧控制字段 1510 和 FD 帧内容 1512。

[0129] FD 帧控制字段 1510 可以位于 FD 帧主体 1504 中任意确定性的位置，只要接收到 FD 帧 1500 的 STA 能够清楚定位该控制字段。在一个实施中，FD 帧控制字段 1510 可以设置为 FD 帧主体 1504 中的第一个信息字段。

[0130] FD 帧控制字段 1510 包括一个或多个控制子字段，其用于支持接收 STA 确定性地解码和解译 FD 帧主体 1504 中的内容项。典型的示例包括指示 FD 帧主体 1504 中存在可选信息项，以及在 FD 帧主体 1504 中提供可变大小的信息。在一个实施中，FD 帧控制字段 1510 可以包括 1 比特指示符，用于指示在特定 FD 帧实例中是否存在可选内容项。与两字节编码开销的 IE 格式相比，使用该 1 比特指示符是更有效率的编码方案。FD 帧控制字段 1510 将 FD 帧主体 1504 中内容项的所有所需控制信息收集到单个控制字段，而 IE 格式将该控制信

息分发给每个内容项。

[0131] 在 FD 帧中需要 SSID 信息以允许 AP 在信道上通告其存在并使得 STA 能够发起关联。注意到 SSID 信息是 FD 帧中需要的唯一信息，且 FD 帧中包含的任意附加信息项是可选的。当前，需要全 SSID（其是 0 到 32 字节长）发起关联。在初始链路建立期间，在信标和探测响应帧中将以 SSID IE 编码的 SSID 信息提供给 STA。

[0132] 虽然 SSID 的最大大小是 32 字节，实际上，SSID 通常具有较小的大小，例如典型地 6 至 8 个字节。根据与于此公开的其它实施方式可结合的特定实施方式，在 FD 帧中可以支持可变长度的 SSID 信息项。该特定实施方式能够减少在 FD 帧中使用的比特的数量并因而使得有效带宽资源能够更有效的使用。在 FD 帧控制字段中可以包含单独的控制子字段以用信号通知 FD 帧中的 SSID 的实际大小，而不是使用 SSID IE 格式。为了最小化 FD 帧大小，FD 帧中的 SSID 信息项可以以精简的格式发送，例如压缩的，裁剪的等。

[0133] 图 16A-16B 示出了 FD 帧的 SSID 信息项设计的两个示例。图 16A 示出了 FD 帧 1600，包括 FD 帧报头 1602、FD 帧主体 1604、以及 FCS 字段 1606。依据使用的帧格式，FD 帧报头 1602 可以包括 MAC 管理帧报头和其他帧字段。FD 帧主体 1604 包括 FD 帧控制字段 1610、SSID 字段 1612 以及 FD 帧的其他信息项 1614。注意其他信息项 1614 是可选的，且在一些实施方式中，在 FD 帧主体 1604 中可以仅包含 SSID 字段 1612。

[0134] FD 帧控制字段 1610 包括 SSID 长度字段 1620 和其他控制子字段 1622。SSID 长度字段 1620 用于指示 SSID 字段 1612 的实际大小（以字节为单位）。在该实施方式中，SSID 保持典型的大小范围，即，0 到 32 字节。

[0135] 图 16B 示出了 FD 帧 1650，包括 FD 帧报头 1652、FD 帧主体 1654 以及 FCS 字段 1656。依据使用的帧格式，FD 帧报头 1652 可以包括 MAC 管理帧报头和其他帧字段。FD 帧主体 1654 包括 FD 帧控制字段 1660、SSID 字段 1662 以及 FD 帧的其他信息项 1664。注意其他信息项 1664 是可选的，且在一些实施方式中，在 FD 帧主体 1654 中可以仅包含 SSID 字段 1662。

[0136] FD 帧控制字段 1660 包括 SSID 指示符子字段 1670、SSID 长度子字段 1672 以及其他控制子字段 1674。SSID 指示符子字段 1670 用于指示 SSID 字段 1662 包含全 SSID 还是精简的 SSID。在一个实施方式中，SSID 指示符子字段 1670 可以实施为 1 比特指示符，但是可以使用其它类型的指示符。SSID 长度子字段 1672 用于指示 SSID 字段 1662 的长度（以字节为单位）。在该实施中，SSID 存在于裁剪的范围，例如从 0 到 8 字节。

[0137] 由于需要全 SSID 供 STA 发起关联，所以任意精简的 SSID（其可以包括例如压缩的 SSID 或裁剪的 SSID）需要被确定性地映射到其全 SSID。在发射机侧可以有精简或压缩 SSID 的多种选项，且在接收机侧可以有映射或解压缩 SSID 的多种选项。所选择的特定选项不会影响 FD 帧 1650 的内容。

[0138] 根据与于此公开的其它实施方式可结合的特定实施方式，并且尤其是与关于图 16 中所公开的特定实施方式可结合的特定实施方式，FD 帧中的能力信息项包括以下特征。其包括 STA 用来在初始链路建立的 AP/ 网络发现过程中解除选择 AP/ 网络所需要的必要 AP/ 网络能力信息的最小集。已有的两个字节的能力字段可以被修改以作为开始点用于该情况中，并为 FD 帧使用移除不必要的子字段。FD 帧相关信息项被添加，例如支持的最小速率、PHY 类型、PHY 模式、IPv4/IPv6 支持等。FD 帧控制字段中的 1 比特指示符可以用于指示在

FD 帧中存在能力信息项。

[0139] 图 17 示出了 FD 帧 1700 的示例，包括三字节长的 FD 能力信息项。FD 帧 1700 包括 FD 帧报头 1702、FD 帧主体 1704 以及 FCS 字段 1706。FD 帧主体 1704 包括 FD 帧控制字段 1710、SSID 字段 1712、FD 能力字段 1714 以及其他信息项 1716。注意其他信息项 1716 是可选的，且在一些实施方式中，可以从 FD 帧主体 1704 中略掉其他信息项 1716。

[0140] 根据特定实施方式，FD 帧控制字段 1710 包括 SSID 长度子字段 1720；能力存在指示符字段 1722，用于指示在 FD 帧 1700 中是否存在 FD 能力字段 1714；以及其他控制子字段 1724。

[0141] 根据特定实施方式，FD 能力字段包括 ESS 子字段 1730、IBSS 子字段 1732、无争用 (CF) 可轮询子字段 1734、CF 轮询请求子字段 1736、隐私子字段 1738、短前导码子字段 1740、网际协议 (IP)v4 支持子字段 1742、IPv6 支持子字段 1744、频谱管理子字段 1746、QoS 子字段 1748、短时隙子字段 1750、第一预留子字段 1752、无线电管理子字段 1754、第二预留子字段 1756、延迟块 ACK 子字段 1758、即时 ACK 子字段 1760、PHY 类型子字段 1762 以及支持的最小速率子字段 1764。也就是说，能力字段包括 AP 的能力信息。

[0142] 基于上述特征，FD 能力字段 1714 的可替换设计可以被生成。例如，可以去除支持的最小速率子字段 1764，这假定该信息可以从 PHY 类型子字段 1762 中推导出作为最小强制性的速率。此外，支持的最小速率子字段 1764 可以被编码为预定义单位的数值，例如 0.5Mbps、1Mbps 等的步长。

[0143] CF 可轮询子字段 1734 和 CF 轮询请求子字段 1736 可以不需要在 FD 能力字段 1714 中，因为 QoS 子字段 1748 可以提供足够信息用于 AP/ 网络初始解除选择目的。

[0144] ACK 相关能力，例如延迟块 ACK 子字段 1758 和即时 ACK 子字段 1760，可以在链路建立过程中较后的消息中（而不是第一个 AP 到 STA 消息中）用信号发送，诸如 FD 帧 1700。这允许延迟块 ACK 和即时 ACK 的两个 FD 能力比特被“预留”或用于其他能力指示。

[0145] 此外，当前在 FD 能力字段 1714 中预留的比特（例如，第一预留子字段 1752 和第二预留子字段 1756）可以在将来用于指示新系统能力，例如新层 3 协议能力。

[0146] 根据与于此公开的其它实施方式可结合的特定实施方式并参考关于图 7-12 的详细描述，FD 安全信息项可以具有固定长度或可变长度。固定长度 FD 安全信息项可以是 4 字节长，但是可以使用固定长度。必需安全信息的最小集被包含以允许 STA 在初始链路建立中 AP/ 网络发现过程中解除选择 AP/ 网络。已有 RSNE 可以被修改以使其大小更小。例如，RSN 能力子字段可以被重新设计成反映其实际用途以及 FD 帧特定考虑。成对套件和 AKM 套件的数量可以限制到例如每种两个。用于标识密码套件和 AKM 套件的 4 比特的码可以被使用。可以移除 PMKID 计数和 PMKID 列表字段。

[0147] FD 安全信息项还可以包括 FILS 认证方法支持（例如基于 FILS 快速 EAP 的认证、基于 FILS EAP 重新认证协议 (RP) 的认证、FILS 非 EAP 快速认证以及没有第三方的 FILS 快速认证）的安全能力指示符。FD 帧控制字段中的 1 比特指示符可以用于指示 FD 帧中存在安全信息项，但是可以使用其它类型的指示符。

[0148] 图 18 示出了 FD 帧 1800 的示例，包括 4 字节 FD 安全信息项。FD 帧 1800 包括 FD 帧报头 1802、FD 帧主体 1804 以及 FCS 字段 1806。FD 帧主体 1804 包括 FD 帧控制字段 1810、SSID 字段 1812、FD 能力字段 1814、用于指示由 AP 提供的接入服务的接入网选项 (ANO) 字

段 1816、FD 安全字段 1818 以及其他信息项 1820。注意其他信息项 1820 是可选的，且在一些实施方式中，其他信息项 1820 可以从 FD 帧主体 1804 中略去。如上所指出的，ANO 字段优选地包括以下任何一者或多者：接入网类型字段、接入所需附加步骤字段、紧急服务可达字段、或未认证紧急服务可接入字段。

[0149] 根据与于此公开的其它实施方式可结合的特定实施方式，FD 帧控制字段 1810 包括 SSID 长度子字段 1830、能力存在指示符字段 1832、用于指示 FD 帧内容中是否存在相应的 ANO 字段的 ANO 存在指示符子字段 1834、用于指示 FD 帧内容中是否存在相应的安全字段的安全存在指示符子字段 1836 以及其他控制子字段 1838。

[0150] FD 安全字段 1818 包括群组数据密码套件选择符子字段 1840、群组管理密码套件选择符子字段 1842、成对密码套件选择符 1 子字段 1844、成对密码套件选择符 2 子字段 1846、AKM 套件选择符 1 子字段 1848、AKM 套件选择符 2 子字段 1850 以及 FD RSN 能力子字段 1852。FD RSN 能力子字段 1852 包括预认证指示符子字段 1860、管理帧保护所需指示符子字段 1862、FILS 快速 EAP 指示符子字段 1864、FILS EAP-RP 指示符子字段 1866、FILS 非 EAP 指示符子字段 1868、没有第三方的 FILS 认证指示符子字段 1870、管理帧保护能力指示符子字段 1872 以及理想转发秘密指示符子字段 1874。在一种实施方式中，指示符子字段中的每一者可以是一比特指示符，但是可以使用其它类型的指示符。

[0151] 基于上述特征，FD 安全字段 1818 的可替换设计可以被生成。例如，如果假定一个 AKM 套件选择符提供足够信息用于 AP/ 网络初始解除选择目的，那么 FD 安全字段 1818 可以包含一个 AKM 套件选择符，而不是两个。

[0152] 可变长度 FD 安全信息项包括与固定长度变量类似的信息，但是有以下改变以反映其可变长度。可变长度安全字段 (RSNE) 可以被使用，且其长度可以例如是 0 至 6 个八位位组。RSNE 字段内的可选 RSN 能力 (RSNC) 子字段也具有可变长度且可以例如是 0 到 3 个八位位组。成对套件和 AKM 套件的数量可以限制到例如每项多达两个。

[0153] 图 19 示出了 FD 帧 1900 的示例，包括可变长度 FD 安全信息项。FD 帧 1900 包括 FD 帧报头 1902、FD 帧主体 1904 以及 FCS 字段 1906。FD 帧主体 1904 包括 FD 帧控制字段 1910、SSID 字段 1912、FD 能力字段 1914、ANO 字段 1916、FD 安全字段 1918 以及其他信息项 1920。注意其他信息项 1920 是可选的，且在一些实施方式中，其他信息项 1920 可以从 FD 帧主体 1904 中略去。

[0154] FD 帧控制字段 1910 包括 SSID 长度子字段 1930、能力存在指示符子字段 1932、ANO 存在指示符子字段 1934、安全存在指示符子字段 1936 以及其他控制子字段 1938。

[0155] FD 安全字段 1918 包括 RSNE 长度子字段 1940、RSNC 长度子字段 1942、群组数据密码套件选择符子字段 1944、成对密码套件选择符 1 子字段 1946、以及 AKM 套件选择符 1 子字段 1948。

[0156] FD 安全字段 1918 可选地包括可变长度 FD RSN 能力子字段 1950、成对密码套件选择符 2 子字段 1952、AKM 套件选择符 2 子字段 1954、以及群组管理密码套件选择符子字段 1956。FD RSN 能力子字段 1950 包括预认证子字段 1960、管理帧保护所需子字段 1962、管理帧保护能力子字段 1964、FILS 快速 EAP 子字段 1966、FILS EAP-RP 子字段 1968、FILS 非 EAP 子字段 1970、没有第三方的 FILS 认证子字段 1972、理想转发秘密子字段 1974 以及预留子字段 1976。

[0157] 在图19中，子字段1950-1956以及1976用虚线轮廓显示，以指示它们在FD帧1900中是可选项。从FD帧1900中包含FD RSN能力子字段1950的程度上来说，子字段1960-1974是强制性的，而预留子字段1976仍然是可选的。

[0158] 通常基于AP与STA之间同步的公共时钟来提供TBTT信息作为时间戳值。但是不期望时间戳信息出现在FD帧中。此外，FD帧旨在成为在初始链路建立中STA接收到的第一个帧。因此，基于时间戳的参数不是用于指示FD帧中下一个TBTT信息的合适方法。

[0159] 为了用信号发送下一个TBTT信息而不需要AP与STA之间的同步，FD帧传输时间与下一个信标帧传输时间之间的时间偏移的1字节偏移值可以被使用，作为FD帧中FD AP的下一个TBTT信息项。该偏移值是以时间单元(TU)为单位的时间，例如1024μs。可以在FD帧控制字段中使用1比特指示符来指示在FD帧中存在AP的下一个TBTT信息字段。

[0160] 图20示出了示例FD帧2000，包括AP的下一个TBTT信息项。根据与于此公开的其它实施方式可结合的该特定实施方式，FD帧2000包括FD帧报头2002、FD帧主体2004、以及FCS字段2006。FD帧主体2004包括FD帧控制字段2010、SSID字段2012、FD能力字段2014、ANO字段2016、FD安全字段2018、用于指示AP配置参数集已发生改变的次数的配置改变计数(CCC)字段2020、用于指示来自AP的下一个全信标帧的传输时间的FD AP下一个TBTT(ANT)字段2022、以及其他信息项2024。注意其他信息项2024是可选的，且在一些实施方式中，其他信息项2024可以从FD帧主体2004中略去。

[0161] 根据特定实施方式，FD帧控制字段2010包括SSID长度子字段2030、能力存在指示符子字段2032、ANO存在指示符子字段2034、安全存在指示符子字段2036、用于指示FD帧内容中是否存在相应的AP配置改变计数字段的CCC存在指示符子字段2038、用于指示FD帧内容中是否存在相应的AP下一个目标信标传输时间字段的ANT存在指示符子字段2040以及其他控制子字段2042。

[0162] 尝试建立WLAN链路的STA扫描信道并接收包含发射AP的下一个TBTT信息的FD帧。如果STA仍然需要来自AP的进一步信息，其可以使用接收到的下一个TBTT信息来做出关于下一步做什么的智能决定。例如，如果下一个TBTT信息告诉STA在下一个TBTT之前有相对长的间隔(例如超过50ms)，则STA可以进入功率节省状态或切换到扫描另一信道，然后在下一个TBTT之前返回到这个信道。如果下一个TBTT信息指示在短时间间隔(例如少于20ms)中将有信标帧传输，则STA可以决定继续监视该信道以接收下一个信标帧或进入功率节省状态并在下一个信标帧及时返回到该信道。此外，FD帧中提供的下一个TBTT信息可以有效减少探测请求传输的次数。

[0163] FD邻居AP信息项用于促进在初始链路建立期间快速扫描多个AP/信道。对于FD邻居AP信息项有两个基本的设计问题：如何标识邻居AP以及在FD帧中需要关于邻居AP的什么信息。与FD帧中的其他信息项类似，期望将FD邻居AP信息项保持小尺寸。

[0164] 每个邻居AP的邻居AP的下一个TBTT是FD帧中需要的最小信息。由于当接收到FD帧时STA与AP之间是未同步状态，来自发射AP的时间戳或邻居AP的时间戳的值不能用于指示邻居AP的下一个TBTT。因此，FD帧传输时间与邻居AP的TBTT之间的偏移时间值可以被使用。发射AP可以通过与邻居AP或第三方的通信来收集邻居AP的信息，第三方例如可以是非AP STA或其他网络元件。当发射AP具有关于邻居AP的TBTT的合适信息且其决定在FD帧传输中包含该信息时，其基于其系统时钟时间值、估计的FD帧传输时间以及预

先收集的邻居 AP 的 TBTT 信息来计算 FD 帧传输时间与邻居 AP 的下一个 TBTT 之间的偏移值。也就是说，根据与上文公开的实施方式可结合的特定实施方式，尤其关于图 15-19，AP 下一个目标信标传输时间被表达为相对于 FD 帧传输时间的偏移值。

[0165] 两个参数（操作种类和信道数量）可以用于标识邻居 AP。操作种类可以是 1 字节枚举值，用于指定邻居 AP 的操作种类。信道数量可以是 1 比特枚举值，用于指定该操作种类的邻居 AP 内的操作信道。

[0166] 为了提供足够量的邻居信息同时尝试保持 FD 帧尺寸小，包含在邻居 AP 信息项中的邻居数量可以被限制到例如多达两个邻居 AP。为了指示存在 FD 邻居 AP 信息项和包含的邻居 AP 的数量，FD 帧控制字段中的控制子字段可以被使用，其大小取决于 FD 邻居 AP 信息项中最大允许邻居 AP 数量。例如，如果最大允许邻居 AP 数量是 k，那么需要 n 个比特的控制子字段，其中 n 是满足 $2^n \geq (k+1)$ 的最小整数。

[0167] 图 21 示出了 FD 帧 2100 的示例，包括 FD 邻居 AP 信息项。根据与于此公开的其它实施方式可结合的特定实施方式，FD 帧 2100 包括 FD 帧报头 2102、FD 帧主体 2104、以及 FCS 字段 2106。FD 帧主体 2104 包括 FD 帧控制字段 2110、SSID 字段 2112、FD 能力字段 2114、ANO 字段 2116、FD 安全字段 2118、CCC 字段 2120、FD ANT 字段 2122、邻居 AP 信息字段 2124、以及其他信息项 2126。注意其他信息项 2126 是可选的，且在一些实施方式中，其他信息项 2126 可以从 FD 帧主体 2104 中略去。

[0168] 根据特定实施方式，FD 帧控制字段 2110 包括 SSID 长度子字段 2130、能力存在指示符子字段 2132、ANO 存在指示符子字段 2134、安全存在指示符子字段 2136、CCC 存在指示符子字段 2138、ANT 存在指示符子字段 2140、用于指示 FD 帧内容中是否存在相应的邻居 AP 信息字段的邻居 AP 信息存在指示符子字段 2142 以及其他控制子字段 2144。邻居 AP 信息存在指示符子字段 2142 用于指示是否存在邻居 AP 信息以及包含在邻居 AP 信息字段 2124 中的邻居 AP 数量。

[0169] 在一个实施中，邻居 AP 信息字段 2124 包括多达两个邻居 AP 2150a 和 2150b 的邻居 AP 信息。邻居 AP 信息 2150 包括操作种类子字段 2152、信道数量子字段 2154 和针对邻居 AP 信息字段中的每个邻居 AP 的下一个 TBTT 偏移子字段 2156。邻居 AP 的操作种类和信道数量可以与发射 AP 的操作信道相同，在这种情况中邻居 AP 在同一个信道上操作。类似地，当包含多个邻居 AP 时，其中的一些可以具有相同的操作种类和信道数量的参数值，但是具有不同的下一个 TBTT 偏移值。

[0170] 根据与关于图 20 公开的实施方式可有利结合的特定实施方式，每个下一个目标信标传输时间字段指示来自相应的邻居 AP 的下一个全信标帧的传输时间。根据与上文实施方式可有利结合的另一个特定实施方式，下一个目标信标传输时间可以被表示为相对于 FD 帧传输时间的偏移值。进一步地，参考图 20，根据特定实施方式，该偏移值被表示为时间单元的数量。

[0171] 包含的邻居 AP 可以基于彼此相对和相对于当前 AP 的下一个 TBTT 偏移的邻居 AP 的下一个 TBTT 偏移从所有邻居 AP 中选择。例如，多达两个邻居 AP 的 TBTT 信息，加上发射 AP 的下一个 TBTT 信息，在 FD 帧中可以包含多达三个 AP 的 TBTT 信息。假定 T 表示典型的信道扫描时间加用于在扫描过程中切换信道的时间。可以从邻居 AP 中选择两个邻居 AP，AP-a 和 AP-b，由此 AP-a 的下一个 TBTT(TBTT-a) 和 AP-b 的下一个 TBTT(TBTT-b) 彼此分开

并与发射 AP 的下一个 TBTT 相隔预定义的间隔，例如 T。FD 帧传输时间与选择的邻居 AP 的下一个 TBTT 之间的偏移总和小于或等于任意其他选择的邻居 AP。

[0172] 其他可替换邻居 AP 选择方案也可以被使用。例如，传送 FD 帧的 AP 可以基于邻居 AP 的业务量负载、信号强度、安全特征、能力等选择将包含在其 FD 邻居 AP 信息项中的邻居 AP。

[0173] 除了上述的信息项，其他信息项也可以包含在 FD 帧中，作为强制性或可选的字段，以向 STA 提供进一步信息并允许 STA 改善初始链路建立。类似地，相应的控制子字段可以被包含在 FD 帧控制字段中以支持信息项的解码和解译，即它们是否是可选信息项，以及它们是否是可变化大小。

[0174] 图 22 示出了 FD 帧 2200 的示例。FD 帧 2200 包括 FD 帧报头 2202、FD 帧主体 2204、以及 FCS 字段 2206。FD 帧主体 2204 包括 FD 帧控制字段 2210、SSID 字段 2212、FD 能力字段 2214 以及 ANO 字段 2216、FD 安全字段 2218、CCC 字段 2220、FD ANT 字段 2222 以及邻居 AP 信息字段 2224。

[0175] FD 帧控制字段 2210 包括 SSID 长度子字段 2230、能力存在指示符子字段 2232、ANO 存在指示符子字段 2234、安全存在指示符子字段 2236、CCC 存在指示符子字段 2238、ANT 存在指示符子字段 2240、邻居 AP 信息存在指示符子字段 2242 以及预留子字段 2244。

[0176] ANO 字段 2216 可以是一字节字段，标识接入网类型、网络是否提供因特网连接的指示、网络是否需要额外接入步骤的指示、紧急服务是否通过 AP 可达的指示以及未授权紧急服务是否通过 AP 可达的指示。AP CCC 字段 2222 可以是一字节无符号整数，每次 AP 配置参数集改变时该值就递增 (increment)。

[0177] 基于图 22 中的 FD 帧主体 2204 设计以及假定 8 字节的典型 SSID 字段 2212，则不需要可选信息项，即仅 SSID 字段 2212，FD 帧主体 2204 大小是 10 字节。如果所有可选信息项 (2214-2224) 被包含，则 FD 帧主体 2204 大小是 26 字节，其也是典型 SSID 的最大 FD 帧主体大小。

[0178] 基于系统业务量测量，大约 75％的信标帧的长度是 158 字节。由于 MAC 帧开销是 28 字节 (包括管理帧 MAC 报头和 FCS)，典型信标帧主体大小大约是 130 字节。因此，如果不包含可选信息项，如图 22 所示的 FD 帧主体是典型信标帧主体大小 (130 字节) 的大约 7.7％。如果包含所有可选信息项，FD 帧主体是典型信标帧主体大小 (130 字节) 的 20％。

[0179] 当在 FD 帧中需要附加信息项时，FD 帧主体设计是可扩展的。存在支持可扩展 FD 帧主体设计的两种机制。在一种选项中，使用 FD 帧控制字段中的可用比特，其是之前预留的比特或来自扩展 FD 帧控制字段大小的新比特。在第二选项中，IE 用于每个信息项，包括三个部分 :元素 ID、长度和主体。

[0180] 图 23 示出了具有扩展的信息项的 FD 帧 2300 的示例。FD 帧 2300 包括 FD 帧报头 2302、FD 帧主体 2304、以及 FCS 字段 2306。FD 帧主体 2304 包括 FD 帧控制字段 2310、SSID 字段 2312、能力字段 2314、ANO 字段 2316、安全字段 2318、CCC 字段 2320、ANT 字段 2322、邻居 AP 信息字段 2324、附加可选字段 2326 以及可选 IE 2328。

[0181] 具有 FD 帧主体可扩展性，AP 可以在 FD 帧中灵活包含附加信息项以促进 FILS 和 / 或减少探测请求 / 响应帧传输的数量。附加可选信息项的一个示例可以是时间同步信息，例如全时间戳值或某种形式的压缩的时间戳信息。另一示例是 BSS 负载信息，使用已有 BSS

负载相关 IE 或用增强的 BSS 负载信息选择和编码引入新可选信息字段或元素。

[0182] FD 帧可以设计为公共动作帧或扩展帧。公共动作帧是 MAC 管理帧。在“公共动作字段”中有一些未使用的码，其当前被预留。可以通过使用预留码中的一个来定义新的公共动作帧。图 24 示出了编码 FD 帧 2400 作为新的公共动作帧的示例，其中公共动作字段＝ 16 被指派给 FD 帧 2400。

[0183] FD 帧 2400 包括 MAC 报头 2402、帧主体 2404、以及 FCS 字段 2406。MAC 报头 2402 包括帧控制字段 2410、持续时间 /ID(UD) 字段 2412、目的地地址字段 2414、源地址字段 2416、BSSID 字段 2418、序列控制 (SC) 字段 2420 以及 HT 控制 (HTC) 字段 2422。帧主体 2404 包括动作字段 2430、一个或多个可选的卖方特定 IE 2432 以及可选管理消息完整性码 (MIC) 元素 2434。

[0184] 动作字段包括类别字段 2440、公共动作字段 2442、FD 帧控制字段 2444、SSID 字段 2446、能力字段 2448、ANO 字段 2450、安全字段 2452、CCC 字段 2454、ANT 字段 2456 以及邻居 AP 信息字段 2458。FD 帧控制字段 2444 包括 SSID 长度子字段 2460、能力存在指示符子字段 2462、ANO 存在指示符子字段 2464、安全存在指示符子字段 2466、CCC 存在指示符子字段 2468、ANT 存在指示符子字段 2470、邻居 AP 信息存在指示符子字段 2472 以及预留子字段 2474。

[0185] 在图 24 中使用基于 802.11g 的 MAC 报头以用于例示。在具有 HT_GF 或 HT_MF PPDU 的 802.11n WLAN 系统中，在 MAC 管理帧的 AMC 报头中还包含 4 字节 HT 控制字段。

[0186] 扩展帧是 MAC 帧类型，其使用 MAC 报头的帧控制字段中的类型＝ 0b11。使用 4 比特子类型字段，可以定义多达 16 个扩展帧。该扩展帧的一个可用子类型值（例如子类型＝ 0b0010）可以用于将 FD 帧定义为新扩展帧。

[0187] 多个可替换详细的 MAC 帧设计可能用于 FD 扩展帧，包括单独的帧控制 (FC) 字段和特定 FD 帧控制字段以及组合的 FC 字段。这些设计之间的一个差别是如何组织帧控制信息，具体地，一般帧控制信息和 FD 帧特定控制信息是分开的还是组合的。

[0188] 图 25 示出了单独的 FC 字段和 FD 帧特定帧控制字段 (FD FC) 的 FD 帧 2500 设计。FD 帧 2500 包括 MAC 报头 2502、帧主体 2504 以及 FCS 字段 2506。MAC 报头 2502 包括帧控制字段 2510、源地址字段 2512 以及 HTC 字段 2514。源地址字段 2512 包含 FD 帧的发射 STA 的 MAC 地址，其也是基础设施 BSS 的 AP STA 的 BSSID。在一种实施中，源地址字段 2512 是 6 字节长。帧控制字段 2510 包括协议版本子字段 2520、类型子字段 2522、子类型子字段 2524、预留部分 2526 以及命令子字段 2528。该命令子字段 2528 用于指示 HTC 是否存在。

[0189] 帧主体 2504 包括 FD 帧控制字段 2530、SSID 字段 2532、FD 能力字段 2534、ANO 字段 2536、FD 安全字段 2538、CCC 字段 2540、ANT 字段 2542 以及邻居 AP 信息字段 2544。FD 帧控制字段 2530 包括 SSID 长度子字段 2550、能力存在指示符子字段 2552、ANO 存在指示符子字段 2554、安全存在指示符子字段 2556、CCC 存在指示符子字段 2558、ANT 存在指示符子字段 2560、邻居 AP 信息存在指示符子字段 2562 以及预留子字段 2564。

[0190] MAC 报头 2502 中的帧控制字段 2510 的第一字节是 FD 扩展帧的通用帧控制 (FC) 字段，其格式与其他 MAC 帧的第一字节相同，其他 MAC 帧包括管理帧、控制帧以及数据帧。使用这种格式对于接收 STA 使用帧控制字段中的信息（例如类型和子类型）来标识接收的帧来说是很重要的。如果其是已知的帧类型，则接收 STA 可以使用帧控制信息来解码接收的

帧的其余部分。如果其是未知帧类型，则接收 STA 使用聚合 MPDU(A-MPDU) 中的 PLCP 报头或 MPDU 分隔符中给定的长度信息跳过该帧。

[0191] 帧控制字段 2510 的第二个字节也是通用的，并包含命令子字段 2528，其用于指示是否存在 4 字节的 HTC 字段。帧控制字段 2510 的第二个字节中的其他 7 个比特被预留或用于其他目的，因为初始子字段不适用于 FD 帧。

[0192] 图 26 示出了通用帧控制信息与 FD 帧特定帧控制信息的组合的帧控制字段的 FD 扩展帧 2600 设计。FD 帧 2600 包括 MAC 报头 2602、帧主体 2604 以及 FCS 字段 2606。MAC 报头 2602 包括帧控制字段 2610、源地址字段 2612 以及 HTC 字段 2614。

[0193] 帧控制字段 2610 包括协议版本子字段 2620、类型子字段 2622、子类型子字段 2624、HTC 存在指示符子字段 2626、SSID 长度子字段 2628、能力存在指示符子字段 2630、ANO 存在指示符子字段 2632、安全存在指示符子字段 2634、CCC 存在指示符子字段 2636、ANT 存在指示符子字段 2638、邻居 AP 信息存在指示符子字段 2640 以及预留子字段 2642。帧控制字段 2610 的第一个字节与所有其他 MAC 帧具有相同格式。其包含用于接收 STA 标识所接收的帧并相应处理该接收的帧的信息。

[0194] 帧主体 2604 包括 SSID 字段 2650、FD 能力字段 2652、ANO 字段 2654、FD 安全字段 2656、CCC 字段 2658、ANT 字段 2660 及邻居 AP 信息字段 2662。

[0195] 如上所提及的，确定是否与 AP 关联是基于所接收的 FD 帧的。根据与上文公开的实施方式可有利结合的特定实施方式，在基于所接收的 FD 帧确定与 AP 相关联的情况下，关联请求帧被传送至所述 AP。

[0196] 根据特定实施方式，参考关于上文图 13 的公开，FD 帧内容包括物理层特定信息，该信息依据无线站接入的无线网络类型。此外，物理层特定信息可以有利地包括以下任何一者或多者：极高吞吐量能力信息、极高吞吐量操作信息或高吞吐量操作信息。

[0197] 虽然本发明的特征和元素以特定的组合在以上进行了描述，但本领域技术人员应该知道每个特征或元素可以单独使用或与其它特征和元素组合使用。尤其参考图 15-26，FD 帧的结构的示例已经详细地公开以增强对本发明概念的理解。应该理解的是，附图中增加细节所公开的 FD 帧元素的不同结合可以被改变。通过示例的方式，图 22 示出包括 FD 帧报头、FD 帧主体及 FCS 字段的 FD 帧，其中 FD 帧主体包括 FD 帧控制字段、SSID 字段、FD 能力字段、ANO 字段、FD 安全字段、CCC 字段、FD ANT 字段及邻居 AP 信息字段。然而，应该理解的是，在很大程度上 FD 中不同字段和项具有独立于其它字段功能的它们自己的可识别的功能，如关于图 22 的实施方式的公开中强调的（例如，因为 FD 能力字段可以是可选的，特定实施方式可以仅包括上文公开的除了 FD 能力字段外的所有字段；这还适用于其他字段，尤其是但不限于被指示为可选的其它字段）。

[0198] 此外，本文中描述的方法可以在由计算机或处理器执行的计算机程序、软件或固件中实施，其中所述计算机程序、软件或固件被包含在计算机可读存储介质中。计算机可读介质包括电子信号（通过有线或者无线连接而传送）和计算机可读存储介质。关于计算机可读存储介质的实例包括但不局限于只读存储器 (ROM)、随机存取存储器 (RAM)、寄存器、缓冲存储器、半导体存储设备、磁介质（例如内部硬盘或可移动磁盘）、磁光介质以及例如 CD-ROM 光盘或者数字多功能光盘 (DVD) 之类的光介质。与软件有关的处理器可以被实现用于 WTRU、UE、终端、基站、RNC 或者任何主计算机中的射频收发信机。

[0199] 实施例

[0200] 1、一种用于在无线站中的方法，该方法包括从接入点 (AP) 接收全信标帧的实例之间的快速初始链路建立发现 (FD) 帧，并基于接收到的 FD 帧确定是否与 AP 相关联。

[0201] 2、根据实施例 1 所述的方法，其中 FD 帧包括 FD 帧内容。

[0202] 3、根据实施例 1 或 2 所述的方法，其中 FD 帧包括 FD 帧控制字段。

[0203] 4、根据实施例 3 所述的方法，其中 FD 帧控制字段包括服务集标识符 (SSID) 长度字段，对应于 FD 帧内容中可变长度 SSID 字段的长度。

[0204] 5、根据实施例 4 所述的方法，其中 FD 帧控制字段包括能力存在指示符，指示相应能力字段在 FD 帧内容中是否存在。

[0205] 6、根据实施例 5 所述的方法，其中能力字段包括 AP 的能力信息。

[0206] 7、根据实施例 6 所述的方法，其中能力信息包括以下的任意一者或多者 :扩展的服务集信息、独立基本服务集信息、无争用 (CF) 可轮询指示、CF 轮询请求指示、隐私信息、短前导码指示、网际协议 (IP)v4 支持指示、IPv6 支持指示、频谱管理信息、服务质量信息、短时隙信息、无线电管理信息、延迟块应答 (ACK) 指示、即时 ACK 指示、物理层类型信息或支持的最小速率信息。

[0207] 8、根据实施例 4-7 中任一个所述的方法，其中 FD 帧控制字段包括接入网选项存在指示符，指示在 FD 帧内容中是否存在相应的接入网选项字段。

[0208] 9、根据实施例 8 所述的方法，其中接入网选项字段指示 AP 提供的接入服务。

[0209] 10、根据实施例 8 或 9 所述的方法，其中接入网选项字段包括以下任意一者或多者 :接入网类型字段、接入字段所需的附加步骤、紧急服务可达字段或未认证紧急服务可接入字段。

[0210] 11、根据实施例 4-10 中任一个所述的方法，其中 FD 帧控制字段包括安全存在指示符，指示 FD 帧内容中是否存在相应的安全字段。

[0211] 12、根据实施例 11 所述的方法，其中安全字段指示 AP 使用的一种或多种类型的安全性。

[0212] 13、根据实施例 12 所述的方法，其中安全字段包括以下任意一者或多者 :群组数据密码套件字段、成对密码套件计数字段、成对密码套件列表字段、认证和密钥管理 (AKM) 套件计数字段、AKM 套件列表字段、鲁棒安全网络能力字段、成对主密钥标识符 (PMKID) 计数字段、PMKID 列表字段、群组管理密码套件字段或组合的群组和成对密码套件字段。

[0213] 14、根据实施例 13 所述的方法，其中鲁棒安全网络能力字段包括以下的任意一者或多者 :预认证指示符、管理帧保护所需指示符、快速初始链路建立 (FILS) 快速可扩展认证协议 (EAP) 指示符、FILS EAP 重新认证协议指示符、FILS 非 EAP 指示符、没有第三方的 FILS 认证指示符、管理帧保护能力指示符或理想转发秘密指示符。

[0214] 15、根据实施例 4-14 中任意一个所述的方法，其中 FD 帧控制字段包括 AP 配置改变计数存在指示符，指示相应 AP 配置改变计数字段是否存在于 FD 帧内容中。

[0215] 16、根据实施例 15 所述的方法，其中 AP 配置改变计数字段指示 AP 配置参数集发生改变的次数。

[0216] 17、根据实施例 4-16 任意一个所述的方法，其中 FD 帧控制字段包括 AP 下一个目标信标传输时间存在指示符，指示 FD 帧内容中是否存在相应 AP 下一个目标信标传输时间

字段。

[0217] 18、根据实施例 17 所述的方法，其中 AP 下一个目标信标传输时间字段指示来自 AP 的下一个全信标帧的传输时间。

[0218] 19、根据实施例 18 所述的方法，其中 AP 下一个目标信标传输时间被表达为相对于 FD 帧传输时间的偏移值。

[0219] 20、根据实施例 4-19 任意一个所述的方法，其中 FD 帧控制字段包括邻居 AP 信息存在指示符，指示在 FD 帧内容中是否存在相应邻居 AP 信息字段。

[0220] 21、根据实施例 20 所述的方法，其中邻居 AP 信息字段包括操作种类字段、信道数量字段以及针对邻居 AP 信息字段中的每个邻居 AP 的下一个目标信标传输时间字段

[0221] 22、根据实施例 21 所述的方法，其中每个下一个目标信标传输时间字段指示来自相应邻居 AP 的下一个全信标帧的传输时间。

[0222] 23、根据实施例 22 所述的方法，其中下一个目标信标传输时间被表达为相对于 FD 帧传输时间的偏移值。

[0223] 24、根据实施例 19 或 23 所述的方法，其中偏移值被表达为时间单元的数量。

[0224] 25、根据实施例 1-24 中任意一个所述的方法，其中 FD 帧内容包括可选字段或可选信息元素。

[0225] 26、根据实施例 25 所述的方法，其中在 FD 帧内容包括任意可选字段的情况下，对应于可选字段的存在指示符被包含在 FD 帧控制字段中。

[0226] 27、根据实施例 1-26 中任意一个所述的方法，该方法还包括在基于接收的 FD 帧确定与 AP 相关联的情况下，向 AP 传送关联请求帧。

[0227] 28、根据实施例 1-27 中任意一个所述的方法，其中 FD 帧内容包括物理层特定信息，该信息依据无线站接入的无线网络的类型。

[0228] 29、根据实施例 28 所述的方法，其中物理层特定信息包括以下中的任意一者或多者：极高吞吐量能力信息、极高吞吐量操作信息或高吞吐量操作信息。

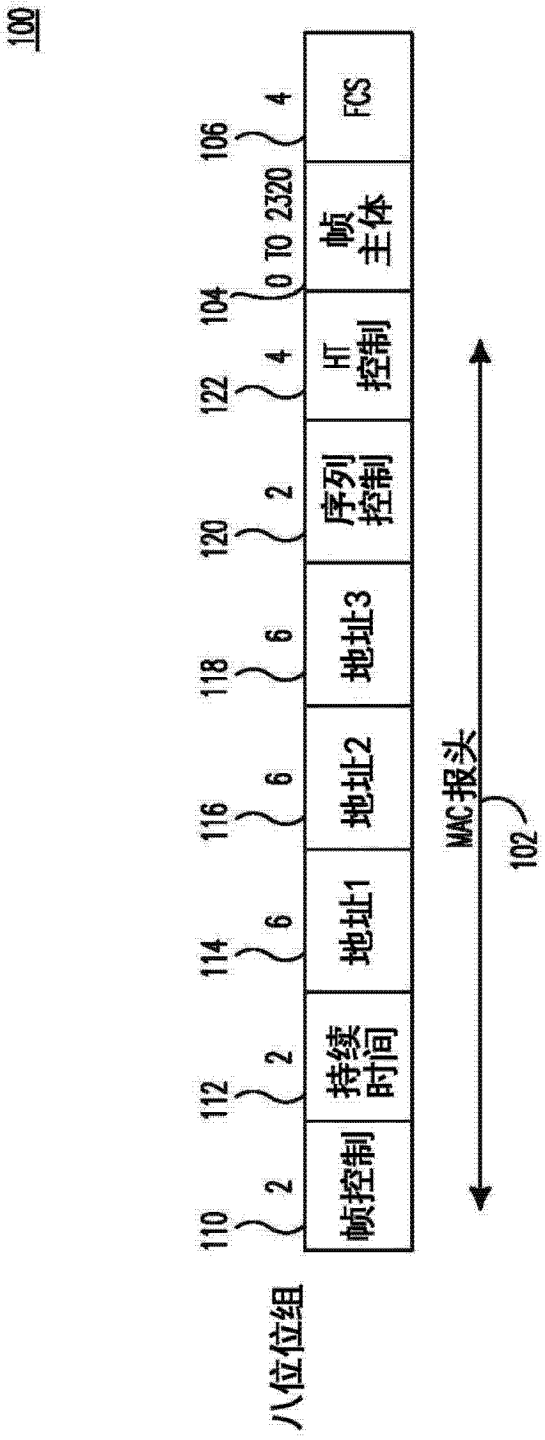

100
帧控制
持续时间
地址1
地址2
地址3
序列控制
HT控制
帧主体
FCS
0 TO 2320
2
2
6
6
6
2
4
4
110
112
114
116
118
120
122
104
106
MAC报头
102
八位位组

图 1

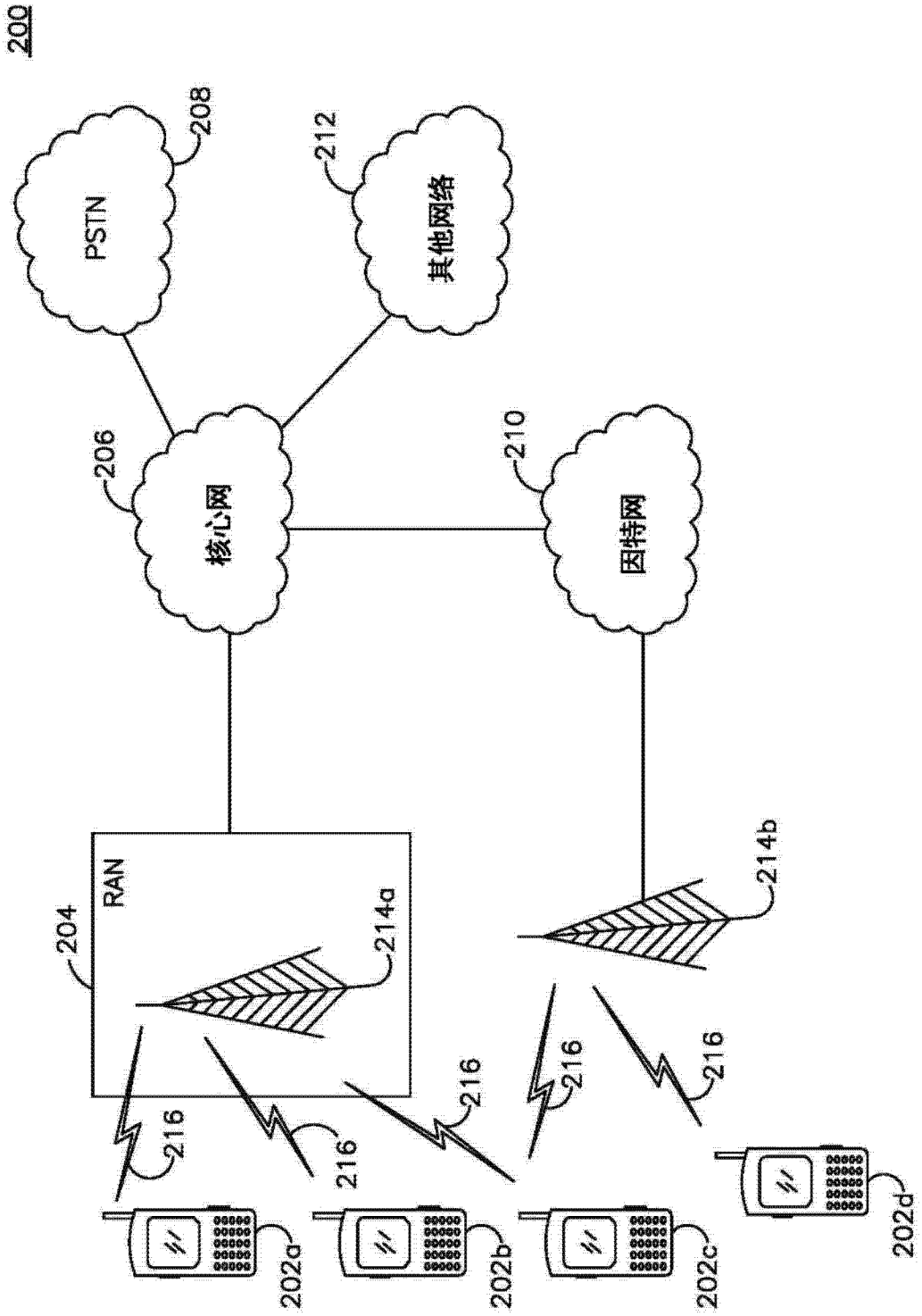

200
PSTN
208
212
其他网络
206
核心网
210
因特网
RAN
204
214a
214b
216
216
216
216
216
202a
202b
202c
202d

图 2A

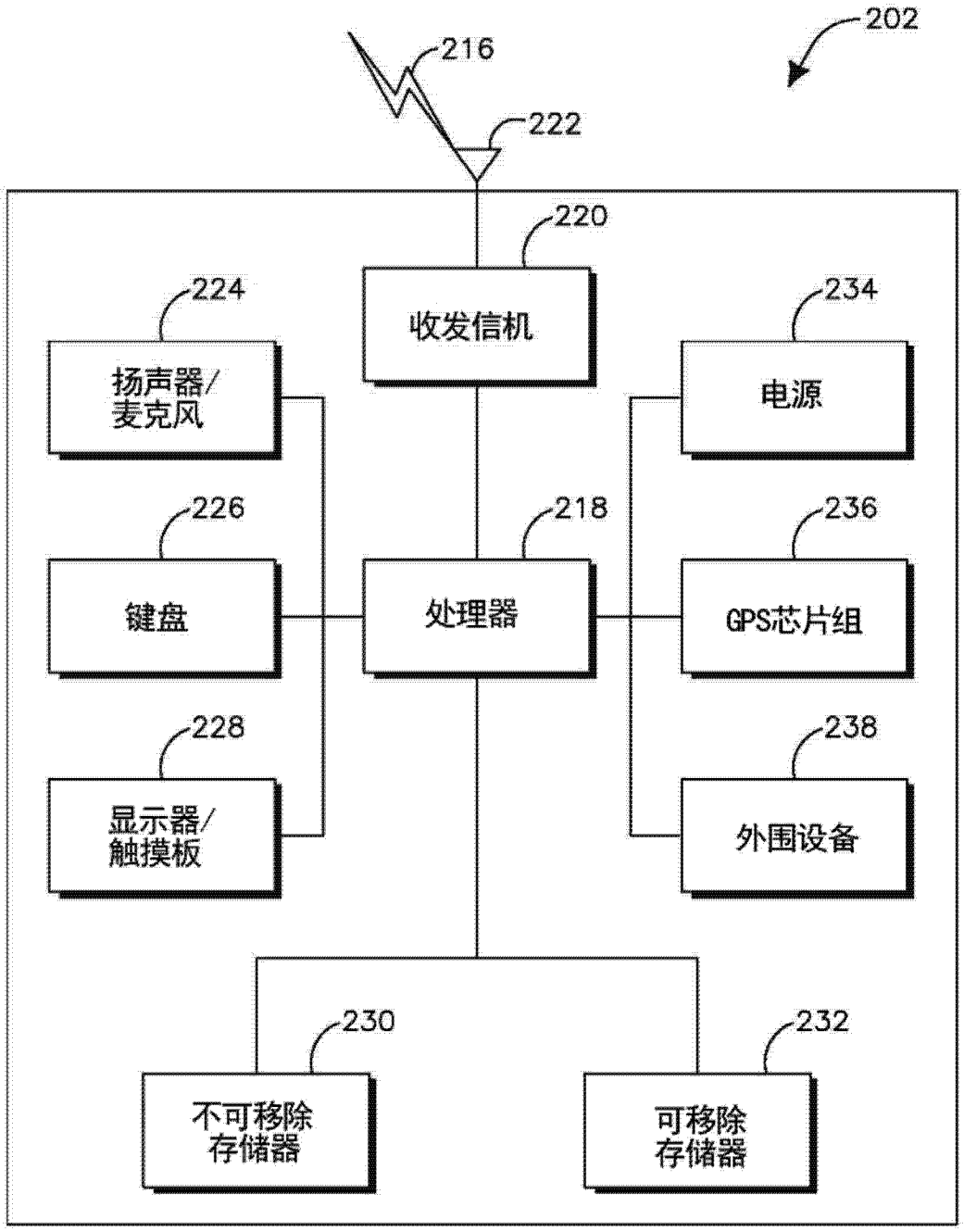

202
216
222
220
收发信机
224
扬声器/
麦克风
234
电源
226
键盘
218
处理器
236
GPS芯片组
228
显示器/
触摸板
238
外围设备
230
不可移除
存储器
232
可移除
存储器

图 2B

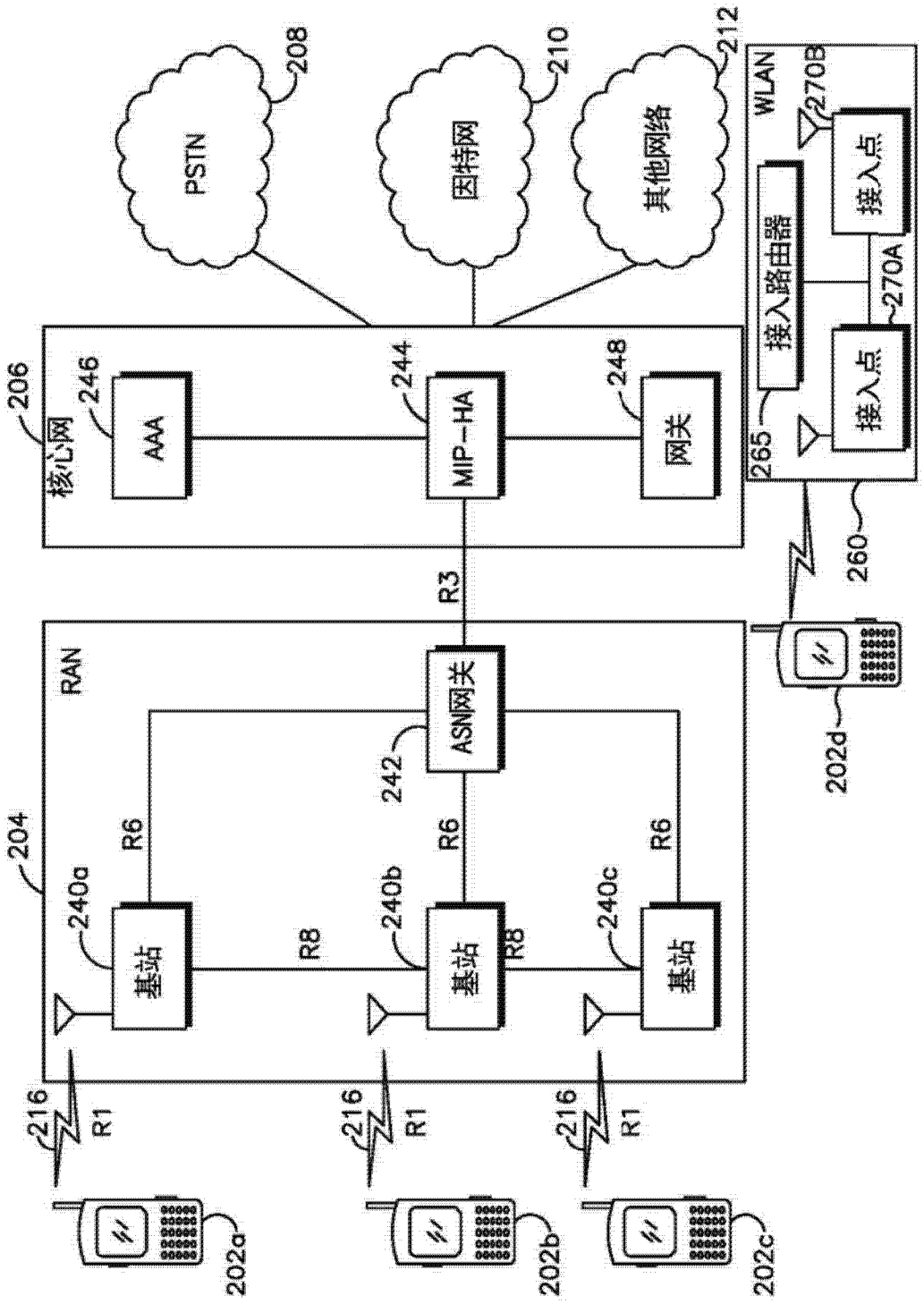

PSTN
208
因特网
210
其他网络
212
WLAN
270B
接入点
接入路由器
270A
接入点
265
206
核心网
246
AAA
244
MIP-HA
248
网关
R3
260
RAN
204
ASN网关
242
R6
R6
R6
240a
240b
240c
基站
基站
基站
R8
R8
216
R1
216
R1
216
R1
202a
202b
202c
202d

图 2C

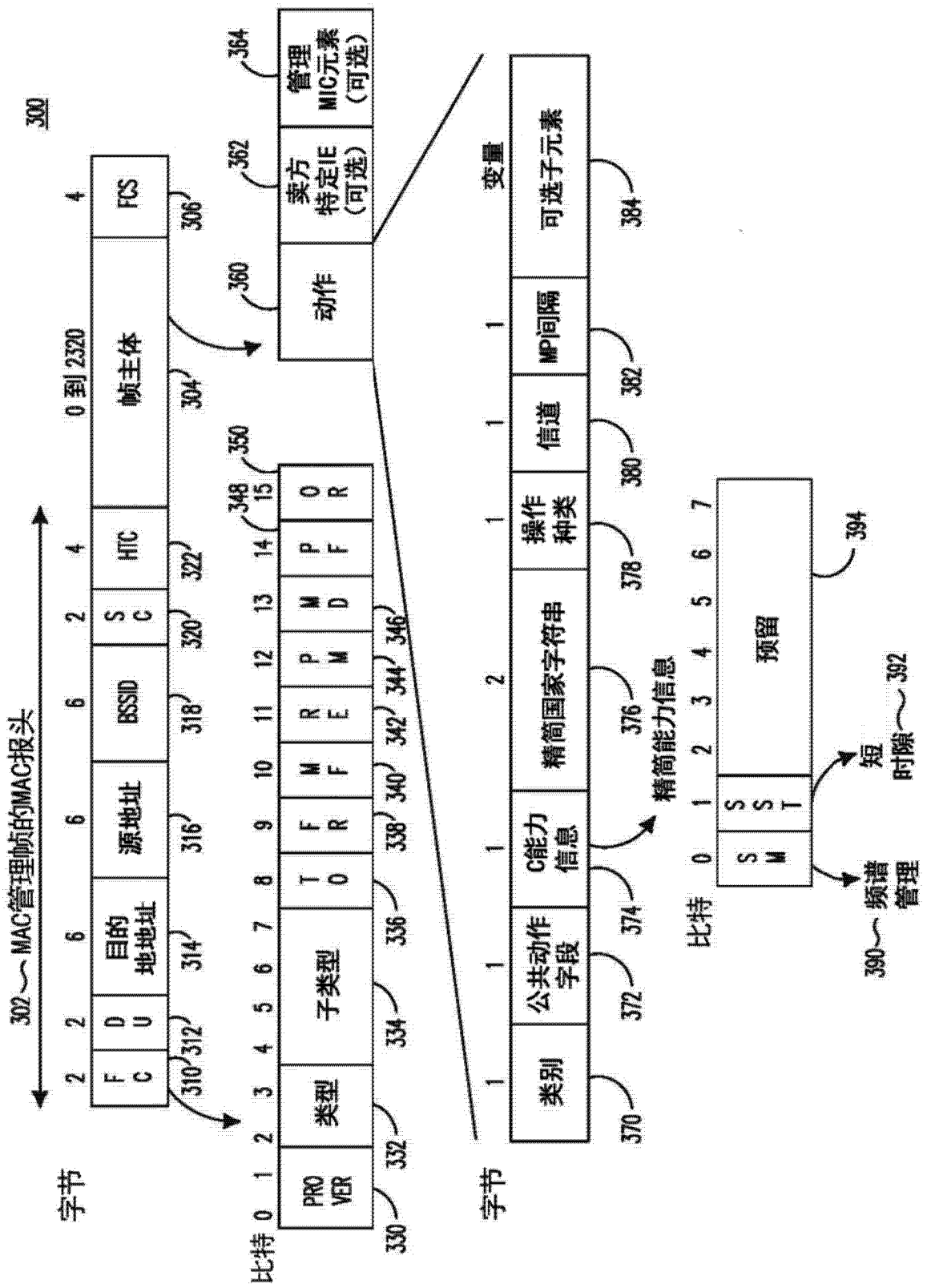

300
302 MAC管理帧的MAC报头
字节
比特
FC
DU
目的地址
源地址
BSSID
SC
HTC
帧主体
FCS
0 到 2320
PRO VER
类型
子类型
TO DS
FR DS
MF
RE
PM
MD
PF
OR
动作
类方特定IE（可选）
管理MIC元素（可选）
变量
类别
公共动作字段
C能力信息
精简国家字符串
操作种类
信道
MP间隔
可选子元素
精简能力信息
SSMT
预留
短时隙
频谱管理

图 3

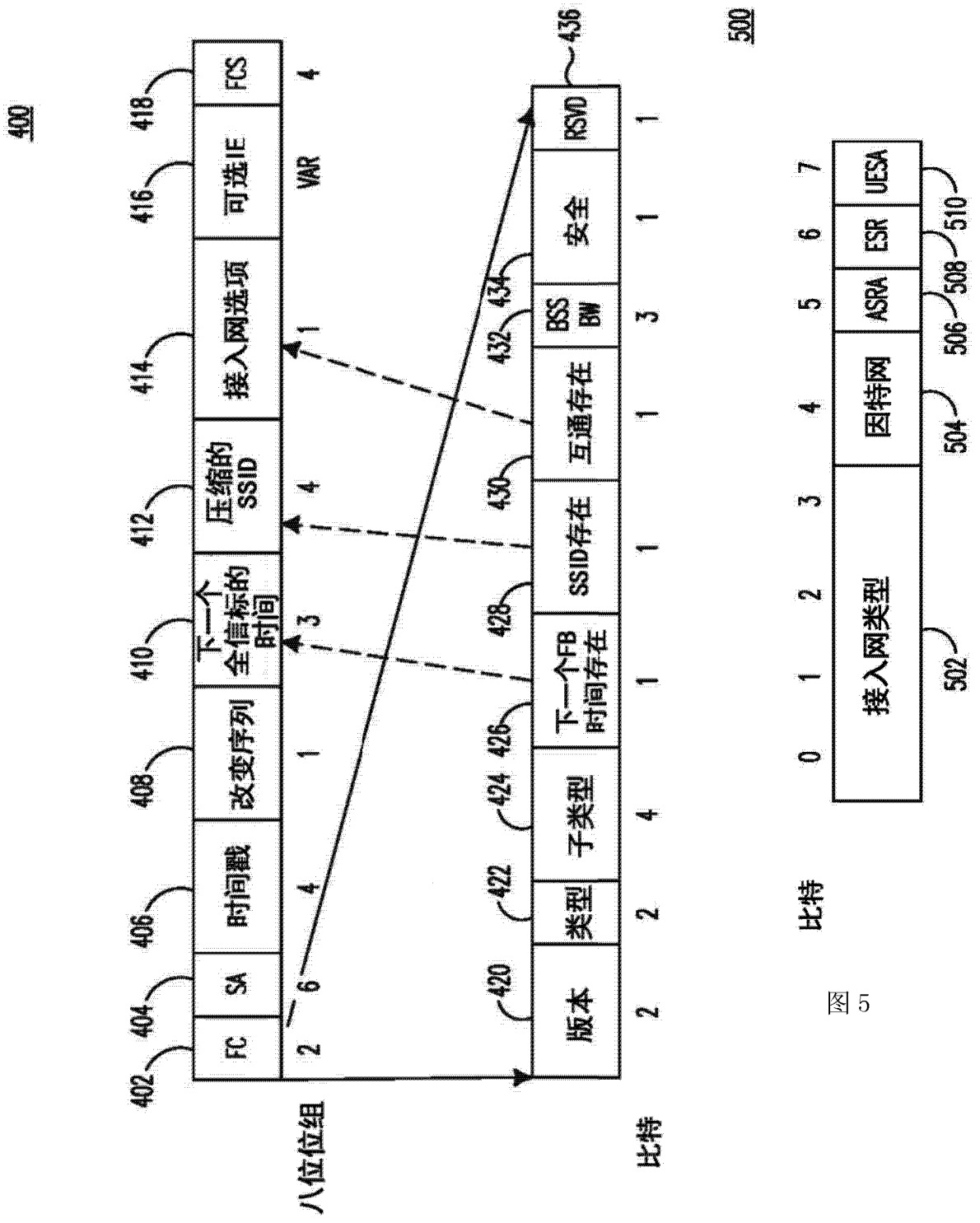

400
FC
SA
时间戳
改变序列
下一个全信标的时间
压缩的SSID
接入网选项
可选IE
FCS
402
404
406
408
410
412
414
416
418
八位位组
2
6
4
1
3
4
VAR
4
版本
类型
子类型
下一个FB时间存在
SSID存在
互通存在
BSS BW
安全
RSVD
420
422
424
426
428
430
432
434
436
比特
2
2
4
1
1
1
3
1
1
500
比特
0 1 2 3 4 5 6 7
接入网类型
因特网
ASRA
ESR
UESA
502
504
506
508
510

图 4

图 5

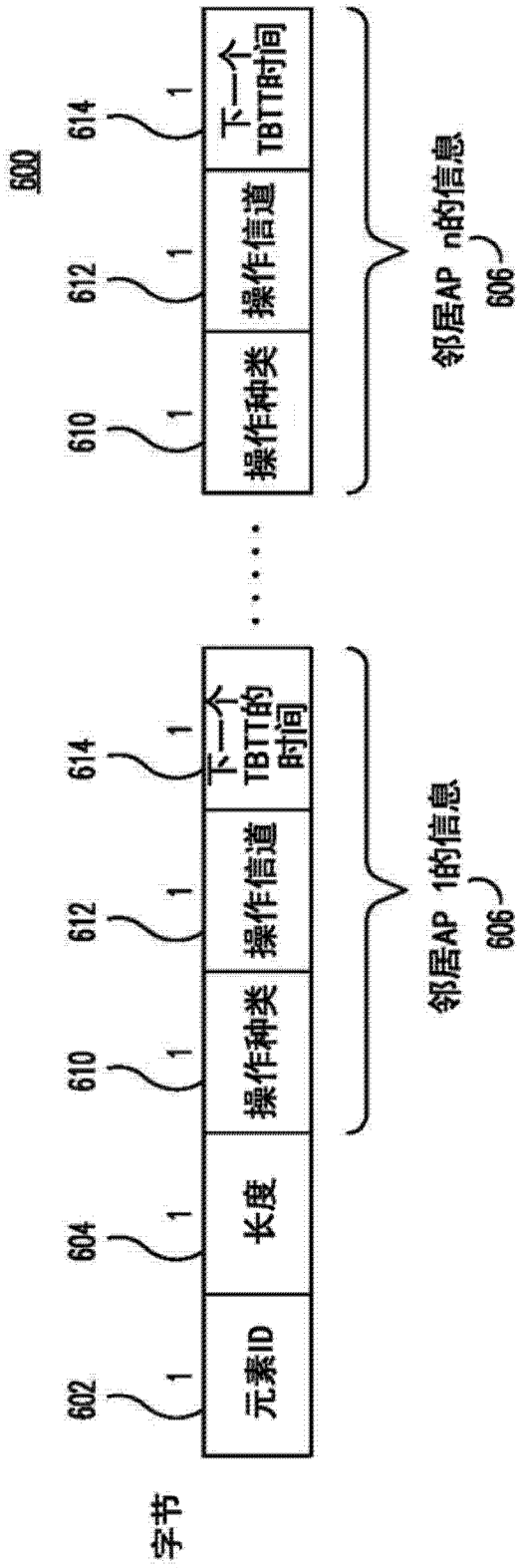

600
602
604
610
612
614
元素ID
长度
操作种类
操作信道
下一个TBTT的时间
邻居AP 1的信息
606
操作种类
操作信道
下一个TBTT时间
邻居AP n的信息
606
字节
1

图 6

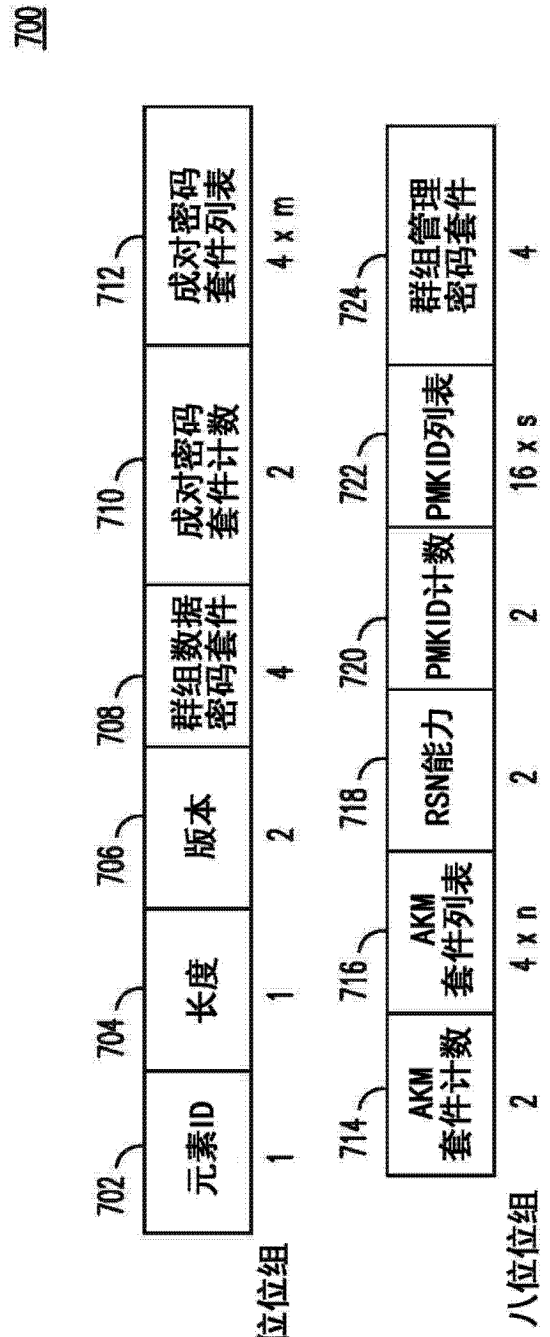

700
702
704
706
708
710
712
元素ID
长度
版本
群组数据密码套件
成对密码套件计数
成对密码套件列表
八位位组
1
1
2
4
2
4 x m
714
716
718
720
722
724
AKM套件计数
AKM套件列表
RSN能力
PMKID计数
PMKID列表
群组管理密码套件
八位位组
2
4 x n
2
2
16 x s
4

图 7

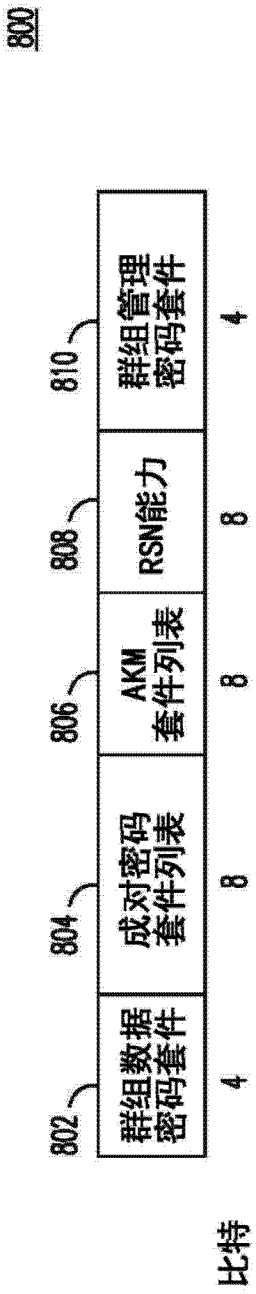

800
802
群组数据密码套件
4
804
成对密码套件列表
8
806
AKM套件列表
8
808
RSN能力
8
810
群组管理密码套件
4
比特

图 8

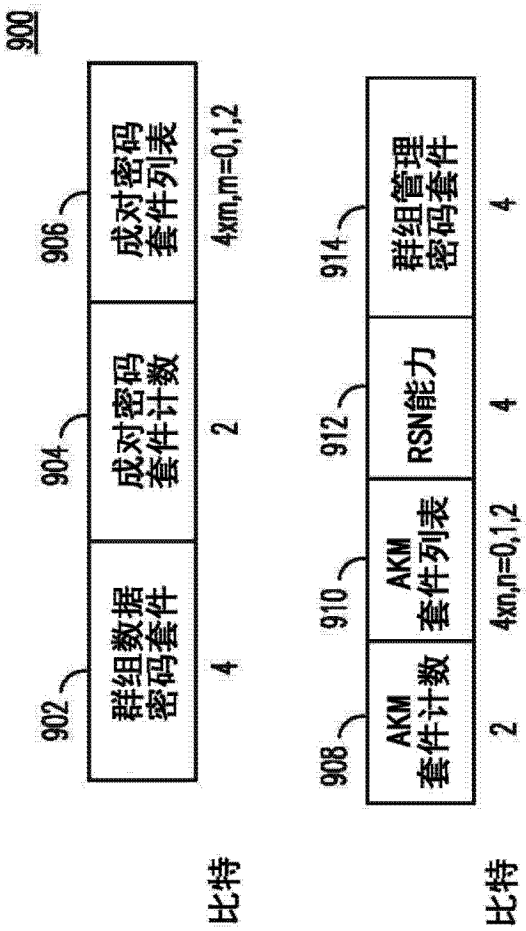

900
902
群组数据密码套件
4
904
成对密码套件计数
2
906
成对密码套件列表
4xm,m=0,1,2
比特
908
AKM套件计数
2
910
AKM套件列表
4xn,n=0,1,2
912
RSN能力
4
914
群组管理密码套件
4
比特

图 9

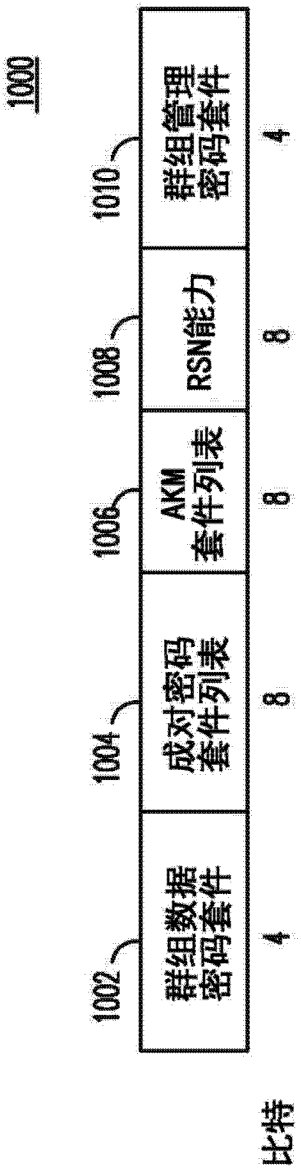

1000
1002
群组数据密码套件
4
1004
成对密码套件列表
8
1006
AKM套件列表
8
1008
RSN能力
8
1010
群组管理密码套件
4
比特

图 10

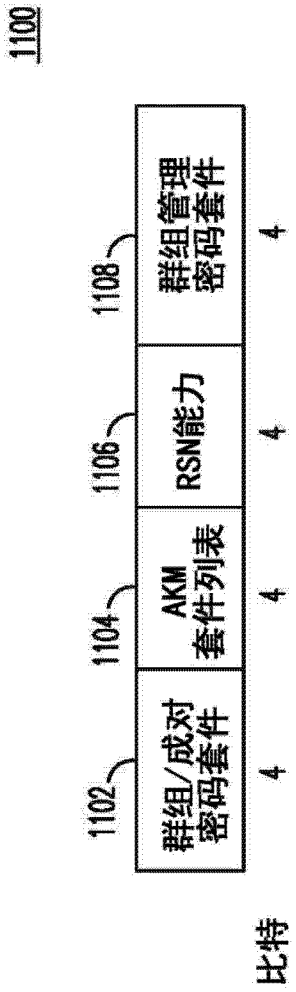

1100
1102
群组/成对密码套件
1104
AKM套件列表
1106
RSN能力
1108
群组管理密码套件
4
4
4
4
比特

图 11

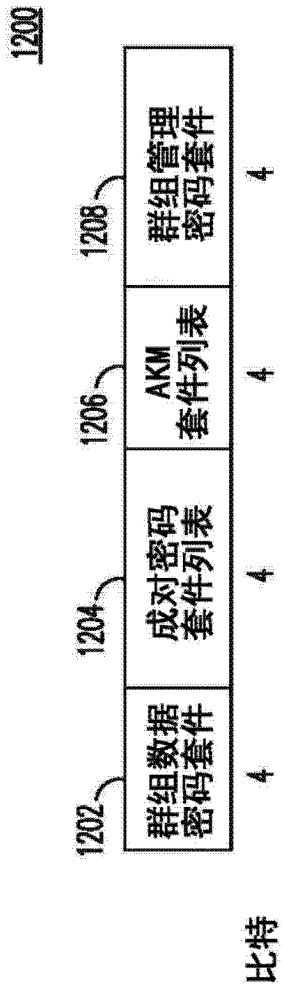

1200
1202
群组数据密码套件
1204
成对密码套件列表
1206
AKM套件列表
1208
群组管理密码套件
4
4
4
4
比特

图 12

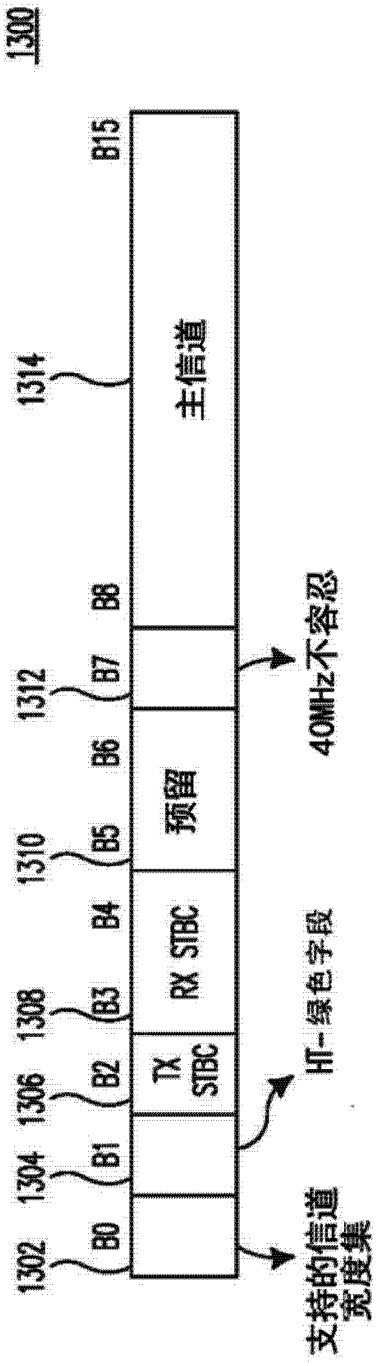

1300
1302
B0
1304
B1
1306
B2
1308
B3
1310
B4
1312
B5
1314
B6
B7
B8
B15
TX STBC
RX STBC
预留
主信道
支持的信道宽度集
HT-绿色字段
40MHz不容忍

图 13

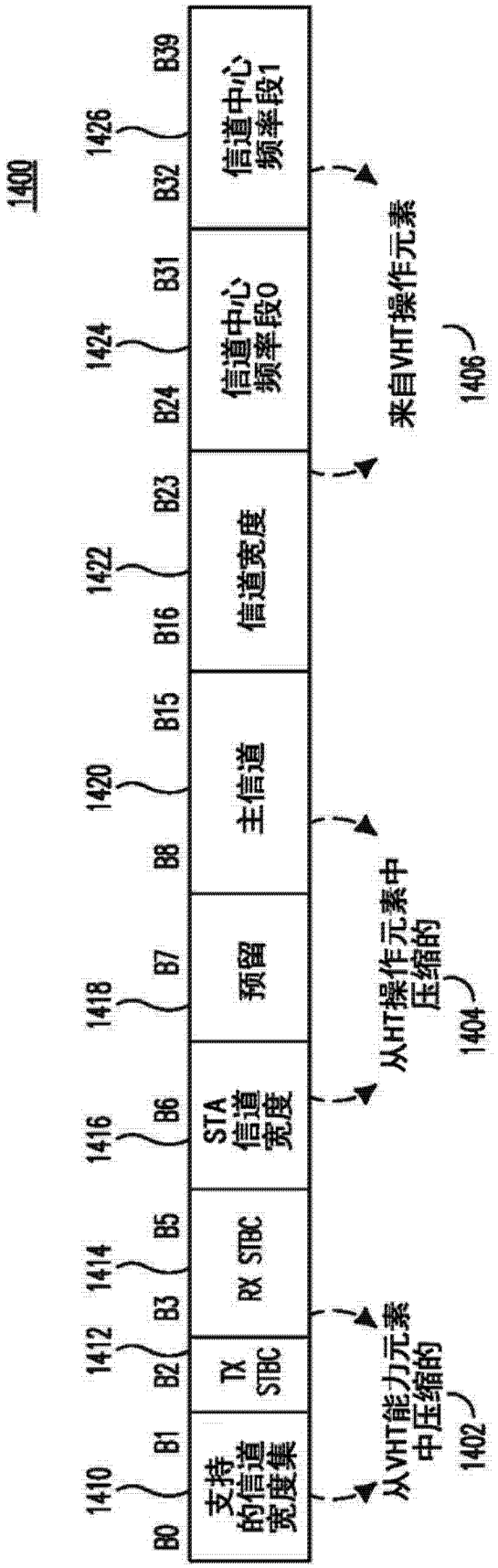

1400
B0
B1
B2
B3
B5
B6
B7
B8
B15
B16
B23
B24
B31
B32
B39
1410
1412
1414
1416
1418
1420
1422
1424
1426
支持的信道宽度集
TX STBC
RX STBC
STA信道宽度
预留
主信道
信道宽度
信道中心频率段0
信道中心频率段1
从VHT能力元素中压缩的
1402
从HT操作元素中压缩的
1404
来自VHT操作元素
1406

图 14

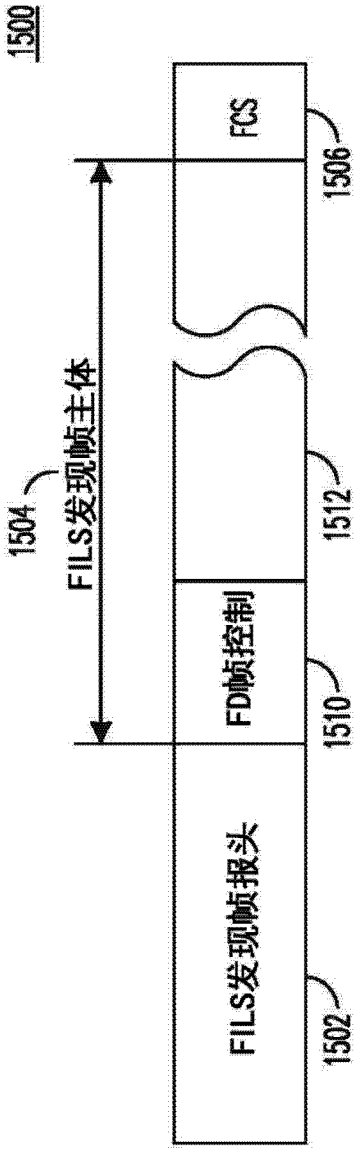

1500
FILS发现帧报头
FD帧控制
FCS
1502
1510
1506
1504
FILS发现帧主体
1512

图 15

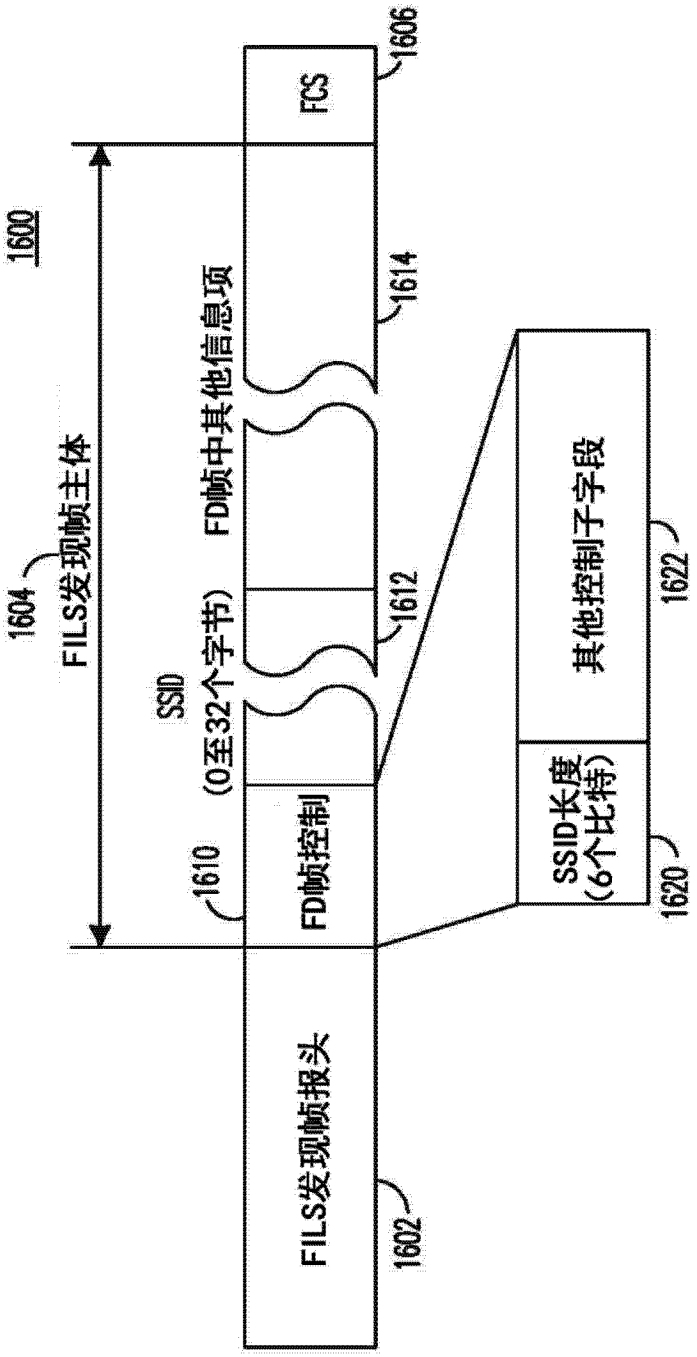

1600
1604
FILS发现帧主体
FILS发现帧报头
1602
FD帧控制
1610
SSID
(0至32个字节)
FD帧中其他信息项
1612
1614
FCS
1606
SSID长度
(6个比特)
1620
其他控制子字段
1622

图 16A

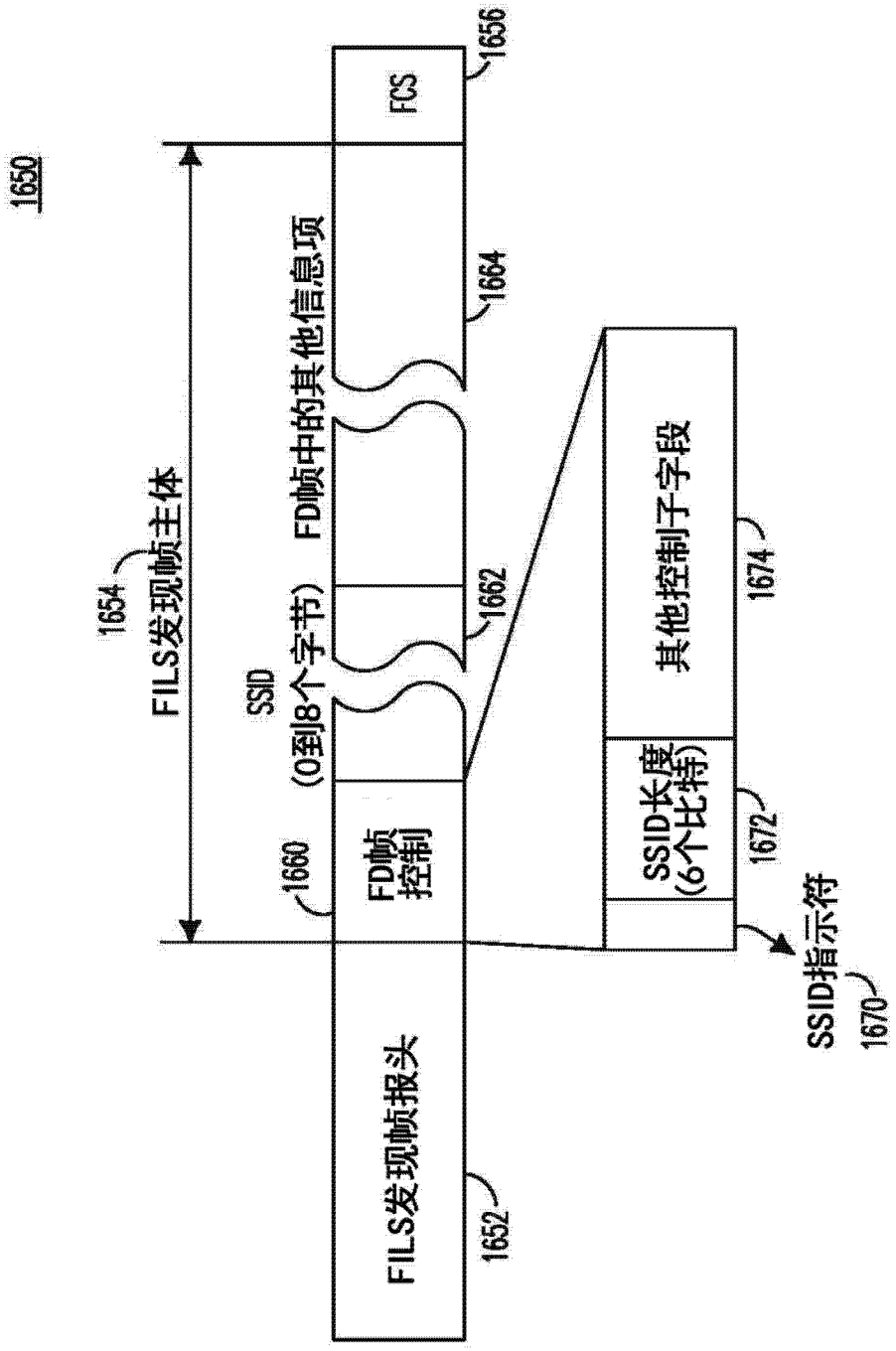

1650
1654
FILS发现帧主体
FILS发现帧报头
1652
SSID
(0到8个字节)
1660
FD帧
控制
FD帧中的其他信息项
1662
1664
FCS
1656
其他控制子字段
1674
SSID长度
(6个比特)
1672
SSID指示符
1670

图 16B

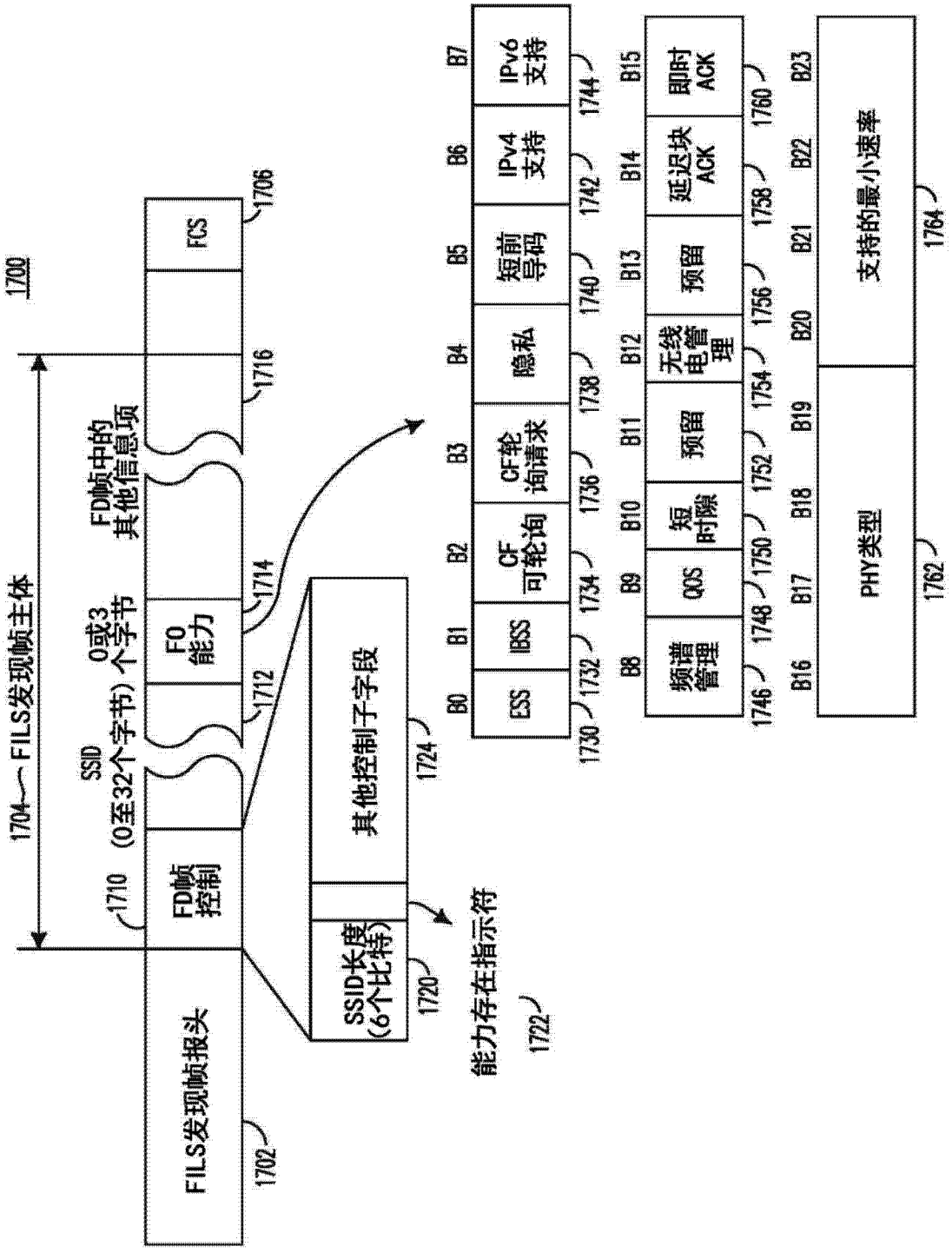

1700
1704
FILS发现帧主体
FILS发现帧报头
1702
FD帧控制
1710
SSID
(0至32个字节)
0或3
个字节
FD能力
1712
1714
FD帧中的
其他信息项
1716
FCS
1706
SSID长度
(6个比特)
1720
其他控制子字段
1724
能力存在指示符
1722
B0 B1 B2 B3 B4 B5 B6 B7
ESS
IBSS
CF
可轮询
CF轮
询请求
隐私
短前
导码
IPv4
支持
IPv6
支持
1730
1732
1734
1736
1738
1740
1742
1744
B8 B9 B10 B11 B12 B13 B14 B15
频谱
管理
QOS
短
时隙
预留
无线
电管
理
预留
延迟块
ACK
即时
ACK
1746
1748
1750
1752
1754
1756
1758
1760
B16 B17 B18 B19 B20 B21 B22 B23
PHY类型
支持的最小速率
1762
1764

图 17

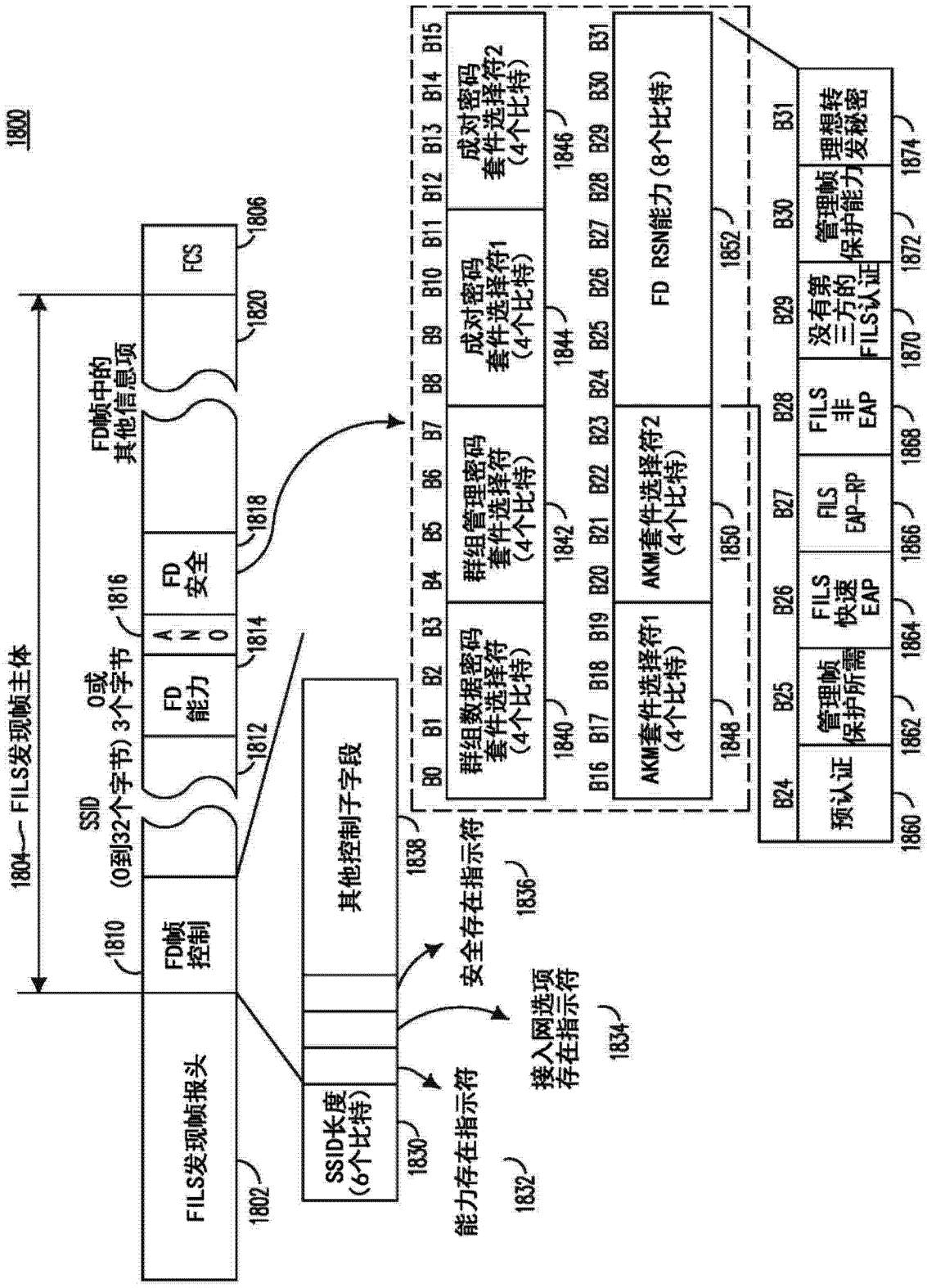

1800
1804 FILS发现帧主体
FILS发现帧报头
1802
SSID
(0到32个字节)
0或
3个字节
FD帧
控制
1810
FD
能力
1812
A
N
O
1814
FD
安全
1816
1818
FD帧中的
其他信息项
1820
FCS
1806
SSID长度
(6个比特)
1830
能力存在指示符
1832
安全存在指示符
1836
其他控制子字段
1838
接入网选项
存在指示符
1834
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15
群组数据密码
套件选择符
(4个比特)
1840
群组管理密码
套件选择符
(4个比特)
1842
成对密码
套件选择符1
(4个比特)
1844
成对密码
套件选择符2
(4个比特)
1846
B16 B17 B18 B19 B20 B21 B22 B23 B24 B25 B26 B27 B28 B29 B30 B31
AKM套件选择符1
(4个比特)
1848
AKM套件选择符2
(4个比特)
1850
FD RSN能力(8个比特)
1852
B24 B25 B26 B27 B28 B29 B30 B31
预认证
1860
管理帧
保护所需
1862
FILS
快速
EAP
1864
FILS
EAP-RP
1866
FILS
非
EAP
1868
没有第
三方的
FILS认证
1870
管理帧
保护能力
1872
理想转
发秘密
1874

图 18

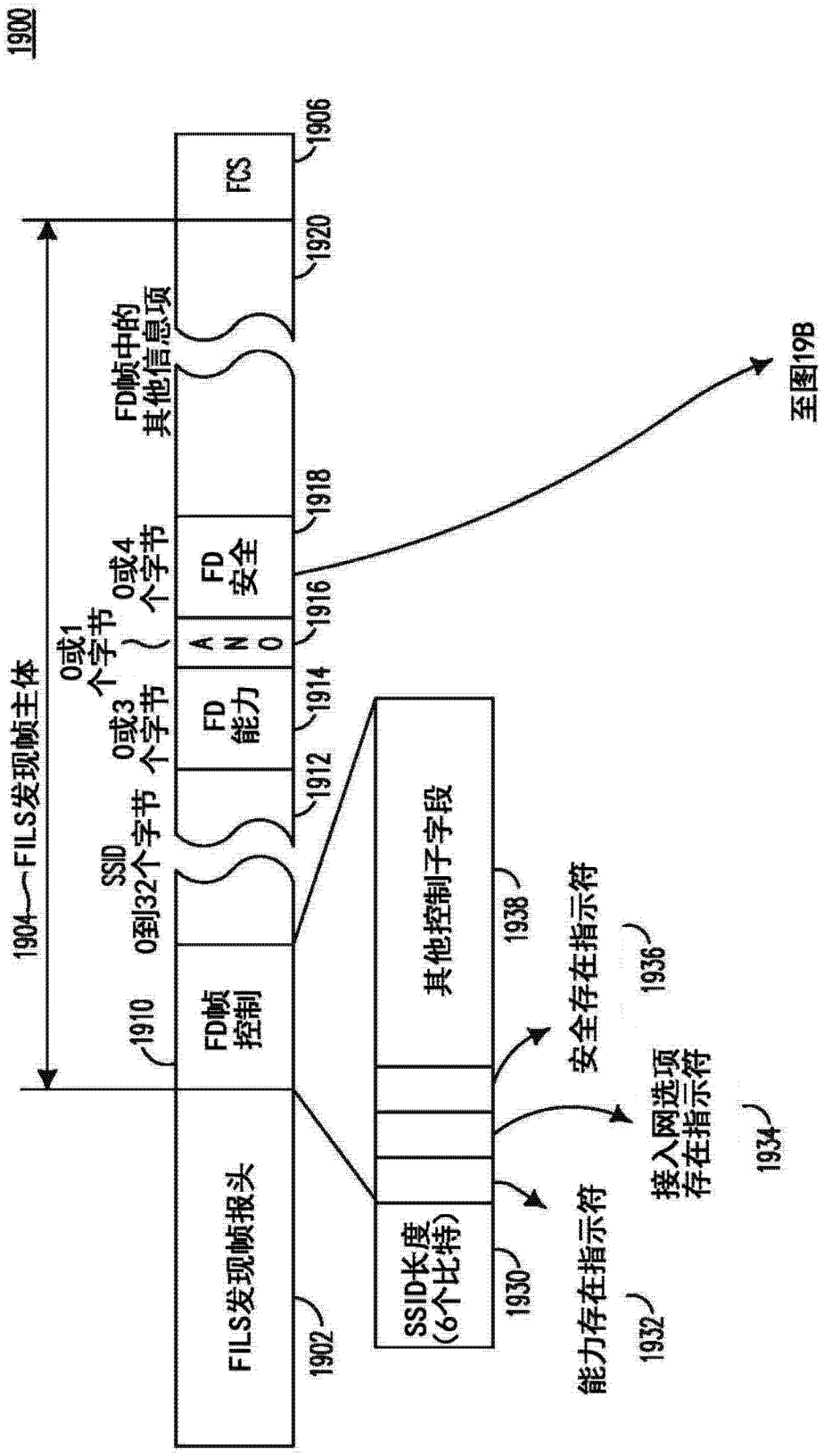

1900
1904 FILS发现帧主体
FILS发现帧报头
1902
FD帧控制
1910
SSID
0到32个字节
0或3个字节
FD能力
1912
1914
ANO
1916
0或1个字节
0或4个字节
FD安全
1918
FD帧中的其他信息项
1920
FCS
1906
至图19B
其他控制子字段
1938
SSID长度(6个比特)
1930
能力存在指示符
1932
安全存在指示符
1936
接入网选项存在指示符
1934

图 19A

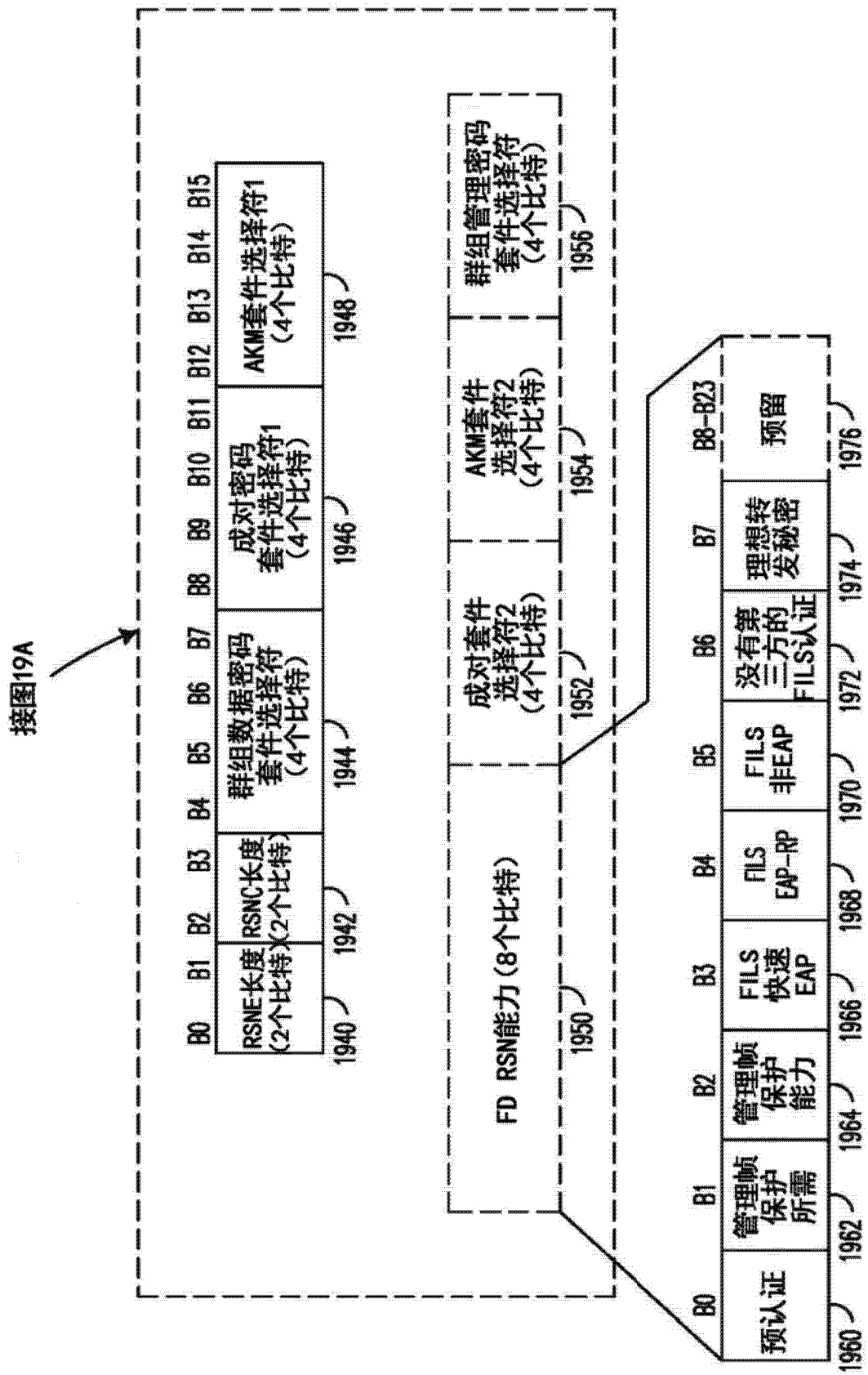

接图19A
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15
RSNE长度(2个比特)
RSNC长度(2个比特)
群组数据密码套件选择符(4个比特)
成对密码套件选择符1(4个比特)
AKM套件选择符1(4个比特)
1940
1942
1944
1946
1948
FD RSN能力(8个比特)
成对套件选择符2(4个比特)
AKM套件选择符2(4个比特)
群组管理密码套件选择符(4个比特)
1950
1952
1954
1956
B0 B1 B2 B3 B4 B5 B6 B7 B8-B23
预认证
管理帧保护所需
管理帧保护能力
FILS快速EAP
FILS EAP-RP
FILS非EAP
没有第三方的FILS认证
理想转发秘密
预留
1960
1962
1964
1966
1968
1970
1972
1974
1976

图 19B

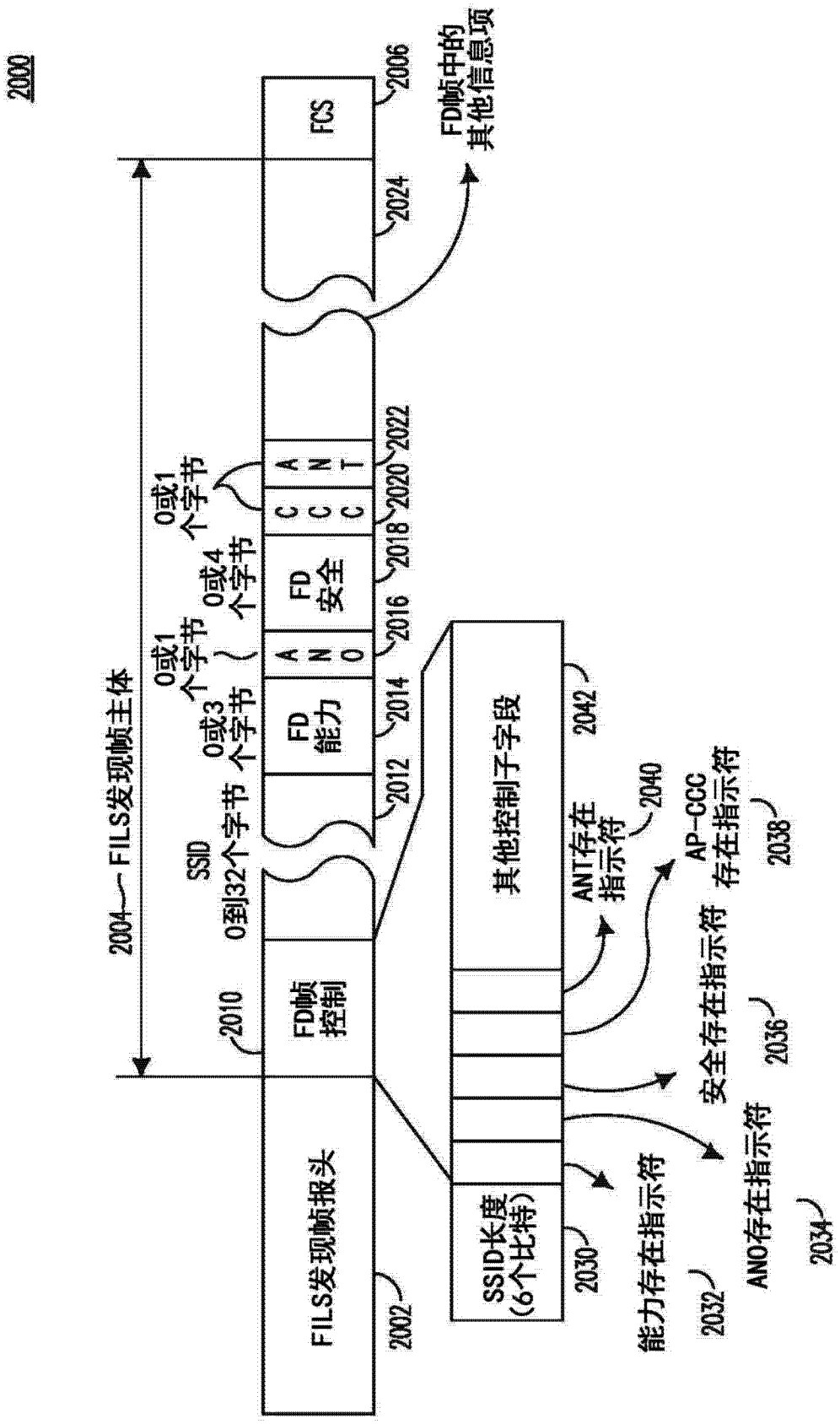

2000
2004 FILS发现帧主体
FILS发现帧报头
2002
SSID长度
(6个比特)
2030
能力存在指示符
2032
ANO存在指示符
2034
安全存在指示符
2036
AP-CCC
存在指示符
2038
ANT存在
指示符
2040
其他控制子字段
2042
FD帧
控制
2010
SSID
0到32个字节
2012
0或3
个字节
FD
能力
2014
0或1
个字节
ANO
2016
0或4
个字节
FD
安全
2018
CCC
2020
0或1
个字节
ANT
2022
FCS
2006
2024
FD帧中的
其他信息项

图 20

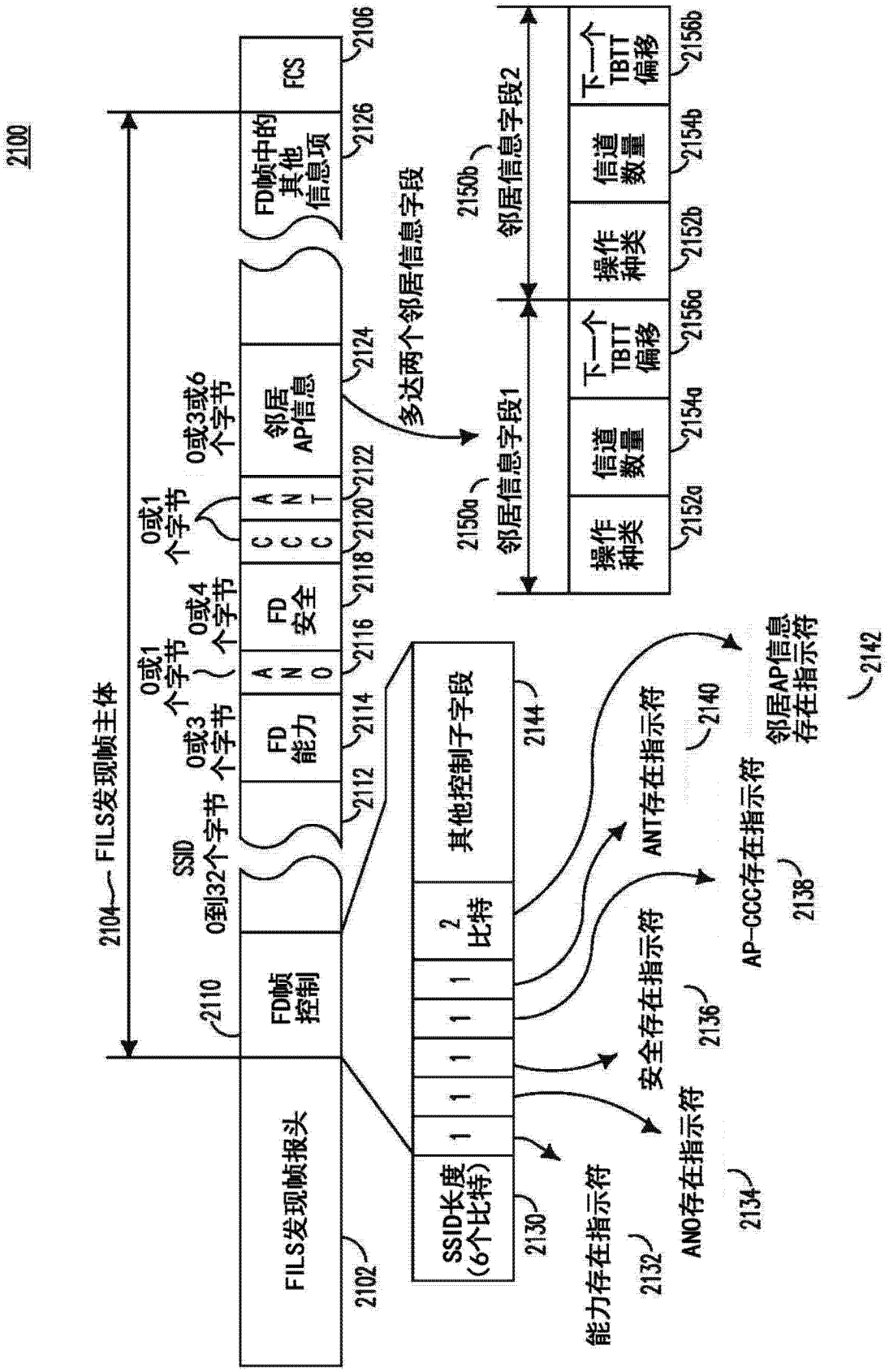

2100
2104 FILS发现帧主体
FILS发现帧报头
2102
FD帧控制
2110
SSID
0到32个字节
0或3个字节
FD能力
2112
2114
ANO
0或1个字节
0或4个字节
FD安全
2116
CCC
ANT
0或1个字节
2118
2120
0或3或6个字节
邻居AP信息
2122
2124
FD帧中的其他信息项
2126
FCS
2106
SSID长度(6个比特)
1
1
1
1
1
2比特
其他控制子字段
2144
2130
能力存在指示符
2132
ANO存在指示符
2134
安全存在指示符
2136
ANT存在指示符
2140
AP-CCC存在指示符
2138
邻居AP信息存在指示符
2142
多达两个邻居信息字段
2150a
邻居信息字段1
操作种类
2152a
信道数量
2154a
下一个TBTT偏移
2156a
2150b
邻居信息字段2
操作种类
2152b
信道数量
2154b
下一个TBTT偏移
2156b

图 21

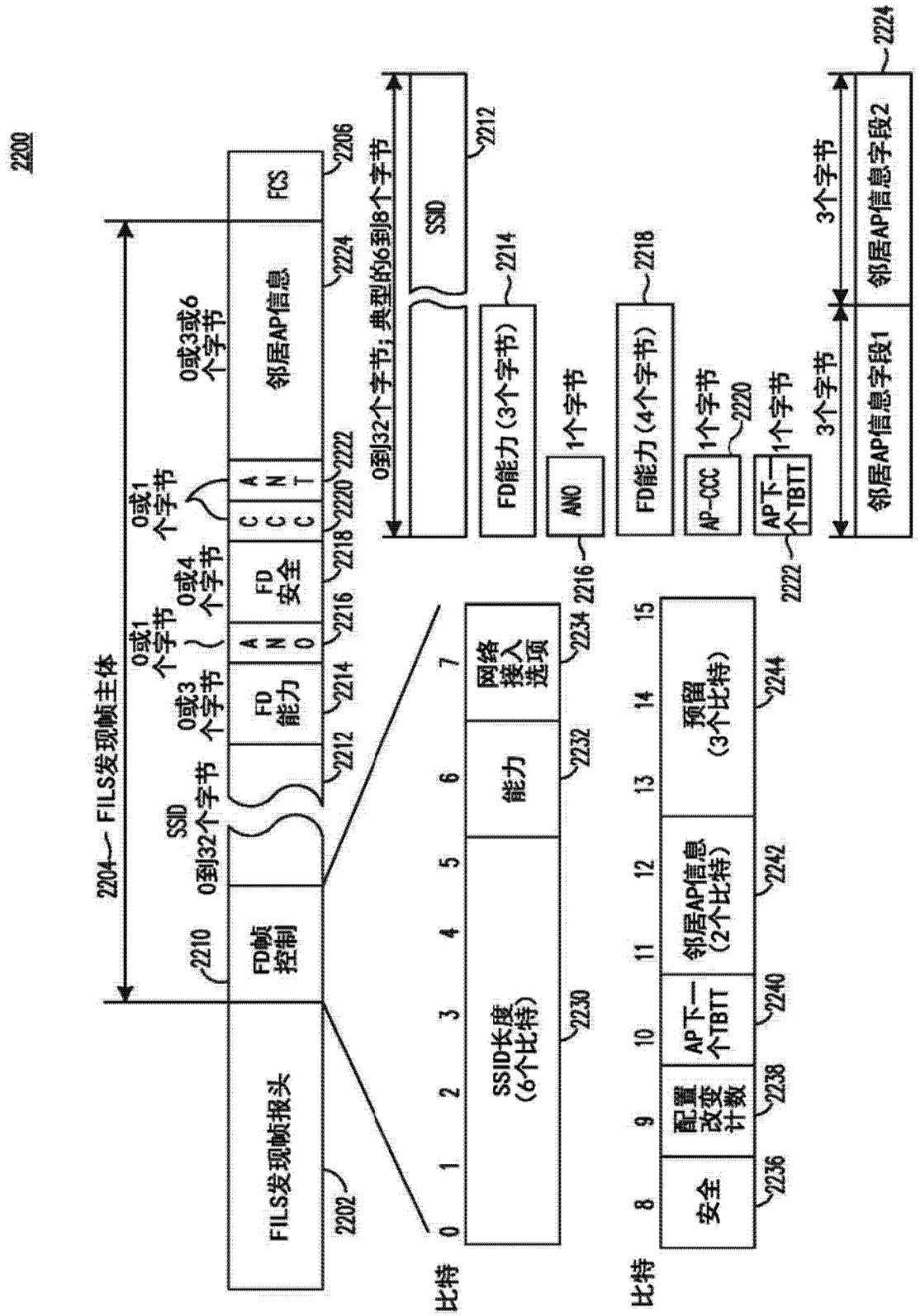

2200
2204 FILS发现帧主体
FILS发现帧报头
2202
FD帧控制
2210
SSID
0到32个字节
FD能力
2212
ANO
2214
FD安全
2216
CCC
2218
ANT
2220
邻居AP信息
2222
FCS
2206
2224
0或1个字节
0或3个字节
0或4个字节
0或1个字节
0或3或6个字节
0到32个字节；典型的6到8个字节
SSID
2212
FD能力（3个字节）
2214
ANO 1个字节
2216
FD能力（4个字节）
2218
AP-CCC 1个字节
2220
AP下一个TBTT 1个字节
2222
3个字节
邻居AP信息字段1
3个字节
邻居AP信息字段2
2224
比特
0 1 2 3 4 5 6 7
SSID长度（6个比特）
2230
能力
2232
网络接入选项
2234
比特
8 9 10 11 12 13 14 15
安全
2236
配置改变计数
2238
AP下一个TBTT
2240
邻居AP信息（2个比特）
2242
预留（3个比特）
2244

图 22

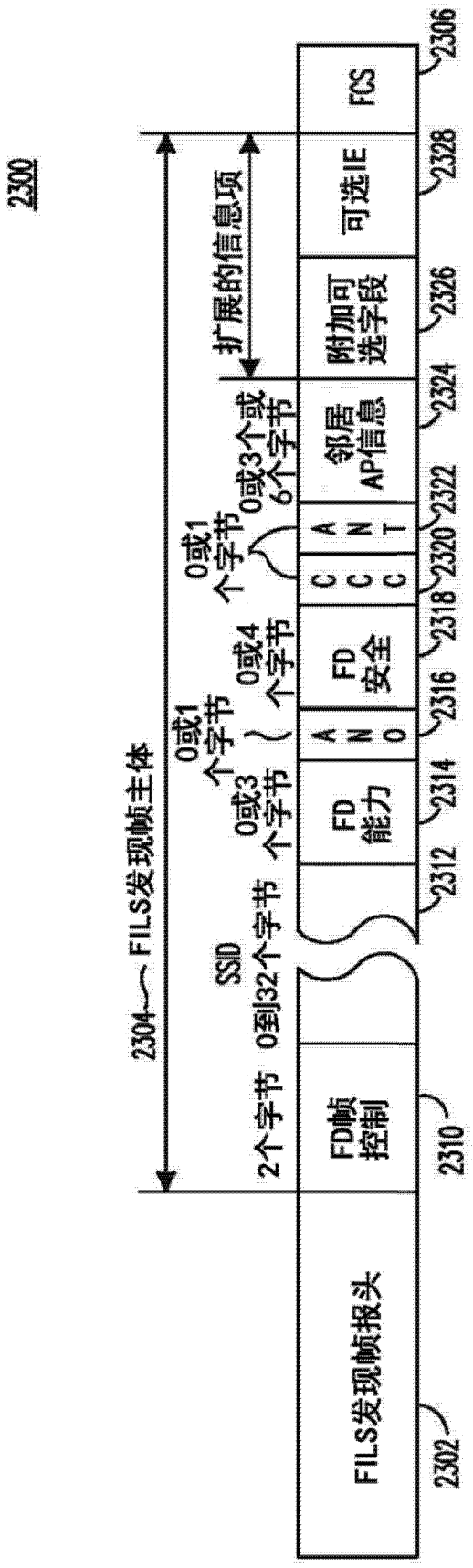

2300
2304
FILS发现帧主体
扩展的信息项
FILS发现帧报头
FD帧控制
SSID
0到32个字节
FD能力
ANO
FD安全
CCC
ANT
邻居AP信息
附加可选字段
可选IE
FCS
2302
2310
2312
2314
2316
2318
2320
2322
2324
2326
2328
2306
2个字节
0或3个字节
0或1个字节
0或4个字节
0或1个字节
0或3个字节

图 23

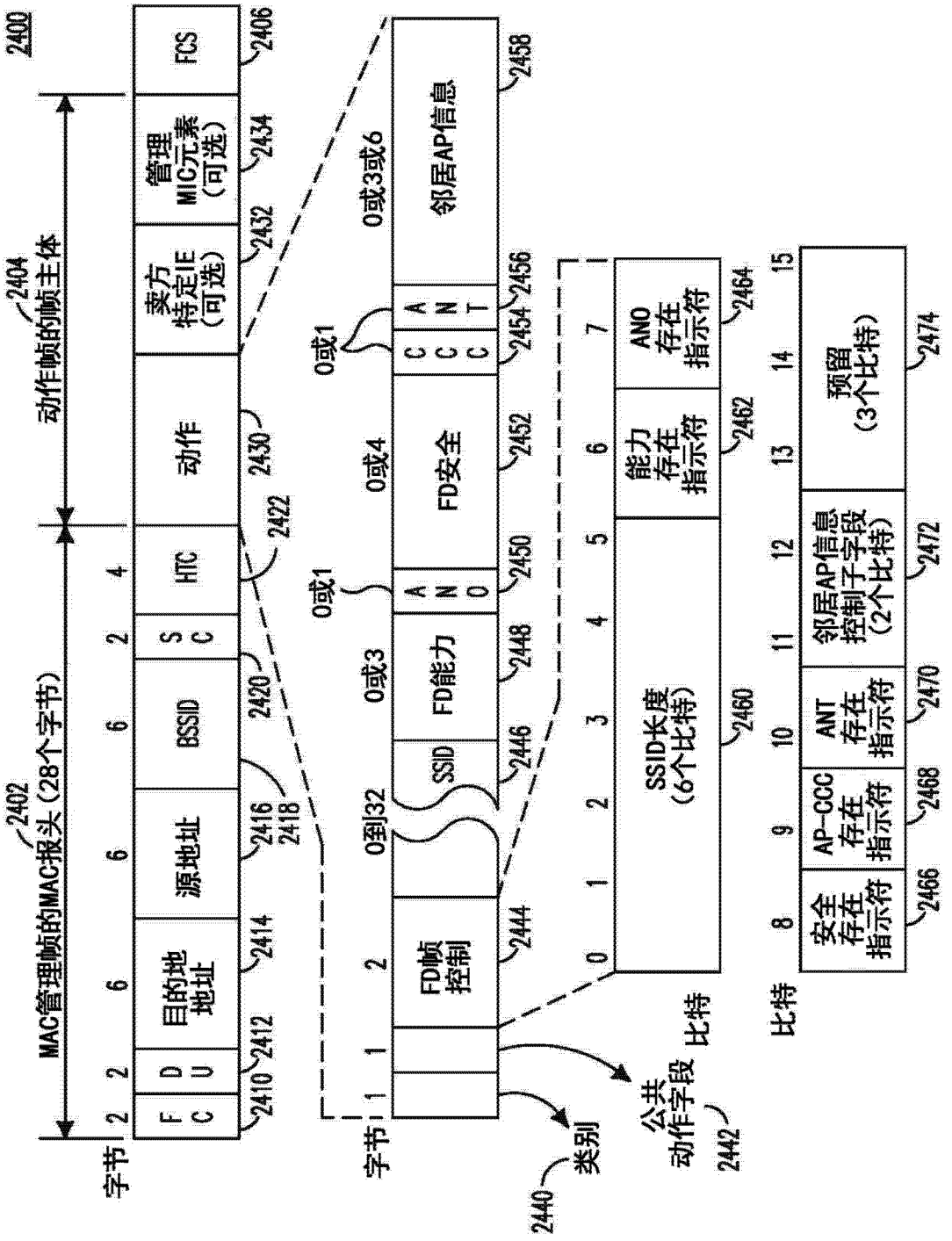

2400
2402
MAC管理帧的MAC报头（28个字节）
2404
动作帧的帧主体
FCS
DU
目的地址
源地址
BSSID
SC
HTC
动作
卖方特定IE（可选）
管理MIC元素（可选）
FCS
2406
2410
2412
2414
2416
2418
2420
2422
2430
2432
2434
字节
2
2
6
6
6
2
4
0或1
0或3
0到32
0或1
0或4
0或3或6
FD帧控制
SSID
FD能力
ANO
FD安全
CCC
ANT
邻居AP信息
2444
2446
2448
2450
2452
2454
2456
2458
1
1
2
0
1
2
3
4
5
6
7
SSID长度（6个比特）
能力存在指示符
ANO存在指示符
2460
2462
2464
比特
公共动作字段
2442
2440
类别
8
9
10
11
12
13
14
15
安全存在指示符
AP-CCC存在指示符
ANT存在指示符
邻居AP信息控制子字段（2个比特）
预留（3个比特）
2466
2468
2470
2472
2474

图 24

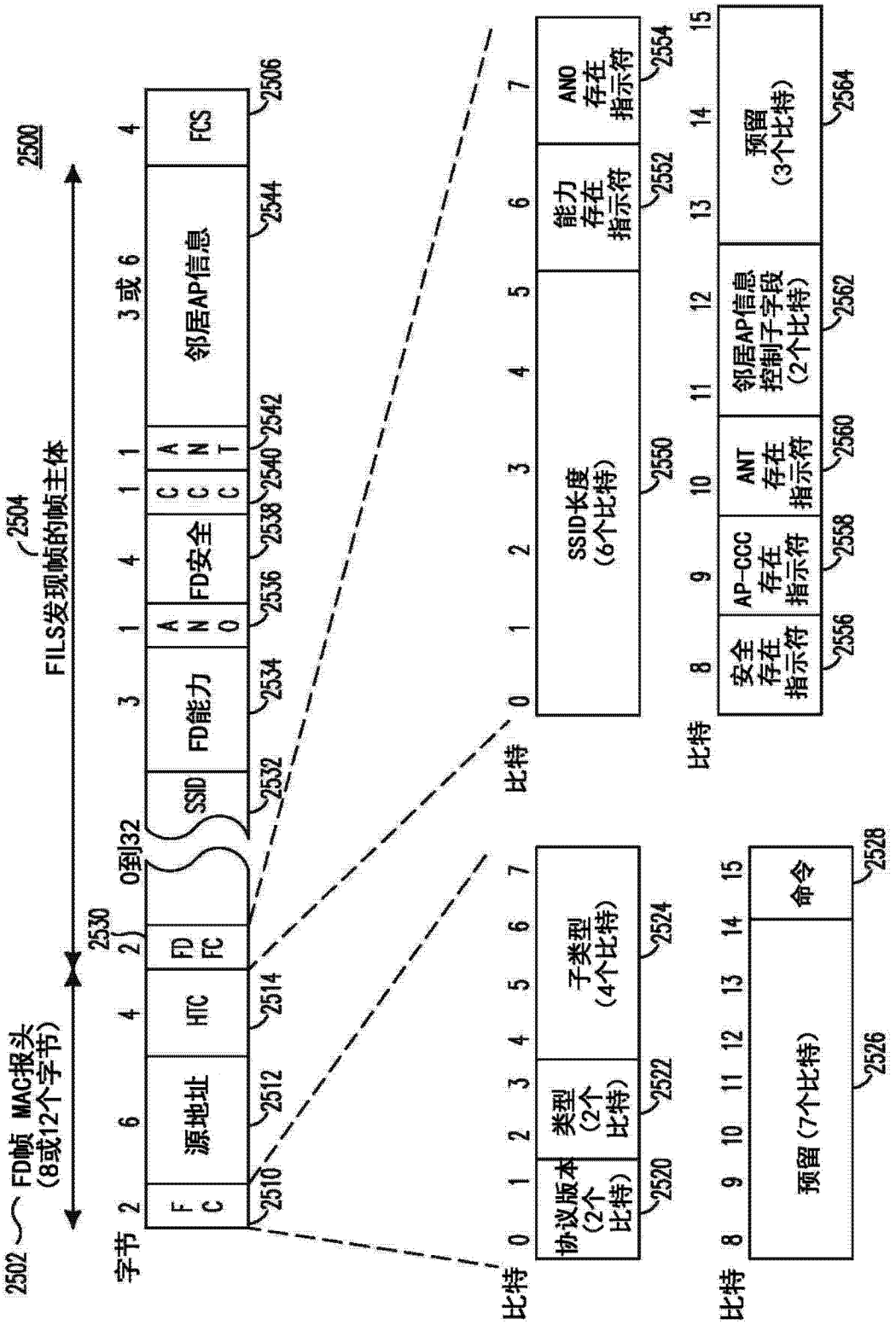

2500
FILS发现帧的帧主体
2504
FD帧 MAC报头
(8或12个字节)
2502
字节
FC
源地址
HTC
FD FC
0到32
SSID
FD能力
ANO
FD安全
CCC
ANT
3或6
邻居AP信息
FCS
2506
2510
2512
2514
2530
2532
2534
2536
2538
2540
2542
2544
比特
协议版本 (2个比特)
类型 (2个比特)
子类型 (4个比特)
2520
2522
2524
预留 (7个比特)
命令
2526
2528
SSID长度 (6个比特)
能力存在指示符
ANO存在指示符
2550
2552
2554
安全存在指示符
AP-CCC存在指示符
ANT存在指示符
邻居AP信息控制子字段 (2个比特)
预留 (3个比特)
2556
2558
2560
2562
2564

图 25

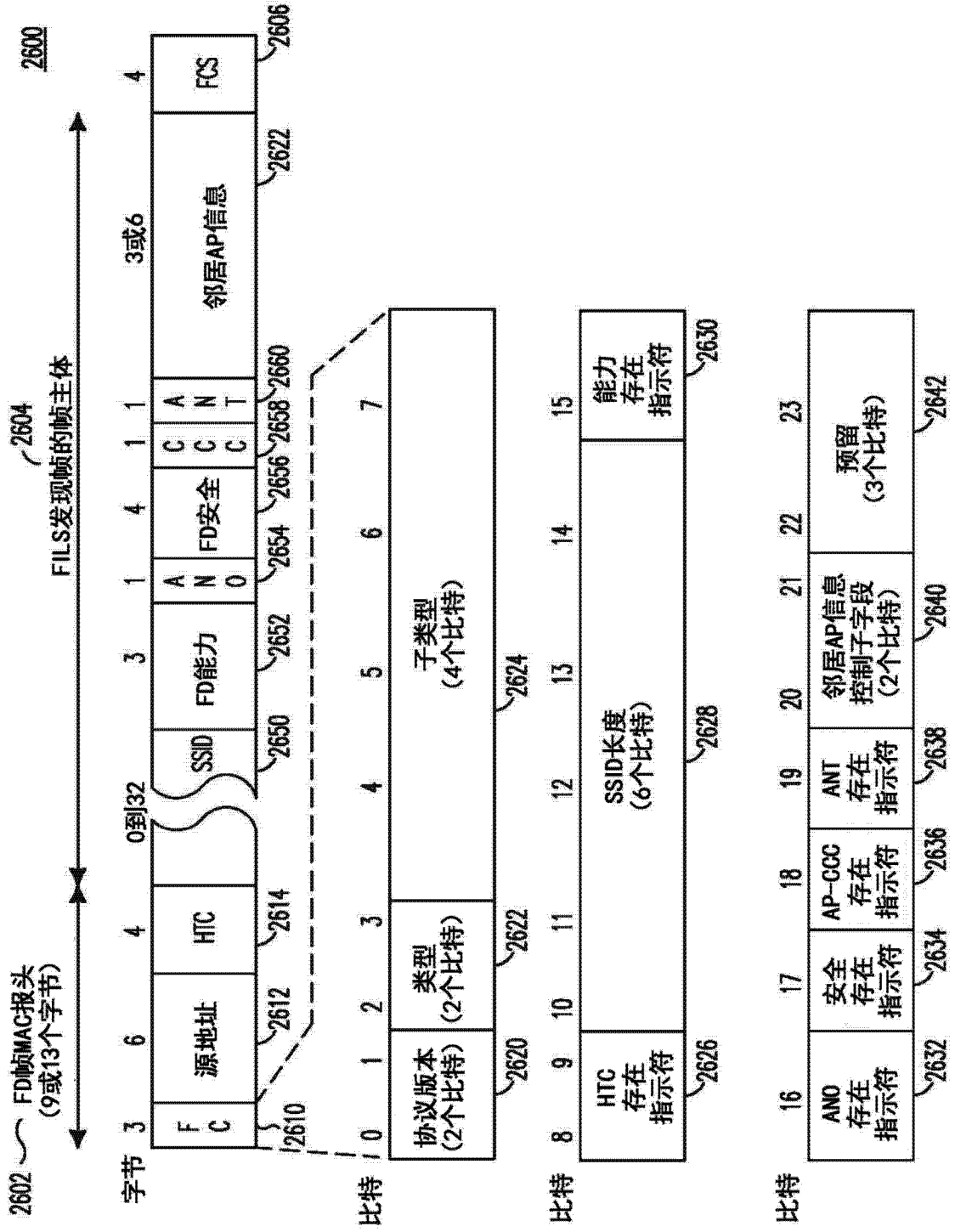

2600
2602
FD帧MAC报头
(9或13个字节)
2604
FILS发现帧的帧主体
2606
FCS
2622
邻居AP信息
3或6
0到32
SSID
FD能力
FD安全
字节
比特
FC
源地址
HTC
协议版本
(2个比特)
类型
(2个比特)
子类型
(4个比特)
SSID长度
(6个比特)
HTC
存在
指示符
能力
存在
指示符
ANO
存在
指示符
安全
存在
指示符
AP-CCC
存在
指示符
ANT
存在
指示符
邻居AP信息
控制子字段
(2个比特)
预留
(3个比特)
2610
2612
2614
2620
2622
2624
2626
2628
2630
2632
2634
2636
2638
2640
2642
2650
2652
2654
2656
2658
2660

图 26