

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2023 年 8 月 3 日 (03.08.2023)



(10) 国际公布号
WO 2023/143244 A1

(51) 国际专利分类号:
H04W 8/22 (2009.01) **H04W 48/16** (2009.01)

(21) 国际申请号: PCT/CN2023/072596

(22) 国际申请日: 2023 年 1 月 17 日 (17.01.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210114767.1 2022 年 1 月 30 日 (30.01.2022) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 徐艺珊(XU, Yishan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129

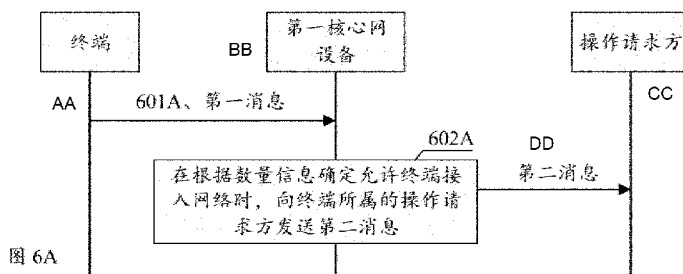
(CN)。 诸华林(ZHU, Hualin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 郭龙华(GUO, Longhua); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

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

(54) Title: TERMINAL MANAGEMENT METHOD AND CORE NETWORK DEVICE

(54) 发明名称: 终端管理方法和核心网设备



601A FIRST MESSAGE
602A WHEN DETERMINING, ACCORDING TO QUANTITY INFORMATION, TO ALLOW THE TERMINAL TO ACCESS A NETWORK, SEND A SECOND MESSAGE TO THE OPERATION REQUESTER TO WHICH THE TERMINAL BELONGS
AA TERMINAL
BB FIRST CORE NETWORK DEVICE
CC OPERATION REQUESTER
DD SECOND MESSAGE

(57) Abstract: Embodiments of the present application disclose a terminal management method and a core network device. The method comprises: a first core network device receives a first message from a terminal, the first message being used for requesting access to a network; when determining, according to quantity information, to allow the terminal to access the network, the first core network device sends a second message to an operation requester to which the terminal belongs; wherein the quantity information comprises the quantity of terminals allowed to be used by the operation requester, the second message comprises first identifier information, and the first identifier information comprises one or more of the terminal identifier of the terminal, an encrypted terminal identifier, a terminal application identifier, a terminal network identifier and an operation requester identifier. In the embodiments of the present application, the first core network device determines, according to the quantity information, to allow the terminal to access the network, and thus, the situation that the quantity of terminals accessing the network in terminals corresponding to the operation requester is greater than or equal to the quantity of terminals allowed to be used by the operation requester can be avoided.



MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE,
PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,
SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW,
MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚
(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,
HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,
PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN,
TD, TG)。

本国际公布:

一 包括国际检索报告 (条约第21条(3))。

(57) 摘要: 本申请实施例公开了一种终端管理方法和核心网设备, 该方法包括: 第一核心网设备接收来自终端的第一消息, 所述第一消息用于请求接入网络; 所述第一核心网设备在根据数量信息确定允许所述终端接入所述网络时, 向所述终端所属的操作请求方发送第二消息; 所述数量信息包括所述操作请求方允许使用的终端数量, 所述第二消息包含第一标识信息, 所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。本申请实施例中, 第一核心网设备根据数量信息确定允许终端接入网络, 可避免操作请求方对应的终端中接入网络的终端数量大于或等于操作请求方允许使用的终端数量。

终端管理方法和核心网设备

本申请要求于 2022 年 01 月 30 日提交中国专利局、申请号为 202210114767.1、申请名称为“终端管理方法和核心网设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信领域，尤其涉及一种终端管理方法和核心网设备。

背景技术

无源物联网（passive IoT, P-IoT）架构中可以包括无源终端、阅读器（reader）以及操作请求方。无源终端可以是标签形态，也可以是其他任意终端形态。下面无源终端以终端为例进行阐述。阅读器（reader）利用无线射频方式对终端（例如电子标签或射频卡）进行读写，从而达到识别目标和数据交换的目的。当操作请求方对终端进行终端操作时，可以通过核心网设备向阅读器发送操作指令，操作指令可以包括但不限于执行获取终端信息、盘点操作（或者称为盘存操作）、读操作、写操作、失效操作、与终端交互信息等操作。当阅读器接收到该操作指令后，会向终端发送该操作指令；终端根据该操作指令获取或者发送相应的信息。例如，当操作指令为盘点指令或者为执行盘点操作时，终端会发送终端的标识信息。又例如，当操作指令为读指令或者为执行读操作时，终端会发送存储在终端存储区中的数据信息。又例如，当操作指令为写指令或者执行写操作时，终端会将指令中包括的待写入终端的数据信息存储至终端的存储区中。阅读器接收终端发送的信息，并通过核心网设备向操作请求方发送该信息。

发明内容

本申请实施例公开了一种终端管理方法和核心网设备，可实现对终端的管理。

第一方面，本申请实施例提供一种终端管理方法，包括：第一核心网设备接收来自终端的第一消息，所述第一消息用于请求接入网络；所述第一核心网设备在根据数量信息确定允许所述终端接入所述网络时，向所述终端所属的操作请求方发送第二消息；所述数量信息包括所述操作请求方允许使用的终端数量，所述第二消息包含第一标识信息，所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

本申请实施例中，第一核心网设备在根据数量信息确定允许终端接入所述网络时，向该终端所属的操作请求方发送第二消息。也就是说，第一核心网设备发送第二消息之前，需要根据数量信息确定允许终端接入网络，而不是直接允许该终端接入网络。第一核心网设备根据数量信息确定允许终端接入网络，可避免操作请求方对应的终端中接入网络的终端数量大于或等于操作请求方允许使用的终端数量。

在一种可能的实现方式中，所述根据数量信息确定允许所述终端接入所述网络包括：当所述操作请求方对应的终端中接入所述网络的终端数量小于数量阈值时，所述第一核心网设

备确定允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

在该实现方式中，当操作请求方对应的终端中接入网络的终端数量小于数量阈值时，第一核心网设备确定允许终端接入网络，可快速、准确地确定是否允许终端接入，并避免操作请求方对应的终端中接入网络的终端数量大于或等于数量阈值。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备在根据所述数量信息确定不允许所述终端接入所述网络的情况下，向所述终端发送第三消息；所述第三消息指示拒绝所述终端接入所述网络。

在该实现方式中，第一核心网设备在根据数量信息确定不允许终端接入网络的情况下，向终端发送第三消息；可避免操作请求方对应的终端中接入网络的终端数量大于或等于操作请求方允许使用的终端数量。

在一种可能的实现方式中，所述根据所述数量信息确定不允许所述终端接入所述网络包括：当所述操作请求方对应的终端中接入所述网络的终端数量大于或等于数量阈值时，所述第一核心网设备确定不允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

在该实现方式中，当操作请求方对应的终端中接入网络的终端数量大于或等于数量阈值时，第一核心网设备确定不允许终端接入所述网络；可快速、准确地确定是否允许终端接入。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备向第二核心网设备发送第四消息；所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息和所述认证信息用于执行所述认证流程；所述第二标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在该实现方式中，第一核心网设备向第二核心网设备发送第四消息，以便于对终端执行认证流程，从而保证该终端为可信的终端。

在一种可能的实现方式中，所述第一核心网设备在根据数量信息确定允许所述终端接入所述网络之后，所述第一核心网设备向第二核心网设备发送第四消息；所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息和所述认证信息用于执行所述认证流程；所述第二标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在该实现方式中，第一核心网设备向第二核心网设备发送第四消息，以便于对终端执行认证流程，从而保证该终端为可信的终端。

在一种可能的实现方式中，所述第四消息还包括指示信息，所述指示信息指示所述认证流程为单向认证、双向认证、所述终端对所述网络或者所述操作请求方的单向认证、所述网络或者所述操作请求方对所述终端的单向认证中的任一种。

在该实现方式中，指示信息指示认证流程为单向认证流程或双向认证流程，以便第二核心网设备根据该指示信息确定待执行的认证流程。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备根据所述第一消息对所述终端执行认证流程；所述第一消息包括第三标识信息和认证信息，所述第三标识信息和所述认证信息用于执行所述认证流程；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在该实现方式中，第一核心网设备根据第一消息对终端执行认证流程，该第一核心网设备自身就可对该终端执行认证流程，不必与其他设备交互，可减少信令开销。

在一种可能的实现方式中，所述第一核心网设备在根据数量信息确定允许所述终端接入所述网络之后，根据所述第一消息对所述终端执行认证流程；所述第一消息包括第三标识信息和认证信息，所述第三标识信息和所述认证信息用于执行所述认证流程；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在该实现方式中，第一核心网设备根据第一消息对终端执行认证流程，该第一核心网设备自身就可对该终端执行认证流程，不必与其他设备交互，可减少信令开销。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在该实现方式中，第一核心网设备根据第一消息包括的第三标识信息，确定终端所属的操作请求方，以便根据数量信息确定是否允许终端接入网络。

在一种可能的实现方式中，所述第一核心网设备根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方包括：所述第一核心网设备根据所述第三标识信息和第一对应关系，确定所述终端所属的所述操作请求方；所述第一对应关系表示所述终端属于所述操作请求方。可选的，第一对应关系包括所述终端的应用标识（终端标识或网络标识）与操作请求方标识的对应关系，所述操作请求方标识为所述操作请求方的标识。

在该实现方式中，第一核心网设备根据第三标识信息和第一对应关系，可快速、准确地确定终端所属的操作请求方。

在一种可能的实现方式中，所述第一核心网设备根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方之前，所述方法还包括：所述第一核心网设备根据来自所述操作请求方的操作指令，确定第二对应关系；所述第二对应关系表示所述终端属于所述操作请求方；所述第一核心网设备根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方包括：所述第一核心网设备根据所述第三标识信息和所述第二对应关系，确定所述终端所属的所述操作请求方。所述操作指令可包含所述终端的第一标识，该第一标识为终端的终端标识、加密的终端标识、终端应用标识、终端网络标识中的任一项。

在该实现方式中，第一核心网设备根据来自操作请求方的操作指令，确定第二对应关系，不必预先存储各终端与其所属的操作请求方的对应关系，可以减少存储开销，并减少检索终端所属的操作请求方的工作量。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备接收第五消息；所述第一核心网设备向所述终端，发送第六消息；所述第五消息指示所述认证流程通过，所述第六消息指示接受所述终端接入所述网络；或者，所述第五消息指示所述认证流程不通过，所述第六消息指示拒绝所述终端接入所述网络。

在该实现方式中，可及时指示接受或拒绝终端接入网络。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备获取所述数量信息和/或所述第一标识信息。

在该实现方式中，第一核心网设备获取数量信息和/或第一标识信息，以便根据该数量信息确定是否允许终端接入网络，以及实现对终端的认证流程。

在一种可能的实现方式中，所述方法还包括：所述第一核心网设备统计所述操作请求方对应的终端中接入所述网络的终端数量。

在该实现方式中，第一核心网设备统计操作请求方对应的终端中接入网络的终端数量，以便根据该终端设备和数量阈值确定是否允许终端接入网络。

在一种可能的实现方式中，所述第一核心网设备统计所述操作请求方对应的终端中接入所述网络的终端数量包括：在所述终端通过认证之后，所述第一核心网设备根据所述第一标识信息和第三对应关系，更新所述操作请求方对应的终端中接入所述网络的终端数量，所述第三对应关系包括：所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项中的一个或多个的对应关系。

在该实现方式中，第一核心网设备根据第一标识信息和第二对应关系，更新操作请求方对应的终端中接入网络的终端数量；可以准确地统计操作请求方对应的终端中接入网络的终端数量，并防止多个终端使用相同的标识接入网络。

第二方面，本申请提供另一种终端管理方法，其特征在于，包括：操作请求方获取数量信息，所述数量信息指示所述操作请求方允许使用的终端数量；所述操作请求方根据所述数量信息，获取一个或多个终端应用标识。

本申请实施例中，操作请求方根据数量信息，获取一个或多个终端应用标识；可以避免该操作请求方获取的终端应用标识的数量超过该操作请求方允许使用的终端数量。

在一种可能的实现方式中，所述方法还包括：所述操作请求方发送操作指令，所述操作指令包括第一应用标识，所述第一应用标识包含于所述一个或多个终端应用标识；所述操作指令用于对所述第一应用标识对应的终端执行操作。

在该实现方式中，操作指令包括第一应用标识；通过包含第一应用标识的操作指令，可方便地对第一应用标识对应的终端执行操作。

在一种可能的实现方式中，所述方法还包括：所述操作请求方获取网络标识信息，所述网络标识信息包括一个或多个终端网络标识。

在该实现方式中，操作请求方获取网络标识信息，以便于该操作请求方利用该网络标识信息实现对终端的管理。

在一种可能的实现方式中，所述方法还包括：所述操作请求方向第一核心网设备发送所述一个或多个终端应用标识和/或所述操作请求方标识。

在该实现方式中，操作请求方向第一核心网设备发送一个或多个终端应用标识和/或操作请求方标识；以便于该第一核心网设备利用该一个或多个终端应用标识和/或操作请求方标识实现终端管理。

第三方面，本申请提供另一种终端管理方法，包括：操作请求方获取一个或多个终端应用标识；所述操作请求方发送操作指令，所述操作指令包括第一应用标识，所述第一应用标识包含于所述一个或多个终端应用标识；所述操作指令用于对所述第一应用标识对应的终端执行操作。

本申请实施例中，操作请求方获取一个或多个终端应用标识，并发送包括第一应用标识的操作指令，可以对第一应用标识对应的终端执行操作。也就是说，根据获取的一个或多个终端应用标识，可对相应的终端执行操作。

在一种可能的实现方式中，所述操作请求方获取一个或多个终端应用标识包括：所述操作请求方接收来自第一核心网设备的所述一个或多个终端应用标识。

在该实现方式中，操作请求方接收来自第一核心网设备的一个或多个终端应用标识；不需要自己分配终端应用标识。

在一种可能的实现方式中，所述方法还包括：所述操作请求方获取数量信息，所述数量

信息指示所述操作请求方允许使用的终端数量。

在该实现方式中，操作请求方获取数量信息，可以获知其允许使用的终端数量。

第四方面，本申请提供另一种终端管理方法，包括：第二核心网设备获取数量信息，所述数量信息指示操作请求方允许使用的终端数量；所述第二核心网设备向第一核心网设备发送所述数量信息和/或第一标识信息；所述第一标识信息包括终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项；所述操作请求方标识为所述操作请求方的标识，所述终端属于所述操作请求方。

本申请实施例中，第二核心网设备向第一核心网设备发送数量信息和/或第一标识信息，以便该第一核心网设备根据该数量信息确定是否允许终端接入网络。

在一种可能的实现方式中，所述方法还包括：所述第二核心网设备配置所述操作请求方允许使用的终端数量。

在该实现方式中，第二核心网设备配置操作请求方允许使用的终端数量，以便利用该终端数量执行终端管理。

在一种可能的实现方式中，在第二核心网设备获取数量信息之后，所述方法还包括：所述第二核心网设备根据所述数量信息，获取（例如分配）所述终端的终端网络标识。

在该实现方式中，第二核心网设备根据所述数量信息，获取终端的终端网络标识，以便后续根据该终端网络标识对该终端执行终端管理。

在一种可能的实现方式中，第二核心网设备根据所述数量信息，获取（例如分配）所述终端的终端网络标识之后，所述方法还包括：所述第二核心网设备向所述操作请求方发送所述终端的终端网络标识。

在该实现方式中，第二核心网设备向操作请求方发送终端网络标识，以便该操作请求方利用该终端网络标识对相应的终端执行终端管理。

在一种可能的实现方式中，所述方法还包括：所述第二核心网设备接收来自操作请求方的一个或多个终端应用标识；所述一个或多个终端应用标识包括所述终端的终端应用标识。

在该实现方式中，第二核心网设备接收来自操作请求方的一个或多个终端应用标识，以便后续利用这些终端应用标识对相应的终端进行终端管理。

在一种可能的实现方式中，所述第二核心网设备接收来自操作请求方的一个或多个终端应用标识之后，所述方法还包括：所述第二核心网设备配置所述一个或多个终端应用标识。

在该实现方式中，第二核心网设备配置一个或多个终端应用标识，以便后续利用这些终端应用标识对相应的终端进行终端管理。

在一种可能的实现方式中，所述方法还包括：所述第二核心网设备获取第七消息；所述第七消息包括所述数量信息和第四标识信息；所述第四标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。所述第二核心网设备获取第七消息可以是接收来自其他设备（例如属于运营商的设备）发送的第七消息。

在该实现方式中，第二核心网设备获取第七消息，以便利用该第七消息得到第一标识信息。

在一种可能的实现方式中，所述方法还包括：所述第二核心网设备向所述操作请求方发送所述终端的应用标识和/或所述数量信息。

在该实现方式中，可以使得操作请求方获得终端的应用标识和/或数量信息。

在一种可能的实现方式中，所述方法还包括：所述第二核心网设备接收来自所述第一核

心网设备的第四消息，所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息包括终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项；所述第二核心网设备根据所述第四消息对所述终端执行认证流程。

本申请实施例中，第二核心网设备根据第四消息对终端执行认证流程，可以快速认证终端。

在一种可能的实现方式中，所述第四消息还包括指示信息，所述指示信息指示所述认证流程为单向认证、双向认证、所述终端对所述网络或者所述操作请求方的单向认证、所述网络或者所述操作请求方对所述终端的单向认证中的任一种；所述方法还包括：所述第二核心网设备根据所述指示信息确定所述认证流程的类型。

在该实现方式中，第二核心网设备根据指示信息确定认证流程的类型；以便对终端执行相应的认证流程。

在一种可能的实现方式中，所述第二标识信息包括操作请求方标识且未包括所述终端的终端标识、加密的终端标识、终端应用标识以及终端网络标识；所述第二核心网设备根据所述第四消息对所述终端执行认证流程之后，所述方法还包括：在所述终端通过认证的情况下，为所述终端分配终端网络标识。

在该实现方式中，在终端通过认证的情况下，为终端分配终端网络标识。这样终端的网络标识可以无需提前配置于操作请求方中，可以防止操作请求方将一个终端的网络标识用于多个终端中，即终端获取终端网络标识可以流程化，更安全。

在一种可能的实现方式中，所述方法还包括：所述第二核心网设备统计所述操作请求方对应的终端中接入所述网络的终端数量。

在该实现方式中，第二核心网设备统计操作请求方对应的终端中接入网络的终端数量，以便根据该终端设备和数量阈值确定是否允许终端接入网络。

在一种可能的实现方式中，所述第二核心网设备统计所述操作请求方对应的终端中接入所述网络的终端数量包括：在所述终端通过认证之后，所述第二核心网设备根据所述第一标识信息和第三对应关系，更新所述操作请求方对应的终端中接入所述网络的终端数量，所述第三对应关系包括：所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项中的一个或多个的对应关系。

在该实现方式中，第二核心网设备根据第一标识信息和第三对应关系，更新操作请求方对应的终端中接入网络的终端数量；可以准确地统计操作请求方对应的终端中接入网络的终端数量，并防止多个终端使用相同的标识接入网络。

在一种可能的实现方式中，所述第二核心网设备统计所述操作请求方对应的终端中接入所述网络的终端数量之后，所述方法还包括：所述第二核心网设备通知所述第一核心网设备所述操作请求方对应的终端中接入所述网络的终端数量。

在该实现方式中，可使得第一核心网设备获知操作请求方对应的终端中接入网络的终端数量。

在一种可能的实现方式中，所述终端为标签；所述方法还包括：所述第二核心网设备更新或者删除失效标签的标识信息，所述失效标签的标识信息包括以下信息中的一项或多项：所述失效标签的终端应用标识、终端网络标识、终端标识、加密的终端标识、第三对应关系，所述第三对应关系包含所述失效标签的终端应用标识、终端网络标识、终端标识、加密的终端标识中的两个或两个以上的对应关系。

在该实现方式中，第二核心网设备更新或者删除失效标签的标识信息，以便更好地管理标签。

在一种可能的实现方式中，所述方法还包括：接收来自所述操作请求方的标签消息；所述第二核心网设备更新或者删除失效标签的标识信息包括：所述第二核心网设备根据所述标签信息，更新或者删除失效标签的标识信息。

在该实现方式中，可按照操作请求方的指示更新或者删除失效标签的标识信息。

第五方面，本申请实施例提供一种通信装置，该通信装置具有实现上述第一方面方法实施例中的行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。在一种可能的实现方式中，包括收发模块和处理模块，其中：所述收发模块，用于接收来自终端的第一消息，所述第一消息用于请求接入网络；所述收发模块，还用于在所述处理模块根据数量信息确定允许所述终端接入所述网络时，向所述终端所属的操作请求方发送第二消息；所述数量信息包括所述操作请求方允许使用的终端数量，所述第二消息包含第一标识信息，所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在一种可能的实现方式中，所述处理模块，具体用于当所述操作请求方对应的终端中接入所述网络的终端数量小于数量阈值时，确定允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

在一种可能的实现方式中，所述收发模块，还用于在所述处理模块根据所述数量信息确定不允许所述终端接入所述网络的情况下，向所述终端发送第三消息；所述第三消息指示拒绝所述终端接入所述网络。

在一种可能的实现方式中，所述处理模块，具体用于当所述操作请求方对应的终端中接入所述网络的终端数量大于或等于数量阈值时，确定不允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

在一种可能的实现方式中，所述收发模块，还用于向第二核心网设备发送第四消息；所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息和所述认证信息用于执行所述认证流程；所述第二标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在一种可能的实现方式中，所述第四消息还包括指示信息，所述指示信息指示所述认证流程为单向认证、双向认证、所述终端对所述网络或者所述操作请求方的单向认证、所述网络或者所述操作请求方对所述终端的单向认证中的任一种。

在一种可能的实现方式中，所述处理模块，还用于根据所述第一消息对所述终端执行认证流程；所述第一消息包括第三标识信息和认证信息，所述第三标识信息和所述认证信息用于执行所述认证流程；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在一种可能的实现方式中，所述处理模块，还用于根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在一种可能的实现方式中，所述处理模块，具体用于根据所述第三标识信息和第一对应关系，确定所述终端所属的所述操作请求方；所述第一对应关系表示所述终端属于所述操作

请求方。可选的，第一对应关系包括所述终端的应用标识（终端标识或网络标识）与操作请求方标识的对应关系，所述操作请求方标识为所述操作请求方的标识。

在一种可能的实现方式中，所述处理模块，具体用于根据来自所述操作请求方的操作指令，确定第二对应关系；所述第二对应关系表示所述终端属于所述操作请求方；根据所述第三标识信息和所述第二对应关系，确定所述终端所属的所述操作请求方。所述操作指令可包含所述终端的第一标识，该第一标识为终端的终端标识、加密的终端标识、终端应用标识、终端网络标识中的任一项。

在一种可能的实现方式中，所述收发模块，还用于接收第五消息；向所述终端，发送第六消息；所述第五消息指示所述认证流程通过，所述第六消息指示接受所述终端接入所述网络；或者，所述第五消息指示所述认证流程不通过，所述第六消息指示拒绝所述终端接入所述网络。

在一种可能的实现方式中，所述处理模块，还用于获取所述数量信息和/或所述第一标识信息。

在一种可能的实现方式中，所述处理模块，还用于统计所述操作请求方对应的终端中接入所述网络的终端数量。

在一种可能的实现方式中，所述处理模块，具体用于在所述终端通过认证之后，根据所述第一标识信息和第三对应关系，更新所述操作请求方对应的终端中接入所述网络的终端数量，所述第三对应关系包括：所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项中的一个或多个的对应关系。

关于第五方面的各种可能的实施方式所带来的技术效果，可参考对于第一方面或第一方面的各种可能的实施方式的技术效果的介绍。

第六方面，本申请实施例提供一种通信装置，该通信装置具有实现上述第一方面方法实施例中的行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。在一种可能的实现方式中，包括收发模块和处理模块，其中：所述收发模块，用于获取数量信息，所述数量信息指示所述操作请求方允许使用的终端数量；所述处理模块，用于根据所述数量信息，获取一个或多个终端应用标识。

在一种可能的实现方式中，所述收发模块，还用于发送操作指令，所述操作指令包括第一应用标识，所述第一应用标识包含于所述一个或多个终端应用标识；所述操作指令用于对所述第一应用标识对应的终端执行操作。

在一种可能的实现方式中，所述收发模块，还用于获取网络标识信息，所述网络标识信息包括一个或多个终端网络标识。

在一种可能的实现方式中，所述收发模块，还用于向第一核心网设备发送所述一个或多个终端应用标识和/或所述操作请求方标识。

关于第六方面的各种可能的实施方式所带来的技术效果，可参考对于第二方面或第二方面的各种可能的实施方式的技术效果的介绍。

第七方面，本申请实施例提供一种通信装置，该通信装置具有实现上述第三方面方法实施例中的行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。在一种可能的实现方式中，包括收发模块，其中：所述收发模块，用于获取一个或多个终端应用标识；发送操作指令，所述操作指令包括第一应用标识，所述第一应用标识包含于所述一个或多个终端应用标识；

所述操作指令用于对所述第一应用标识对应的终端执行操作。

在一种可能的实现方式中，所述收发模块，具体用于接收来自第一核心网设备的所述一个或多个终端应用标识。

在一种可能的实现方式中，所述收发模块，还用于获取数量信息，所述数量信息指示所述操作请求方允许使用的终端数量。

关于第七方面的各种可能的实施方式所带来的技术效果，可参考对于第三方面或第三方面的各种可能的实施方式的技术效果的介绍。

第八方面，本申请实施例提供一种通信装置，该通信装置具有实现上述第四方面方法实施例中的行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。在一种可能的实现方式中，包括收发模块，其中：所述收发模块，用于获取数量信息，所述数量信息指示操作请求方允许使用的终端数量；向第一核心网设备发送所述数量信息和/或第一标识信息；所述第一标识信息包括终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项；所述操作请求方标识为所述操作请求方的标识，所述终端属于所述操作请求方。

在一种可能的实现方式中，所述通信装置还包括：处理模块，用于配置所述操作请求方允许使用的终端数量。

在一种可能的实现方式中，所述处理模块，具体用于根据所述数量信息，获取（例如分配）所述终端的终端网络标识。

在一种可能的实现方式中，所述收发模块，还用于向所述操作请求方发送所述终端的终端网络标识。

在一种可能的实现方式中，所述收发模块，还用于接收来自操作请求方的一个或多个终端应用标识；所述一个或多个终端应用标识包括所述终端的终端应用标识。

在一种可能的实现方式中，所述处理模块，还用于配置所述一个或多个终端应用标识。

在一种可能的实现方式中，所述收发模块，还用于获取第七消息；所述第七消息包括所述数量信息和第四标识信息；所述第四标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在一种可能的实现方式中，所述收发模块，还用于向所述操作请求方发送所述终端的应用标识和/或所述数量信息。

在一种可能的实现方式中，所述收发模块，还用于接收来自所述第一核心网设备的第四消息，所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息包括终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项；所述处理模块，还用于根据所述第四消息对所述终端执行认证流程。

在一种可能的实现方式中，所述第四消息还包括指示信息，所述指示信息指示所述认证流程为单向认证、双向认证、所述终端对所述网络或者所述操作请求方的单向认证、所述网络或者所述操作请求方对所述终端的单向认证中的任一种；所述处理模块，具体用于根据所述指示信息确定所述认证流程的类型。

在一种可能的实现方式中，所述第二标识信息包括操作请求方标识且未包括所述终端的终端标识、加密的终端标识、终端应用标识以及终端网络标识；所述处理模块，还用于在所述终端通过认证的情况下，为所述终端分配终端网络标识。

在一种可能的实现方式中，所述处理模块，还用于统计所述操作请求方对应的终端中接入所述网络的终端数量。

在一种可能的实现方式中，所述处理模块，具体用于在所述终端通过认证之后，所述第二核心网设备根据所述第一标识信息和第三对应关系，更新所述操作请求方对应的终端中接入所述网络的终端数量，所述第三对应关系包括：所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项中的一个或多个的对应关系。

在一种可能的实现方式中，所述收发模块，还用于通知所述第一核心网设备所述操作请求方对应的终端中接入所述网络的终端数量。例如，收发模块向第一核心网设备发送一个通知消息，该通知消息包括操作请求方对应的终端中接入网络的终端数量。

在一种可能的实现方式中，所述终端为标签；所述处理模块，还用于更新或者删除失效标签的标识信息，所述失效标签的标识信息包括以下信息中的一项或多项：所述失效标签的终端应用标识、终端网络标识、终端标识、加密的终端标识、第三对应关系，所述第三对应关系包含所述失效标签的终端应用标识、终端网络标识、终端标识、加密的终端标识中的两个或两个以上的对应关系。

在一种可能的实现方式中，所述收发模块，还用于接收来自所述操作请求方的标签消息；所述第二核心网设备更新或者删除失效标签的标识信息包括：所述第二核心网设备根据所述标签信息，更新或者删除失效标签的标识信息。

关于第八方面的各种可能的实施方式所带来的技术效果，可参考对于第四方面或第四方面的各种可能的实施方式的技术效果的介绍。

第九方面，本申请提供一种通信装置，该通信装置包括处理器，该处理器可以用于执行存储器所存储的计算机执行指令，以使上述第一方面或第一方面的任意可能的实现方式所示的方法被执行，或者以使上述第二方面或第二方面的任意可能的实现方式所示的方法被执行，或者以使上述第三方面或第三方面的任意可能的实现方式所示的方法被执行，或者以使上述第四方面或第四方面的任意可能的实现方式所示的方法被执行。

本申请实施例中，在执行上述方法的过程中，上述方法中有关发送信息的过程，可以理解为基于处理器的指令进行输出信息的过程。在输出信息时，处理器将信息输出给收发器，以便由收发器进行发射。该信息在由处理器输出之后，还可能需要进行其他的处理，然后到达收发器。类似的，处理器接收输入的信息时，收发器接收该信息，并将其输入处理器。更进一步的，在收发器收到该信息之后，该信息可能需要进行其他的处理，然后才输入处理器。

对于处理器所涉及的发送和/或接收等操作，如果没有特殊说明，或者，如果未与其在相关描述中的实际作用或者内在逻辑相抵触，则可以一般性的理解为基于处理器的指令输出。

在实现过程中，上述处理器可以是专门用于执行这些方法的处理器，也可以是执行存储器中的计算机指令来执行这些方法的处理器，例如通用处理器等。例如，处理器还可以用于执行存储器中存储的程序，当该程序被执行时，使得该通信装置执行如上述第一方面或第一方面的任意可能的实现方式所示的方法。在一种可能的实现方式中，存储器位于上述通信装置之外。在一种可能的实现方式中，存储器位于上述通信装置之内。

本申请实施例中，处理器和存储器还可能集成于一个器件中，即处理器和存储器还可能被集成于一起。

在一种可能的实现方式中，通信装置还包括收发器，该收发器，用于接收报文或发送报文等。

第十方面，本申请提供一种数据处理装置，该数据处理装置包括处理电路和接口电路，

该接口电路用于获取数据或输出数据；处理电路用于执行如上述第一方面或第一方面的任意可能的实现方式所示的相应的方法，或者处理电路用于执行如上述第二方面或第二方面的任意可能的实现方式所示的相应的方法，或者处理电路用于执行如上述第三方面或第三方面的任意可能的实现方式所示的相应的方法，或者处理电路用于执行如上述第四方面或第四方面的任意可能的实现方式所示的相应的方法。

第十一方面，本申请提供一种计算机可读存储介质，该计算机可读存储介质用于存储计算机程序，当其在计算机上运行时，使得上述第一方面或第一方面的任意可能的实现方式所示的方法被执行，或者使得上述第二方面或第二方面的任意可能的实现方式所示的方法被执行，或者使得上述第三方面或第三方面的任意可能的实现方式所示的方法被执行，或者使得上述第四方面或第四方面的任意可能的实现方式所示的方法被执行。

第十二方面，本申请提供一种计算机程序产品，该计算机程序产品包括计算机程序或计算机代码，当其在计算机上运行时，使得上述第一方面或第一方面的任意可能的实现方式所示的方法被执行，或者使得上述第二方面或第二方面的任意可能的实现方式所示的方法被执行，或者使得上述第三方面或第三方面的任意可能的实现方式所示的方法被执行，或者使得上述第四方面或第四方面的任意可能的实现方式所示的方法被执行。

第十三方面，本申请提供一种通信系统，包括上述第五方面或第五方面的任意可能的实现方式的所述第一核心网设备、上述第六方面或第七方面所述的操作请求方以及上述第八方面或第八方面的任意可能的实现方式所述第二核心网设备中的一个或多个。

附图说明

为了更清楚地说明本申请实施例或背景技术中的技术方案，下面将对本申请实施例或背景技术中所需要使用的附图进行说明。

图 1 为一种无源物联网业务流的示意图；

图 2A、图 2B、图 2C 示出了 3GPP 网络支持 P-IoT 的三种架构示意图；

图 3 为本申请实施例提供的一种 UE 的注册流程的示例；

图 4 示出了本申请实施例提供的几种分配终端的应用标识的方式的示例；

图 5 为本申请实施例提供的一种终端管理方法流程图；

图 6A 为本申请实施例提供的另一种终端管理方法流程图；

图 6B 为本申请实施例提供的另一种终端管理方法流程图；

图 7 为本申请实施例提供的另一种终端管理方法流程图；

图 8 为本申请实施例提供的另一种终端管理方法流程图；

图 9 为本申请实施例提供的另一种终端管理方法流程图；

图 10 为本申请实施例提供的另一种终端管理方法流程图；

图 11 为本申请实施例提供的另一种终端管理方法流程图；

图 12 示出了一种通信装置 1200 的结构示意图；

图 13 为本申请实施例提供的另一种通信装置 130 的结构示意图；

图 14 为本申请实施例提供的另一种通信装置 140 的结构示意图。

具体实施方式

本申请的说明书、权利要求书及附图中的术语“第一”和“第二”等仅用于区别不同对象，

而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们的任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备等，没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元等，或可选地还包括对于这些过程、方法、产品或设备等固有的其它步骤或单元。

在本文中提及的“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员可以显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

本申请以下实施例中所使用的术语只是为了描述特定实施例的目的，而并非旨在作为对本申请的限制。如在本申请的说明书和所附权利要求书中所使用的那样，单数表达形式“一个”、“一种”、“所述”、“上述”、“该”和“这一”旨在也包括复数表达形式，除非其上下文中明确地有相反指示。还应当理解，本申请中使用的术语“和/或”是指并包含一个或多个所列项目的任何或所有可能组合。例如，“A 和/或 B”可以表示：只存在 A，只存在 B 以及同时存在 A 和 B 三种情况，其中 A，B 可以是单数或者复数。本申请中使用的术语“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a、b 和 c 中的至少一项(个)，可以表示：a，或，b，或，c，或，a 和 b，或，a 和 c，或，b 和 c，或，a、b 和 c。其中 a、b 和 c 分别可以是单个，也可以是多个。

下面首先介绍本申请实施例中所涉及的术语和技术特征。

无源物联网 (P-IoT)

无源物联网中的部分网络节点可以是无源的，它们可以通过太阳能、射频、风能、水能或者潮汐能等方式获取能量，获取能量的方式不做限制。这些节点自身不配备或者不依赖电池等电源设备，而是从环境中获取能量，支撑数据的感知、传输和分布式计算。这些节点还可以将获取的能量进行存储。无源物联网架构中可以包括无源终端、阅读器 (reader) 以及操作请求方。无源终端可以是标签形态 (例如电子标签)，也可以是其他任意终端形态，本申请不做限制。阅读器 (reader) 可利用无线射频方式对电子标签或射频卡 (Tag) 进行读写，从而达到识别目标和数据交换的目的。它的工作方式有两种情况：一种就是当标签进入阅读器有效识别范围内时，接收阅读器发出的射频信号，凭借感应电流所获得的能量发出存储在芯片中的信息 (对应于无源标签)；另一种就是标签 (这种可以称为半无源或者半有源标签) 可以通过太阳能等方式存储部分电能，使得可以主动发送某一频率的信号或者利用存储的电能进行通信、数据读取或者数据写入等操作，阅读器接收信息并解码后，送至中央信息系统进行有关数据处理。本申请中，标签可以是指电子标签，也可以是指无源或半无源物联网标签 (例如用于嵌入或贴在物品上的非电子标签)。本申请中，终端的一种示例为标签。本申请中，阅读器可以是接入网设备，接入网设备包括基站、杆站、微型基站、无线接入网设备、无线接入网节点、接入回传一体化节点等，本申请不做限制。本申请中，操作请求方可以是服务器 (server)、无源物联网服务器 (P-IoT server)、应用功能 (application function, AF)、无源物联网应用功能 (P-IoT AF) 或者其他发送操作指令的设备。

无源物联网也可以称为环境能量获取物联网 (ambient IoT 或者 ambient power-enabled IoT, A-IoT)。其中，无源物联网或者环境能量获取物联网中的物联终端可以包括无源终端、半无源终端、半有源终端或者有源终端。一种可能的实现方式中，无源终端、半无源终端或者半有源终端可以通过反射载波的通信方式进行通信。例如接收阅读器发出的射频信号，凭借感

应电流所获得的能量发出存储在芯片中的信息。可选的，半无源终端或半有源终端可以具备电容，存储从环境中获取的能量（例如太阳能、无线射频能量等，对获取能量的方式不做限定）。该能量可以用于计算、通信、数据读取、数据存储等。另一种可能的实现方式中，半有源终端或者有源终端可以主动生成载波进行通信。例如可以通过太阳能等方式存储部分电能，使得可以主动发送某一频率的信号或者利用存储的电进行通信、数据读取或者数据写入等操作。

该技术广泛应用于各行业领域，下面简单列举了两个应用场景。

仓库/运输/物资：给货品嵌入或贴上无源或半无源标签。存放在仓库、商场等地方的货品在物流过程中，货品相关信息通过物联网标签被阅读器自动采集。管理人员就可以在系统迅速查询货品信息，降低货品被丢弃或者被盗的风险，可以提高货品交接速度，提高准确率，并且防止窜货和防伪。

固定资产管理：像图书馆、艺术馆及博物馆等资产庞大或者物品贵重的一些场所，就需要有完整的管理程序或者严谨的保护措施。当书籍或者贵重物品的存放信息有异常变动，就会及时提醒管理员，从而处理相关情况。

图 1 为一种无源物联网业务流的示意图。图 1 示出了如下操作：1、操作请求方通过 AMF 向接入网设备发送操作指令。2、终端执行操作。接入网设备接收到来自移动管理设备的操作指令后，向终端发送该操作指令。终端根据操作指令获取或者发送相应的信息，即根据该操作指令执行相应的操作。3、终端接入核心网。4、终端通过核心网设备（例如图 1 所示的 AMF）向操作请求方发送操作结果。操作结果为终端根据操作指令执行相应的操作得到。

如图 1 所示，当操作请求方请求对终端进行操作时，可以通过核心网设备（例如可以是接入与移动管理功能（access and mobility management function, AMF）设备）、接入网设备向终端发送操作指令，操作指令可以包括但不限于执行获取标签信息、盘点操作（或者称为盘存操作）、读操作、写操作、失效操作、与标签交互信息操作。AMF 设备为移动管理设备的一个示例。操作指令可以包括区域位置信息、终端的标识信息等。当接入网设备接收到该操作指令后，会向终端发送该操作指令。终端根据该操作指令获取或者发送相应的信息。例如，当操作指令为盘点指令或者为执行盘点操作的指令时，终端会发送其标识信息。又例如，当操作指令为读指令或者为执行读操作的指令时，终端会发送存储在其存储区中的数据信息。又例如，当操作指令为写指令或者为执行写操作的指令时，终端会将该操作指令中包括的待写入终端的数据信息存储至终端的存储区中。接入网设备接收终端发送的信息，并通过核心网设备向操作请求方发送该信息。操作请求方向接入网设备发送指令的方式可以通过控制面通道发送，例如操作请求方通过控制面设备向接入网设备发送指令。控制面设备可以包括移动管理设备、网络开放功能设备、会话管理设备、策略控制设备、统一数据管理设备、统一数据存储库、物联管理设备（例如可称为标签管理功能（tagmanagementfunction, TMF）网元、无源物联管理功能（passiveIoTmanagementfunction, PIMF）网元、环境能量获取物联管理功能（ambient IoT managementfunction, AIMF）网元、具备物联终端管理或者具备处理物联业务功能的设备）等，本申请对控制面设备的名称不做限定。图 1 以控制面设备为移动管理设备为例。如图 1 所示：操作请求方向 AMF 发送指令；此时，操作请求方可以理解为应用功能（application function, AF）、服务器或者无源物联网应用功能（P-IoT AF）、无源物联服务器。一种可能的实现方式中，P-IoTAF 向 AMF 发送指令。另一种可能的实现方式中，P-IoTAF 通过控制面设备向 AMF 发送指令。该控制面设备可以是网络开放功能设备（network exposure function, NEF）、会话管理设备（session management function, SMF）、策略控制设备（policy

control function, PCF)、统一数据管理设备 (unified data management, UDM)、统一数据存储库 (unified data repository, UDR)。此外, 操作请求方还可以通过用户面通道向接入网设备发送指令。一种可能的实现方式中, 操作请求方通过用户面设备 (user plane function, UPF) 向阅读器发送指令。另一种可能的实现方式, 操作请求方通过用户面设备和其他接入网设备, 例如无线接入网设备 (radio access network, RAN) 向阅读器发送指令; 此时, 阅读器可以是杆站、接入回传一体化 (integrated access and backhaul, IAB) 节点、终端设备等。

终端操作

操作请求方可以对终端执行不同的终端操作。以下列举了几种常见的终端操作。

盘点操作 (也可以称为盘存操作), 即盘点当前存在的终端情况, 也可以理解为获取终端的标识信息。每个终端会有其标识。终端的标识可以由企业或者第三方实体分配 (即在企业生产或制造终端时写入终端中), 也可以由运营商分配。在一种可能的实现方式中, 终端的标识可以是一个全球唯一的码, 例如电子产品代码 (electronic product code, EPC), 也可以是临时的标识或者不为全球唯一的标识。在盘点流程中, 操作请求方可以向阅读器下发盘点指令。通常, 盘点指令会包括终端的标识范围、阅读器的标识、位置信息等信息。阅读器接收到盘点指令后, 会根据盘点指令向相应终端进行盘点, 并向操作请求方发送终端的标识信息。或者, 操作请求方向阅读器发送指令, 阅读器向相应终端发送该指令。终端根据指令的内容获知为盘点操作, 终端向阅读器发送终端的标识信息。阅读器向操作请求方发送终端的标识信息。

读操作, 即对终端进行数据读取。终端可以有存储功能, 其存储区可以存储数据。若操作请求方欲对终端进行读操作, 则会向阅读器发送读指令, 阅读器根据读指令对终端进行读操作, 从终端的存储区中读取数据, 并向操作请求方发送该数据。

写操作, 即对终端进行数据写入。操作请求方可以向阅读器发送写指令, 阅读器根据指令对终端进行写操作, 向终端的存储区写入数据。

失效操作, 即能使终端失效。操作请求方可以向阅读器发送失效指令, 失效指令中可以包括终端标识 (即希望失效的终端的标识)。阅读器根据指令对终端进行失效操作, 操作完成后, 该终端会失效, 而不得再被盘点或被执行其他操作。本申请中, 终端的示例为标签。例如, 失效操作能使标签失效, 失效指令中可以包含标签标识 (即希望失效的标签的标识)。

获取标签信息, 可以理解为是上述各种操作的一个上位描述 (例如是盘点操作和读操作的上位描述), 它不区分操作请求方是盘点终端还是读终端数据, 该操作会获取终端信息, 该终端信息可以是终端的标识信息或者是终端的存储区中存储的信息。

与终端的消息交互操作, 可以理解为是上述各种操作的一个上位描述。阅读器接收操作请求方发送的指令后, 与终端进行信息或者消息交互, 并向操作请求方发送来自终端的信息。该操作主要是针对上述阅读器不查看指令内容, 只负责转发操作请求方发送给终端的消息和终端发送给操作请求方的消息。因此在该场景下, 阅读器对终端执行的操作可以理解为是与终端的消息交互操作。

无源物联网的几种可能架构

当第三代合作伙伴项目 (the 3rd generation partnership project, 3GPP) 网络支持无源物联网时, 需要支持无源物联网指令的传输。图 2A、图 2B、图 2C 示出了 3GPP 网络支持 P-IoT 的三种架构示意图。图 2A 示出了 3GPP 网络支持 P-IoT 的技术路径 1 的架构示意图。图 2B 示出了 3GPP 网络支持 P-IoT 的技术路径 2 的架构示意图。图 2C 示出了 3GPP 网络支持 P-IoT 的技术路径 3 的架构示意图。

对于技术路径 1，指令的传输方式可以通过用户面连接传输。图 2A 中的斜线区域表示用户面连接或者用户面通道，N2、N3、N4、N6 以及 N11 均表示接口。例如 RAN 与 UPF 通过 N3 接口通信，或者可以理解为 RAN 与 UPF 建立了 N3 隧道。又例如，UPF 与数据网络的接口是 N6。在一种可能的实现方式中，阅读器建立用户面连接，操作请求方（例如服务器）通过用户面连接向阅读器发送指令。阅读器可以是终端设备，也可以是无无线接入网设备、基站、微站、接入回传一体化（integrated access and backhaul, IAB）、杆站等。图 2A 以阅读器为接入网设备为例进行示意。

对于技术路径 2，指令的传输方式仍可以通过用户面连接传输。图 2B 中的斜线区域表示用户面连接或者用户面通道。图 2B 中，N2、N3、N4、N6 以及 N11 均表示接口。例如 RAN 与 UPF 通过 N3 接口通信，或者可以理解为 RAN 与 UPF 建立了 N3 隧道。又例如，UPF 与数据网络的接口是 N6。与技术路径 1 不同的是，阅读器与用户面设备建立用户面连接，用户面设备与操作请求方（例如服务器）建立连接。也就是说，阅读器并非建立数据网络粒度的会话。例如，若服务器 1 位于数据网络（data network, DN）1 中，而服务器 2 位于数据网络 2 中。若在技术路径 1 中，阅读器需要建立两个会话分别连接数据网络 1 和数据网络 2。若在技术路径 2 中，阅读器只需与同 1 个用户面设备建立一个用户面连接，由用户面设备分别与服务器 1 与服务器 2 建立连接。技术路径 2 的好处在于，当服务器需要向多个接入网设备发送指令，且多个阅读器均由同一用户面设备服务时，在技术路径 1 中，服务器需要向该用户面设备发送多个指令；而在技术路径 2 中服务器只需向该用户面设备发送一个指令，由用户面设备分别向多个阅读器发送指令。技术路径 2 中，阅读器可以是终端设备，也可以是无无线接入网设备、基站、微站、接入回传一体化（integrated access and backhaul, IAB）、杆站等。图 2B 以阅读器为接入网设备为例进行示意。

对于技术路径 3，指令的传输方式可以通过控制面通道传输，即服务器（或者应用功能）通过 NEF 向 AMF 发送指令。图 2C 中，N2、N3、N4 以及 N11 均表示接口。例如 RAN 与 UPF 通过 N3 接口通信，或者可以理解为 RAN 与 UPF 建立了 N3 隧道。AMF 向接入网设备发送该指令。当接入网设备与终端完成信息交互后，向 AMF 发送信息（如来自终端的信息）。AMF 通过 NEF 向服务器发送信息。图 2C 以阅读器为接入网设备为例进行示意。当阅读器是终端设备时，在技术路径 3 中，指令的传输方式可以是服务器（或者应用功能）通过 NEF 向 AMF 发送指令。AMF 通过接入网设备向阅读器发送该指令。

3GPP 网络支持无源物联网的运营模式

运营商建立的 3GPP 网络支持的无源物联网，其商业模式可能有以下几种可能：

(1)、运营商为企业建立独立的网络，该网络支持无源物联网。运营商通过向企业收取建站的费用来盈利。

(2)、运营商可以为企业建立独立的网络或者非独立的网络，该网络支持无源物联网。运营商通过合约或者套餐的方式向企业收取费用。例如，运营商可以与企业签订合同，每月 100 元，允许企业使用 1 万个终端（例如标签）。

(3)、运营商可能还会有其他的商业模式，本申请不限制运营商的商业模式。除了第一种商业模式中，运营商无需获取企业使用终端的情况之外，对于其他运营商需要获取企业使用的终端情况或者运营商需要对终端进行管理、接入认证、计费等情况，运营商需要获取终端的标识信息从而对终端进行管理。

终端的注册流程

本申请中，终端可称为终端设备或者用户设备（user equipment, UE），后续以 UE 代指

终端。图3为本申请实施例提供的一种UE的注册流程的示例。如图3所示，一种可能的UE的注册流程如下：

1. UE向RAN发送注册请求消息。

注册请求消息可包含注册类型(registration type)以及UE的标识信息。UE的标识信息可以包括用户隐藏标识符(subscription concealed identifier, SUCI)、全局唯一的临时UE标识(5G globally unique temporary UE identity, 5G-GUTI)或者永久设备标识符(permanent equipment identifier, PEI)中的一个或多个。

注册类型有如下几种：

初始注册(initial registration)：当UE处于去注册状态时发起的注册流程；

移动性注册更新(mobility registration update)：当UE因移动而需要发起的注册流程；

周期性注册更新(periodic registration update)：当UE处于注册状态，因周期性注册更新计时器超时而发起的注册流程；

紧急注册(emergency registration)：当UE处于业务受限状态时发起的注册流程。

对于UE的标识信息，当UE有有效的5G-GUTI(一个临时身份标识，由服务于它的AMF分配)时，在注册请求中携带该5G-GUTI；若UE无有效的5G-GUTI，则携带SUCI。在紧急注册中，若UE无有效的5G-GUTI以及无SUPI(即无SUCI，SUCI是加密的SUPI)，则携带PEI。

2. RAN选择AMF。

3. RAN将UE发送的注册请求消息发给AMF。

4. AMF选择合适的AUSF以进行鉴权等安全流程；UE、AMF、AUSF、UDM交互，以完成鉴权等安全流程。

5. 当UE与网络侧相互鉴权成功后，AMF与UDM交互以获取UE的签约数据。

6. AMF向RAN发送N2消息。

N2消息中可包括需要让RAN转发给UE的NAS消息。该NAS消息中可包括AMF向UE发送的注册接受消息(NAS消息)。

7. RAN向UE转发AMF发送的注册接受消息。

操作请求方进行终端操作时，需要采用终端的标识来识别终端，以便被执行操作的终端获知该指令是否对应自身。因此操作请求方需要使用一个终端标识来标识终端。本申请中，将操作请求方识别终端的标识称为终端应用标识(或者称为终端的应用标识)。3GPP网络支持无源物联网，若3GPP网络想要对终端进行接入认证、管理或者计费等，3GPP网络也需要获取终端的标识信息。本申请中，可以将网络识别终端的标识信息称为终端网络标识(或者称为终端的网络标识)。一种可能的实现方式中，同一个终端的应用标识和网络标识可以相同，也可以不同。在一种可能的实现方式中，由企业(或者运营商)分配终端的应用标识和/或网络标识。由于企业可能存在安全隐私的诉求，不希望网络获取终端的应用标识，那么一种可能的实现方式是，终端的应用标识与网络标识不同，且终端的应用标识由企业分配，终端的网络标识由运营商分配。若运营商需要获取终端的标识信息对终端进行管理，那么运营商如何防止企业盗用标签(例如不同的终端采用同样的网络标识接入网络，导致明明每月只能使用1万标签，企业却可以使用多于1万数量的标签)，这也是需要思考和解决的。本申请中，企业对应的实体是为企业提供服务的设备，例如服务器或者应用功能；运营商对应的实体是为运营商提供服务的设备，例如业务运营支撑系统(business & operation support system, BOSS)、服务器或者核心网设备。可理解，企业分配终端的应用标识和/或网络标识是指操作请求方(例

如服务器或者应用功能)分配终端的应用标识和/或网络标识;运营商分配终端的应用标识和/或网络标识是指运营商通过其对应的设备(例如服务器、业务运营支撑系统或者核心网设备)分配终端的应用标识和/或网络标识。

本申请中,企业可以理解为第三方、应用方、服务提供商、核心网或者网络或者移动网络之外的实体。

由于操作请求方和终端需要通过核心网设备进行通信,因此需要研究如何对终端进行接入管理的方案。对终端进行接入管理涉及的问题的举例如下:1、如何合理分配终端的标识,例如如何分配终端的网络标识和/或应用标识;2、终端的网络标识和/或应用标识由谁分配;3、如何防止终端的标识被盗用;4、如何认证授权终端;5、终端的标识由谁写入。

对于如何分配终端的标识,本申请提供了几种可能的方案。

方案一运营商预配置终端的应用标识。

运营商分配终端的应用标识(类似于运营商分配手机号)。本申请中,运营商可替换为网络、运营系统、服务器或核心网设备。或者,操作请求方分配终端的应用标识并通知运营商。运营商向终端写入标识(类似运营商烧卡发卡)或者运营商授权企业向终端写入标识。向终端写入标识时可以写入安全参数(或者称为安全上下文)。安全参数可以包括但不限于预配置密钥(例如用于标识加解密或者进行校验运算)或者哈希参数(例如用于认证或者鉴权);网络对终端的应用标识进行认证(例如认证随机数与哈希后的校验值(AUTH值))。本申请中,网络可以是指核心网和/或接入网。通过向终端写入安全参数来执行认证流程。终端可以发送终端标识(或者加密的终端标识),网络记录终端的应用标识与终端标识的对应关系,一个终端的应用标识只能与一个终端标识对应,从而防止多个终端采用同样的标识,即防止盗用终端的标识。在一种可能的实现方式中,终端为标签,终端标识为标签标识(tag identifier, TID),加密的终端标识为加密的标签标识(concealed tag identifier, CTID)。TID是标签的唯一标识,在生产标签时,会将TID和/或CTID写入标签的存储区中,只可读不可写。TID可用于标识标签本身,可以不同于标签的应用标识。

方案二企业或者操作请求方分配终端的应用标识,运营商未预配置终端的应用标识(即运营商不预先获取终端的应用标识)。

企业向终端写入标识或者运营商授权企业向终端写入标识。在一种可能的实现方式中,终端为标签,向终端写入标识是指将标签的标识信息写入标签。向终端写入标识时可写入安全参数(或者称为安全上下文)。通过在向终端写入标识时写入安全参数来认证终端。终端注册时发送终端标识,网络记录终端标识,可根据终端标识监控企业使用终端的数量。

方案三企业或者操作请求方分配终端的应用标识,运营商分配终端的网络标识

运营商分配终端的网络标识可以是授权企业或操作请求方将终端的网络标识写入至终端中。向终端写入标识时可以写入安全参数(或者称为安全上下文)。通过在向终端写入标识时写入安全参数来认证授权终端。终端注册时可发送终端标识,网络记录终端标识,根据终端标识监控企业使用终端的数量,以便防止终端的标识被盗用。

方案四企业或者操作请求方分配终端的应用标识,运营商通过在线签约分配终端的网络标识。

本申请中,在线签约可以是指终端采用默认的凭证接入网络,网络认证后,向终端发送用于后续接入网络的签约数据或者凭证(即可以理解为在线获取签约数据)。一种可能的实现方式是,终端采用企业或者操作请求方粒度的标识或者凭证或者一个默认的凭证接入网络,认证通过后,网络向终端发送网络标识。后续终端再采用获得的网络标识接入网络中。向终

端写入标识时可写入安全参数（或者称为安全上下文），网络对企业粒度的标识进行认证（如认证随机数与密钥进行运算后的 AUTH 值），这样就可以实现网络认证终端。

终端执行在线签约时需要发送企业标识或者默认标识，网络根据企业标识或者默认标识分配网络标识。默认标识可以是终端与网络协商或约定的任意标识。终端注册时需要发送网络标识，网络记录网络标识。网络根据网络标识记录或者监控企业（或者操作请求方）使用的终端数量，从而防止企业（或者操作请求方）使用的终端数量超过允许使用的数量（即数量阈值）。网络根据网络标识记录或者监控企业（或者操作请求方）使用的终端数量的一种举例是：UDM 或者 AMF 根据网络标识记录或者监控企业（或者操作请求方）使用的终端数量。

为解决如何对终端进行接入管理的问题，本申请提供了终端管理方法。采用本申请提供的终端管理方法，可实现对终端的接入管理，防止终端的标识被盗用。本申请提供的终端管理方法适用于图 2A 至图 2C 所示的无源物联网架构，还适用于其他对终端进行接入管理的架构。本申请以 5G 网络为例说明本方案。需注意的是，本申请提供的终端管理方法也适用于 4G、6G 网络等。

对于 5G 网络的系统架构，涉及的设备有核心网设备，例如 AMF、AUSF、UDM，还有服务器，例如操作请求方（即下发指令的服务器或者应用功能 AF）。下面介绍本申请涉及的设备。

移动性管理网元：主要用于移动性管理和接入管理等，可以用于实现移动性管理网元（mobility management entity, MME）功能中除会话管理之外的其它功能，例如，合法监听以及接入授权/鉴权等功能。移动性管理网元（也可称为接入与移动性管理设备、接入与移动性管理功能实体、接入与移动性管理功能网元、移动管理网元、移动管理实体），是核心网设备的一种。移动管理设备可用于对用户设备的接入控制和移动性进行管理。移动管理设备的一种举例为 5G 中的 AMF 网元。在实际应用中，AMF 网元包括长期演进(long term evolution, LTE)的网络框架中的移动性管理实体（mobility management entity, MME）的接入与移动性管理功能，并加入了接入管理功能。AMF 网元具体可以负责用户设备的注册、移动性管理、跟踪区更新流程、可达性检测、会话管理网元的选择、移动状态转换管理等。例如，在 5G 中，接入与移动性管理网元可以是接入与 AMF 网元。在未来通信，如 6G 中，接入与移动性管理网元仍可以是 AMF 网元，或有其它的名称，本申请不做限定。当接入与移动性管理网元是 AMF 网元时，AMF 网元可以提供 Namf 服务。例如，AMF 可以提供 N1N2 消息传输服务（Namf_Communication_N1N2MessageTransfer service），其他核心网网元可以通过该 AMF 服务向终端设备发送 N1 消息或者向接入网设备发送 N2 消息。

物联管理设备：用于管理物联终端或者处理物联业务的设备。例如，物联管理设备的功能可以包括以下功能中的一项或多项：识别来自操作请求方的业务指令、指示阅读器执行物联终端的接入流程（例如随机接入流程）、收集和/或处理来自物联终端的业务数据、对物联业务进行数据路由等。物联管理设备可以是 TMF 网元、PIMF 网元、或 AIMF 网元等，本申请对物联管理设备的名称不做限定。

用户面网元：用于分组路由和转发以及用户面数据的服务质量（quality of service, QoS）处理等。在 5G 通信系统中，该用户面网元可以是用户面功能（user plane function, UPF）网元，可以包括中间用户面功能（intermediate user plane function, I-UPF）网元、锚点用户面功能（PDU Session anchor user plane function, PSA-UPF）网元。在未来通信系统中，用户面网元仍可以是 UPF 网元，或者，还可以有其它的名称，本申请不做限定。UPF 网元（也可称为用户面设备），是核心网设备的一种。UPF 网元可以负责用户设备中用户数据的转发和接收。UPF 网

元可以从数据网络接收用户数据，通过接入网网元传输给用户设备。用户面功能网元还可以通过接入网网元从用户设备接收用户数据，并将用户数据转发到数据网络。用户面功能网元中为用户设备提供服务的传输资源和调度功能由会话管理功能网元管理控制。

会话管理网元：主要用于会话管理、终端设备的网络互连协议（internet protocol, IP）地址分配和管理、选择可管理终端设备平面功能、策略控制和收费功能接口的终结点以及下行数据通知等。在 5G 通信系统中，该会话管理网元可以是会话管理功能（session management function, SMF）网元，可以包括中间会话管理功能（intermediate session management function, I-SMF）网元、锚点会话管理功能（anchor session management function, A-SMF）网元。在未来通信系统中，会话管理网元仍可以是 SMF 网元，或者，还可以有其它的名称，本申请不做限定。SMF 网元（也可称为会话管理设备），是核心网设备的一种。SMF 网元可用于负责用户设备的会话管理（包括会话的建立、修改和释放），用户面功能网元的选择和重选、用户设备的互联网协议（internet protocol, IP）地址分配、服务质量（quality of service, QoS）控制等。例如，在 5G 中，会话管理网元可以是会话管理功能（session management function, SMF）网元。在未来通信系统中，如 6G 中，会话管理网元仍可以是 SMF 网元，或有其它的名称，本申请不做限定。当会话管理网元是 SMF 网元时，SMF 网元可以提供 Nsmf 服务。

认证服务网元：用于鉴权服务、产生密钥实现对终端设备的双向鉴权，支持统一的鉴权框架。在 5G 通信系统中，该认证服务网元可以是认证服务功能（authentication server function, AUSF）网元。在未来通信系统中，认证服务功能网元仍可以是 AUSF 网元，或者，还可以有其它的名称，本申请不做限定。

应用功能网元：应用功能网元可以通过应用功能网元与 5G 系统交互，用于接入网络开放功能网元或与策略框架交互进行策略控制等。在 5G 通信系统中，该应用功能网元可以是（application function, AF）网元。在未来通信系统中，应用功能网元仍可以是 AF 网元，或者，还可以有其它的名称，本申请不做限定。

网络开放功能网元：用于提供网络开放的定制功能。在 5G 通信系统中，该网络开放功能网元可以是网络开放功能（network exposure function, NEF）网元。在未来通信系统中，该网络开放功能网元仍可以是 NEF 网元，或者，还可以有其它的名称，本申请不做限定。5G 通信系统还可以通过 NEF 网元，向外部的应用功能网元开放 5GC 支持的能力，譬如提供小数据传递能力等。NEF 网元（也可以称为网络开放设备），是核心网设备的一种。网络开放功能网元可用于使 3GPP 能够安全地向第三方的 AF（例如，业务能力服务器（services capability server, SCS）、应用服务器（application server, AS）等）提供网络业务能力等。例如，在 5G 中，网络开放网元可以是网络开放功能（network exposure function, NEF）网元。在未来通信系统中，如 6G 中，网络开放网元仍可以是 NEF 网元，或有其它的名称，本申请不做限定。当网络开放网元是 NEF 网元时，NEF 网元可以向其他网络功能网元提供 Nnef 服务。

数据管理网元：用于处理终端设备标识，接入鉴权，注册以及移动性管理等。在 5G 通信系统中，该数据管理网元可以是统一数据管理（unified data management, UDM）网元或统一数据存储库（unified data repository, UDR）网元。在未来通信系统中，统一数据管理仍可以是 UDM、UDR 网元，或者，还可以有其它的名称，本申请不做限定。本申请实施例中的 UDM 或 UDR 网元可以是指用户数据库。可以作为一个存储用户数据的单一逻辑存储库存在。UDM 网元（也可以称为统一数据管理设备、数据管理设备、统一数据管理实体）。在 5G 通信系统中，统一数据管理网元可以是 UDM 网元或者统一数据管理设备。在未来的通信系统中，统一数据管理网元还可以是 UDM 网元，或者还可以有其它的名称，本申请实施例不做

限定。统一数据管理设备可以是核心网设备。统一数据管理设备可以是控制面设备。UDR 网元（也可以称为用户数据库设备、用户数据库实体）可以理解为统一数据存储网元在 5G 架构中的命名。其中，用户数据库主要包括以下功能：签约数据、策略数据、应用数据等类型数据的存取功能。

用户设备（user equipment, UE）：可以称终端设备、终端、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、无线通信设备、用户代理或用户装置。UE 还可以是蜂窝电话、无绳电话、会话启动协议（session initiation protocol, SIP）电话、无线本地环路（wireless local loop, WLL）站、个人数字助理（personal digital assistant, PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，5G 网络中的终端设备或者未来演进的公用陆地移动通信网络（public land mobile network, PLMN）中或者非陆地网络（non-terrestrial networks, NTN）的终端设备等，还可以是端设备，逻辑实体，智能设备，如手机，智能终端等终端设备，还可以是服务器，网关，基站，控制器等通信设备，或者物联网设备，如标签，无源标签，有源标签，半有源标签、半无源标签、传感器，电表，水表等物联网（internet of things, IoT）设备。UE 还可以是具有通信功能的无人机（unmanned aerial vehicle 或 uncrewed aerial vehicle, UAV）。当终端为无源或者半无源或者半有源的终端或者标签时，可以通过获取能量以接收或者发送数据。获取能量的方式可以通过无线电、太阳能、光能、风能、水能、热能、动能等方式获取。本申请对于无源或者半无源或者半有源的终端获取能量的方式不做限定。本申请实施例对此并不限定。

操作请求方：操作请求方可以理解为发送操作指令的设备，比如操作请求方可以是服务器（server）或者 P-IoT server 或者应用功能（application function, AF）或者其他发送操作指令的设备。操作请求方可以对应某类用户，该类用户可以包括企业、租户、第三方或者公司，不予限制。其中，操作请求方对应某类用户可以理解为该操作请求方属于该类用户，由该类用户管理。

接入网设备通过射频信号或者无线信号与终端（例如标签）交互。应理解，本申请对接入网设备的名称不做限定，接入网设备还可以命名为其他名称，这里的接入网设备具备本申请中阅读器所涉及的部分或者全部功能，比如具备对终端（比如标签）执行本申请所述的操作（比如获取标签信息、盘点操作、读操作、写操作或者、失效操作或者与标签的消息交互操作等）的功能、具备获取计费相关信息和/或计费信息、向计费功能（charging function, CHF）发送计费信息的功能等。一种可能的实现方式中，接入网设备可以向终端（例如标签）发送来自服务器或者应用功能或者核心网设备的指令，或者接入网设备可以向服务器或者应用功能发送来自终端（例如标签）的消息。一种可能的实现方式中，接入网设备可以根据服务器下发的指令来获取指定的终端（例如标签）中存储的信息。例如若为盘点操作（或者可以称为盘存操作），接入网设备获取终端（例如标签）的标识信息；该标识信息可以是终端的唯一标识，也可以是终端的临时标识。例如若为读操作，接入网设备则读取该终端的存储区中的数据或者向核心网设备发送来自终端的存储区中的数据。可选的，在一些需要改写终端内存储的信息的场合下，接入网设备可以具有写的功能。例如若为写操作，则接入网设备将数据写入终端（例如标签）的存储区中或者向终端（例如标签）转发来自服务器或者应用功能或者核心网设备的指令，向标签的存储区写入数据。除此之外，接入网设备还可以对终端（例如标签）执行失效操作。在终端（例如标签）被执行失效操作后，该终端（例如标签）失效，该终端（例如标签）不可被执行获取标签信息、盘点操作、读操作、与终端的消息交互操作

或者写操作等操作。一种可能的实现方式中，终端失效不可被执行获取标签信息可以理解为终端失效后，接入网设备无法获取该失效终端的标签信息。另一种可能的实现方式中，终端失效不可被执行与终端的消息交互操作可以理解为终端失效后，接入网设备无法与该失效终端进行消息交互。本申请中，接入网设备可以是杆站、eNodeB、gNodeB、接入回传一体化（integrated access and backhaul, IAB）节点等等，本申请对接入网设备的形态不做限定。本申请中，阅读器可以是接入网设备，也可以是终端设备。本申请对阅读器的形态不做限定。

在介绍本申请提供的一些可能的实施例之前，先整体介绍一下终端的应用标识和/或网络标识分配的几种可能的方式。这样后续在描述各个实施例时，可以直接引用几种可能方式中的一个或多个，从而可以不用重复赘述。图4示出了本申请实施例提供的几种分配终端的应用标识的方式的示例。

方式一：操作请求方分配终端的应用标识，第二核心网设备获取放号数量。

放号数量可以理解为操作请求方（例如企业）允许使用的终端数量。在一种可能的实现方式中，终端为标签，终端数量是标签标识的数量或者是实体标签的数量。两者差异在于，前者是标签标识的数量，若某个标签损坏了，那么可以替换为新标签，但新标签的标签标识可以为原先损坏的标签的标签标识。后者就是标签这个终端本身。本申请实施例中，第二核心网设备可以是UDM、UDR或者其他核心网网元。如图4所示，方式一中分配终端的应用标识包括以下操作：

401.第二核心网设备获取第一信息。

第一信息中可包括放号数量。本申请中，放号数量可以理解为号码的数量、终端的数量或者标识的数量。放号数量可与标识数量、终端数量、号码数量或者数量信息等互换。步骤401一种可能的实现方式如下：第二核心网设备接收运营商的运营业务支撑（business & operation support System, BOSS）系统发送的第一信息（可称为放号消息）。BOSS可替换为运营商对应的其他实体。也就是说，本申请实施例不限定运营商通过哪种方式向第二核心网设备发送第一信息。

在一种可能的实现方式中，第一信息中还可以包括企业标识。企业标识用于标识企业。由于企业可以部署独立的网络，因此第二核心网设备（例如UDM或UDR）可以只服务该企业，因此企业标识是作为可选的参数。对于公共网络场景或者核心网设备是服务多个企业时，企业标识可以用于标识不同的企业。本申请中，企业标识可以理解或者可以替换为操作请求方标识或者用户标识。操作请求方标识可以包括地址信息、标识信息、端口号、服务标识、事务号中的一项或多项。

402.第二核心网设备配置放号数量。

第二核心网设备配置放号数量，以便根据该放号数量执行接入管理。根据放号数量执行接入管理可以包括以下一项或多项：根据放号数量分配终端的网络标识、根据放号数量分配终端的应用标识、根据放号数量确定操作请求方允许使用的终端数量、根据放号数量确定操作请求方已使用的终端数量是否超过该操作请求方允许使用的终端数量。

403.操作请求方获取第二信息。

第二信息中包括放号数量。步骤403一种可能的实现方式如下：操作请求方接收运营商的BOSS系统发送的第二信息（例如可以是放号消息）。BOSS可替换为运营商对应的其他实体。也就是说，本申请实施例不限定运营商通过哪种方式向操作请求方发送第二信息。第一信息和第二信息可相同，也可以不同。例如，第一信息和第二信息均为放号消息，且均包含放号数量。又例如，第一信息包含放号数量和企业标识，第二信息包含放号数量且未包含企

业标识。在方式一中，步骤 401 和步骤 403 的先后顺序不作限定。可理解，第二核心网设备执行的操作（步骤 401 和步骤 402）与操作请求方执行的操作（步骤 403 和步骤 404）是相互独立的。

404.操作请求方分配终端的应用标识。

在一种可能的实现方式中，操作请求方根据放号数量分配终端的应用标识。举例来说，放号数量为 1 万，操作请求方根据放号数量分配 1 万个终端的应用标识，每个终端对应一个应用标识。

405.第一核心网设备接收来自第二核心网设备的数量信息和/或第一标识信息。

第一核心网设备可以是 AMF，也可以是物联管理设备，即具备物联终端管理或者具备处理物联业务功能的设备。所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、所述操作请求方标识中的一项或多项。操作请求方标识用于标识操作请求方。数量信息可包括操作请求方允许使用的终端数量（可以理解为放号数量）。

方式二：操作请求方分配终端的应用标识，运营商分配终端的网络标识并向操作请求方发送终端的网络标识或者操作请求方分配终端的网络标识。

411.第二核心网设备获取第一信息。

步骤 411 可参阅步骤 401。第一信息还可以包括企业标识或者终端的网络标识。在一种可能的实现方式中，终端的网络标识由 BOSS 系统分配，则在上述第一信息中还可包括终端的网络标识。另一种可能的实现方式中，终端的网络标识由第二核心网设备（例如 UDM 或 UDR）分配，则第一信息中无需包括终端的网络标识。

412.第二核心网设备配置放号数量。

步骤 412 可参阅步骤 402。

413.操作请求方获取第二信息。

步骤 413 可参阅步骤 403。第二信息还可以包括终端的网络标识。若终端的网络标识由 BOSS 系统分配，则第二信息中还包括终端的网络标识。若终端的网络标识由第二核心网设备（例如 UDM 或 UDR）分配，则第二信息中无需包括终端的网络标识。

414.操作请求方分配终端的应用标识。

步骤 414 可参阅步骤 404。

415.第二核心网设备分配终端的网络标识。

步骤 415 一种可能的实现方式如下：第二核心网设备根据放号数量分配终端的网络标识。第二核心网设备分配的终端网络标识可以是第二核心网设备为操作请求方分配的终端网络标识，即为操作请求方的终端分配的网络标识。

步骤 415 可替换为：第一信息包括终端的网络标识，第二核心网设备根据该第一信息获取一个或多个终端的网络标识。

416.第二核心网设备向操作请求方发送终端的网络标识。

步骤 415 和步骤 416 是可选的，而非必要的。可理解，若终端的网络标识由第二核心网设备分配，则第二核心网设备可根据放号数量分配终端的网络标识，以便根据终端的网络标识执行接入管理。若终端的网络标识由第二核心网设备分配，则第二核心网设备执行步骤 415 之后，向操作请求方发送分配的终端网络标识，即执行步骤 416。在一种可能的实现方式中，第二核心网设备可以通过 NEF 向操作请求方发送分配的终端网络标识。若终端的网络标识由运营商分配，第一信息和第二信息中均可包含运营商为操作请求方的终端分配的网络标识，则第二核心网设备可根据第一信息获取终端的网络标识，操作请求方可根据第二信息获取终

端的网络标识。也就是说，若终端的网络标识由运营商分配，则第二核心网设备不必分配终端的网络标识，也不需要执行步骤 416。

417.第一核心网设备接收来自第二核心网设备的数量信息和/或第一标识信息。

步骤 417 可参阅步骤 405。

方式三：操作请求方分配终端的应用标识，第二核心网设备获取放号数量和操作请求方分配的终端的应用标识。

421.第二核心网设备获取第一信息。

步骤 421 可参阅步骤 401。

422.第二核心网设备配置放号数量。

步骤 422 可参阅步骤 402。

423.操作请求方获取第二信息。

步骤 423 可参阅步骤 403。

424.操作请求方分配终端的应用标识。

步骤 424 可参阅步骤 404。

425.第二核心网设备获取终端的应用标识。

步骤 425 一种可能的实现方式如下：第二核心网设备接收操作请求方根据放号数量分配的终端的应用标识。相应地，操作请求方向第二核心网设备发送其分配的终端的应用标识。在一种可能的实现方式中，操作请求方向第二核心网设备发送终端的应用标识列表，即包括一个或多个终端的应用标识的列表。在一种可能的实现方式中，操作请求方向第二核心网设备发送一个消息，该消息包含一个或多个终端应用标识。可选的，操作请求方向第二核心网设备发送的包含终端应用标识的消息还可以包括企业标识。企业标识用于标识企业。由于企业可以部署独立的网络，第二核心网设备可以只服务该企业，因此企业标识是作为可选的参数。对于公共网络场景或者第二核心网设备是服务多个企业时，企业标识可以用于标识不同的企业。一种可能的实现方式中，操作请求方通过 NEF 向第二核心网设备发送包括一个或多个终端的应用标识的消息。

426.第二核心网设备配置终端的应用标识。

第二核心网设备配置终端的应用标识可以是第二核心网设备存储终端的终端标识与终端应用标识的对应关系，也可以是将该一个或多个终端应用标识配置为操作请求方可用的终端应用标识。

427.第一核心网设备接收来自第二核心网设备的数量信息和/或第一标识信息。

步骤 427 可参阅步骤 405。

方式四：运营商分配终端的应用标识，运营商向操作请求方发送终端的应用标识。

431.运营商的 BOSS 系统分配终端的应用标识。

步骤 431 一种可能的实现方式如下：运营商的 BOSS 系统根据放号数量，分配终端的应用标识。也就是说，运营商的 BOSS 系统根据操作请求方允许使用的终端数量，为操作请求方分配相应数量的终端应用标识。

432.第二核心网设备获取第一信息。

第一信息包括放号数量和终端应用标识。第一信息包括的终端应用标识可以是步骤 431 中运营商的 BOSS 系统为操作请求方分配的终端的应用标识。第一信息还可以包括企业标识。步骤 432 可参阅步骤 401。

433.第二核心网设备配置放号数量和终端的应用标识。

434.操作请求方获取终端的应用标识。

步骤 434 中，操作请求方获取的终端的应用标识可以是分配给该操作请求方的终端应用标识。

步骤 434 一种可能的实现方式是：操作请求方接收运营商的 BOSS 系统发送的终端应用标识。操作请求方还可以通过其他方式从为运营商提供服务的设备获取一个或多个终端应用标识。可选的，操作请求方还可以获取放号数量和/或企业标识。举例来说，操作请求方接收来自运营商的 BOSS 系统的第二信息，该第二信息包括运营商为操作请求方分配的一个或多个终端应用标识。该第二信息还可以包括放号数量和/或企业标识。

步骤 434 另一种可能的实现方式是：操作请求方接收第二核心网设备发送的终端应用标识。举例来说，操作请求方接收来自第二核心网设备的第二信息，该第二信息包括运营商为操作请求方分配的一个或多个终端应用标识。该第二信息还可以包括放号数量和/或企业标识。

435.第一核心网设备接收来自第二核心网设备的数量信息和/或第一标识信息。

步骤 435 可参阅步骤 405。

需要说明，方式一至方式四仅为本申请实施例提供的几种可能的分配终端的应用标识和/或网络标识的举例，而不是全部举例。

图 4 示出了操作请求方、BOSS 系统、第二核心网设备以及第一核心网设备实现的几种可能的分配终端的应用标识和/或网络标识的举例。下面结合附图单独描述操作请求方在分配终端的应用标识和/或网络标识的过程中执行的方法流程。

本申请中，第一核心网设备可以是移动管理设备、会话管理设备、策略控制设备、统一数据管理设备、统一数据存储库、网络开放功能设备、用户面设备、或物联管理设备，本申请对第一核心网设备不做限制。本申请中，第二核心网设备可以是移动管理设备、会话管理设备、策略控制设备、统一数据管理设备、统一数据存储库、网络开放功能设备、用户面设备，本申请对第二核心网设备不做限制。

本申请中，终端接入网络可以理解为终端注册网络、终端成功注册核心网或者终端成功执行流程。网络接受终端接入网络可以理解为网络接受终端的注册、网络接受终端的注册请求、网络接受终端注册网络、网络接受终端注册流程、核心网接受终端注册网络、核心网接受终端注册核心网。网络拒绝终端接入网络可以理解为网络拒绝终端的注册、网络拒绝终端的注册请求、网络拒绝终端注册网络、网络拒绝终端注册流程、核心网拒绝终端注册网络、核心网拒绝终端注册核心网。

图 5 为本申请实施例提供的一种终端管理方法流程图。如图 5 所示，该方法包括：

501、操作请求方获取数量信息。

所述数量信息指示所述操作请求方允许使用的终端数量。操作请求方获取数量信息可以是操作请求方接收 BOSS 系统发送的数量信息，可参阅步骤 403。

502、操作请求方根据数量信息，获取一个或多个终端应用标识。

步骤 502 一种可能的实现方式如下：操作请求方根据数量信息，分配一个或多个终端应用标识；其中，操作请求方分配的终端应用标识的个数为操作请求方允许使用的终端数量。举例来说，操作请求方允许使用的终端数量为 1 万个，该操作请求方分配 1 万个终端应用标识，每个终端应用标识对应于一个终端。

操作请求方还可执行如下操作：发送操作指令，所述操作指令包括第一终端应用标识，所述第一终端应用标识包含于所述一个或多个终端应用标识；所述操作指令用于对所述第一终端应用标识对应的终端执行操作。这里的操作可包括盘存(或者称为盘点)、请求标签信息、

读、写、失效、安全认证等操作。操作请求方可通过核心网设备、接入网设备向终端发送操作指令。

操作请求方还可执行如下操作：获取网络标识信息，所述网络标识信息包括一个或多个终端网络标识。操作请求方获取网络标识信息可以是接收第二核心网设备发送的一个或多个终端网络标识，也可以是接收来自 BOSS 系统的一个或多个终端网络标识。

操作请求方还可执行如下操作：向核心网设备发送所述一个或多个终端应用标识和/或所述操作请求方标识。图 4 中操作请求方向第二核心网设备发送终端应用标识和/或操作请求方标识的操作为向核心网设备发送所述一个或多个终端应用标识和/或所述操作请求方标识的示例。

图 5 中的方法流程描述的是操作请求方获取一个或多个终端应用标识的一种可能的示例。图 5 中的方法流程描述了方式一、方式二以及方式三中操作请求方执行的方法流程。步骤 501 和步骤 502 可替换为：操作请求方获取一个或多个终端应用标识（参阅步骤 434）。操作请求方获取一个或多个终端应用标识可以是接收来自 BOSS 系统的一个或多个终端应用标识，也可以是接收来自核心网设备的所述一个或多个终端应用标识。例如，第二核心网设备接收来自 BOSS 系统的第一信息之后，向操作请求方发送一个或多个终端应用标识，该第一信息包含运营商的 BOSS 系统为操作请求方分配的终端的应用标识。

本申请实施例中，操作请求方根据数量信息，获取一个或多个终端应用标识；以便获取的终端应用标识的个数小于或等于或者不多于操作请求方允许使用的终端数量。

下面结合附图介绍本申请提供的终端管理方法。

图 6A 为本申请实施例提供的另一种终端管理方法流程图。第一核心网设备在执行图 6A 中的方法流程之前，可通过执行其在方式一至方式四中执行的操作来获取数量信息和/或第一标识信息。如图 6A 所示，该方法包括：

601A、第一核心网设备接收来自终端的第一消息。

所述第一消息用于请求接入网络，该网络可以包括核心网、接入网或者其他网络，该网络中可部署有一个或多个核心网设备以及接入网设备。例如，终端请求接入的网络为企业部署的独立的网络或者公共网络或者公共网络集成非公共网络。又例如，终端请求接入的网络为多个企业公用的网络。第一核心网设备可以是移动管理设备 AMF，也可以是其他可实现终端管理功能的设备，还可以是物联管理设备。第一消息可以是用于请求接入网络的注册请求消息。第一消息可以是非接入层（non-access stratum, NAS）消息或者其他协议消息，本申请不做限制。

第一核心网设备接收来自终端的第一消息可以是第一核心网设备接收接入网设备转发的终端的第一消息。举例来说，终端向接入网设备发送注册请求消息（第一消息的示例），第一核心网设备接收该接入网设备向其转发的该注册请求消息。

在一种可能的实现方式中，第一消息包括第一标识信息，该第一标识信息标识该终端。该第一标识信息包括终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

在一种可能的实现方式中，所述第一消息包括标识信息和认证信息，所述标识信息和所述认证信息用于执行所述认证流程；所述标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、所述操作请求方标识中的一项或多项。认证信息可包括随机数、消息认证码（message authentication code, MAC）、校验值、令牌（token）等信息中的一项或多项。

602A、第一核心网设备在根据数量信息确定允许终端接入网络时，向终端所属的操作请求方发送第二消息。

所述数量信息包括所述终端所属的操作请求方允许使用的终端数量，即放号数量。操作请求方允许使用的终端数量可理解为操作请求方被允许使用的终端的数量。第二消息可包含第一标识信息，所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。示例性的，第二消息用于向操作请求方反馈接入网络的终端的标识信息；或者第二消息作为操作请求方请求获取终端信息的响应消息。

在一种可能的实现方式中，第一核心网设备为 AMF，第一核心网设备在根据数量信息确定允许终端接入网络时，通过 NEF 向终端所属的操作请求方发送第二消息。举例来说，第二消息为终端执行来自操作请求方的操作指令得到的操作结果。

步骤 602A 一种可能的实现方式如下：当所述操作请求方对应的终端中接入所述网络的终端数量小于或等于数量阈值时，所述核心网设备确定允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。操作请求方对应的终端是指属于该操作请求方的终端或者允许被该操作请求方使用的终端。操作请求方对应的终端中接入网络的终端数量可理解为属于该操作请求方的终端中已接入网络的数量。假定属于操作请求方的终端有 F 个，该 F 个终端中的 H 个已接入网络，该操作请求方对应的终端中接入网络的终端数量为 H 个， F 和 H 均为大于或者等于 0 的整数。

本申请实施例中，第一核心网设备在根据数量信息确定允许终端接入所述网络时，向该终端所属的操作请求方发送第二消息。也就是说，第一核心网设备发送第二消息之前，需要根据数量信息确定允许终端接入网络，而不是直接允许该终端接入网络。第一核心网设备根据数量信息确定允许终端接入网络，可避免操作请求方对应的终端中接入网络的终端数量大于或等于操作请求方允许使用的终端数量。

图 6B 为本申请实施例提供的另一种终端管理方法流程图。第一核心网设备在执行图 6A 中的方法流程之前，可通过执行其在方式一至方式四中执行的操作来获取数量信息和/或第一标识信息。图 6B 中的方法流程为图 6A 中描述的方法的一种可能的实现方式。如图 6B 所示，该方法包括：

601B、第一核心网设备接收来自终端的第一消息。

步骤 601B 可参阅步骤 601A。

602B、第一核心网设备在根据数量信息确定允许终端接入网络时，向第二核心网设备发送第四消息。

第二核心网设备可以是 UDM、UDR 或其他核心网设备。举例来说，第一核心网设备通过其他核心网设备（例如 AUSF）向第二核心网设备发送第四消息。

在一种可能的实现方式中，所述第四消息用于请求对所述终端执行认证流程或鉴权流程。本申请中，认证和鉴权可以是相同的概念，认证和鉴权可以相互替换。认证流程可以是认证终端是否为可信的终端或授权的终端的单向认证；或者认证流程可以是终端认证网络或者操作请求方是否为可信的网络或者操作请求方的单向认证；或者认证流程可以是双向认证，即认证流程包括终端认证网络或者操作请求方，也包括网络或者操作请求方认证终端。

在一种可能的实现方式中，所述第四消息包括第二标识信息和认证信息。所述第二标识信息和所述认证信息用于执行所述认证流程。所述第二标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。认证信

息可包括随机数、MAC 等。在一种可能的实现方式中，所述第四消息还包括指示信息；所述指示信息指示所述认证流程为单向认证、双向认证、终端对网络或者操作请求方的单向认证、网络或者操作请求方对终端的单向认证中的任一种。一种可能的实现方式中，所述指示信息指示所述认证流程为应用于无源物联网的认证流程。举例来说，第四消息为鉴权请求消息，该第四消息包含的指示信息指示该鉴权为应用于无源物联网的鉴权。

在一种可能的实现方式中，第一核心网设备在接收来自终端的第一消息之后，第一核心网设备根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。第一核心网设备确定终端所属的操作请求方，以便根据数量信息确定是否允许终端接入网络。举例来说，第一核心网设备根据第三标识信息和第一对应关系，确定终端所属的操作请求方；所述第一对应关系表示终端属于操作请求方。可选的，第一对应关系包括所述终端的应用标识（终端标识或网络标识）与操作请求方标识的对应关系，所述操作请求方标识为所述操作请求方的标识。第一核心网设备可配置或存储有一个或多个终端与其所属的操作请求方的对应关系，该第一核心网设备可根据该对应关系确定终端所属的操作请求方。又举例来说，第一核心网设备根据来自操作请求方的操作指令，确定第二对应关系，该第二对应关系表示终端属于操作请求方；第一核心网设备根据第一消息包括的第三标识信息和该第二对应关系，确定该终端所属的操作请求方。所述操作指令可包含所述终端的第一标识，该第一标识为终端的终端标识、加密的终端标识、终端应用标识、终端网络标识中的任一项。

603B、第一核心网设备接收来自第二核心网设备的第五消息。

第五消息指示操作请求方成功接收或者未成功接收终端的标识信息，或者第五消息指示终端的认证流程通过或不通过。第五消息可以通知终端其认证结果，以便终端根据该认证结果执行相应的后续操作。第一核心网设备接收第五消息可以是接收其他核心网设备发送的第五消息。第二核心网设备可以是 UDM、UDR 或其他核心网设备。在一种可能的实现方式中，第一核心网设备为 AMF，第一核心网设备接收其他核心网设备（例如 UDM 或者 AUSF）发送的第五消息。举例来说，第一核心网设备为 AMF，AMF 接收 UDM（对应于第二核心网设备）通过 AUSF 或者接收 AUSF（对应于第二核心网设备）向其发送的第五消息。

在一种可能的实现方式中，步骤 602B 和步骤 603B 可替换为：第一核心网设备根据所述第一消息对所述终端执行认证流程。所述第一消息包括第三标识信息和认证信息，所述第三标识信息和所述认证信息用于执行所述认证流程。所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。举例来说，第一消息包括终端的应用标识、随机数和消息认证码；第一核心网设备根据终端的应用标识检索安全参数，并根据安全参数和随机数验证消息认证码；若一致，则可以认为终端通过认证（或者认为终端为可信的终端）；若不一致，则可以认为终端不通过认证（或者认为终端不为可信的终端）。安全参数可以是密钥或者是 hash 算法。如果是密钥，则消息认证码可以是随机数利用该密钥加密后的值。如果是 hash 算法，则消息认证码可以是随机数经过该 hash 算法运算后得到的值。

604B、第一核心网设备向终端，发送第六消息。

所述第五消息指示操作请求方成功接收终端的标识信息或者所述认证流程通过，所述第六消息指示接受所述终端接入所述网络。或者，所述第五消息指示操作请求方未成功接收终端的标识信息或者所述认证流程不通过，所述第六消息指示拒绝所述终端接入所述网络。步

骤 604B 一种可能的实现方式如下：第一核心网设备根据第五消息向终端，发送第六消息。若第五消息指示操作请求方成功接收终端的标识信息或者指示终端的认证流程通过，第一核心网设备向终端发送指示接受所述终端接入所述网络的第六消息。若第五消息指示操作请求方未成功接收终端的标识信息或者指示终端的认证流程不通过，第一核心网设备向终端发送指示拒绝所述终端接入所述网络的第六消息。也就是说，第一核心网设备可以根据第五消息，向终端发送相应的第六消息。

在一种可能的实现方式中，第一核心网设备还可执行如下操作：获取所述数量信息和/或第一标识信息；所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、所述操作请求方标识中的一项或多项。第一核心网设备还可配置放号数量（或者数量信息）以及第一标识信息。例如，第一核心网设备配置终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、所述操作请求方标识中的一项或多项以及放号数量（或者数量信息）。在一些实施例中，第一核心网设备可以是图 4 中的第一核心网设备，通过执行方式一至方式四中的任一种方法流程来获取数量信息和/或第一标识信息。应理解，第一核心网设备获取到数量信息和/或第一标识信息之后，才可执行图 6A 和图 6B 中的方法流程。

605B、第一核心网设备向终端所属的操作请求方发送第二消息。

本申请实施例中，第一核心网设备向第二核心网设备发送第四消息，以便于对终端执行认证流程，从而保证该终端为可信的终端。

本申请实施例中，第一核心网设备发送第二消息之前，需要根据数量信息确定允许终端接入网络。若第一核心网设备根据数量信息确定不允许终端接入网络，则不必发送用于请求对该终端执行认证流程的第四消息，这样可以减少信令开销。第一核心网设备根据数量信息确定允许终端接入网络，可快速、准确地确定是否对该终端执行认证流程。应理解，第一核心网设备在根据数量信息确定允许终端接入网络时，可以不代表该终端能通过所述认证流程。

图 7 为本申请实施例提供的另一种终端管理方法流程图。第一核心网设备在执行图 6A 中的方法流程之前，可通过执行其在方式一至方式四中执行的操作来获取数量信息和/或第一标识信息。图 7 与图 6A 是第一核心网设备接收来自终端的第一消息之后，可能执行的两种不同的方法流程。如图 7 所示，该方法包括：

701、第一核心网设备接收来自终端的第一消息。

步骤 701 可参阅步骤 601B。第一核心网设备可以是 AMF，也可以是其他可实现 AMF 具备的功能的设备，还可以是物联管理设备。

702、第一核心网设备在根据数量信息确定不允许终端接入网络的情况下，向终端发送第三消息。

所述第三消息指示拒绝所述终端接入所述网络。第三消息可以是注册拒绝消息。所述数量信息包括所述终端所属的操作请求方允许使用的终端数量，可以理解为放号数量。

步骤 702 一种可能的实现方式如下：当操作请求方对应的终端中接入所述网络的终端数量大于或等于数量阈值时，所述第一核心网设备确定不允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

在一种可能的实现方式中，第一核心网设备还可执行如下操作：获取所述数量信息和/或第一标识信息；所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、所述操作请求方标识中的一项或多项。核心网设备还可配置放号数量以及标识信息。例如，第一核心网设备配置终端的终端标识、加密的终端标识、终端应用标识、

终端网络标识、所述操作请求方标识中的一项或多项以及放号数量。在一些实施例中，第一核心网设备可以是图 4 中的第一核心网设备，通过执行方式一至方式四中的任一种方法流程来获取数量信息和/或第一标识信息。应理解，第一核心网设备获取到数量信息和/或第一标识信息之后，才可执行图 7 中的方法流程。

本申请实施例中，第一核心网设备在根据数量信息确定不允许终端接入网络的情况下，向终端发送第三消息，不需要对该终端执行认证流程，可以减少不必要的操作，并及时拒绝该终端的接入。

下面结合附图介绍本申请实施例提供的一些可能的终端管理方法流程。

下面结合具体实施例图 8，对上述实施例图 6A、图 6B 以及图 7 中的终端管理方法进行详细的说明。图 8 为本申请实施例提供的一种终端管理方法交互流程图。图 8 以阅读器为接入网设备为例进行阐述，该方法也适用于阅读器为终端设备（例如 UE）的场景。如图 8 所示，该方法包括：

801、UDM 和操作请求方获取终端的应用标识。

步骤 801 一种可能的实现方式如下：UDM（或 UDR）、操作请求方、运营商的 BOSS 系统按照上述方式三或者方式四分配终端的应用标识。图 8 中的 UDM 为图 4 中的第二核心网设备的一种示例，图 8 中的 UDM 可替换为 UDR 或者其他核心网网元。参阅图 4 中的方式三和方式四可知，按照方式三或者方式四分配终端的应用标识，第二核心网设备（例如 UDM 或者 UDR）和操作请求方均可获取终端的应用标识，第一核心网设备（图 8 中的 AMF）可获取数量信息和/或标识信息。图 8 中的 AMF 为图 4 中的第一核心网设备的一种示例。

802、终端初始化。

当终端为标签时，终端初始化可以理解为标签方打印标签。标签打印方可以是运营商，也可以是操作请求方。终端的标签可以由运营商打印或者由运营商授权操作请求方（例如企业）打印。终端初始化内容可包括终端的应用标识。可选的，终端的标签的内容还可以包括安全参数（或者称为安全上下文）。安全参数可以包括预配置密钥、哈希（hash）参数等。预配置密钥可以用于对数据进行加解密或者用于生产或者推衍密钥或者用于执行哈希算法或其他用于执行认证的算法。hash 参数用于进行 hash 运算。哈希运算可以理解为哈希算法（hash），又称摘要算法（digest），它的作用是：对任意一组输入数据进行计算，得到一个固定长度的输出摘要。哈希算法最重要的特点就是：相同的输入一定得到相同的输出；不同的输入大概率得到不同的输出。

步骤 801 和步骤 802 是可选的。步骤 801 和步骤 802 可以是在执行图 8 中的其他步骤之前预先完成的操作。图 8 的方法流程中，步骤 801 和步骤 802 可视为准备阶段执行的操作，其他步骤为应用阶段执行的操作。应理解，若终端的标签已被打印，且 UDM 和操作请求方已获取终端的应用标识，则可直接执行图 8 的方法流程中步骤 803 之后的步骤（包括步骤 803），以实现终端的接入管理。

803、操作请求方向接入网设备发送操作指令。

操作指令中可以包括一个或多个终端的应用标识。操作请求方可以通过控制面通道或者用户面通道向接入网设备发送操作指令。图 8 中以操作请求方（例如 P-IoT AF）通过控制面通道向接入网设备发送操作指令为例展示。例如，操作请求方可以通过 NEF 网元、AMF 网元向接入网设备发送操作指令。或者，操作请求方可以通过 AMF 向接入网设备发送操作指令。若通过用户面通道发送，则操作请求方（例如 P-IoT 服务器）可以通过 UPF 向接入网设备发送操作指令。

一种可能实现方式中，步骤 803 可以为操作请求方向核心网设备发送操作指令，由核心网设备通过接入网设备向终端发送操作指令。可以理解的，操作请求方向核心网设备发送的操作指令（或者消息）可以不同于核心网设备向终端发送的操作指令（或者消息）；即核心网设备可以根据来自操作请求方的操作指令，生成向终端发送的操作指令（或者消息）。一种可能的实现方式中，操作请求方与核心网设备采用第一协议通信，核心网设备与终端采用第二协议通信。第一协议可以与第二协议相同，也可以不同。示例性的，第一协议可以是服务化接口协议或者应用编程接口协议（application programming interface）；第二协议可以是 NAS 协议或者其他非接入层协议。

804、接入网设备与终端交互消息。

在一种可能的实现方式中，接入网设备可以获知操作指令的内容，根据获知的该操作指令的内容执行相应的操作。例如接入网设备与终端交互消息以执行盘点操作、读操作或者写操作。

在另一种可能的实现方式中，接入网设备向终端转发操作指令，并与终端交互消息。

805、终端判断自身的注册状态。

步骤 805 是可选的，而非必要的。终端可以判断自身的注册状态。若终端未注册，则可以执行步骤 805 至步骤 816；若终端已注册，则可以执行步骤 817。若终端无判断其自身的注册状态的能力，或者无记录注册状态的能力，则终端需执行步骤 806。

806、终端向接入网设备发送注册请求消息。

注册请求消息（例如 registration request）中可包括终端的应用标识。在一种可能的实现方式中，注册请求消息中还可以包括终端标识、加密的终端标识、随机数、消息认证码（message authentication code, MAC）、校验值、token 中的一个或多个。注册请求消息可以包括多个随机数和消息认证码。终端标识可以理解为是用于唯一标识终端（或者是唯一标识终端这个物体或者设备）的标识。而加密的终端标识则可以理解为是将终端标识加密后的标识。本申请实施例中，终端一种可能的形态是标签，可将标签标识（tag identifier, TID）作为终端标识的示例，将加密的标签标识（concealed tag Identifier, CTID）作为加密的终端标识的示例。

在一种可能的实现方式中，终端采用预配置的密钥（或者称为预配置密钥）将终端标识加密后获取加密的终端标识。在另一种可能的实现方式中，可以向终端写入加密的终端标识。可能的方式有，操作请求方可以预先生成加密的终端标识，并在打印标签时或者在打印标签之后写入终端（例如标签）中。随机数和消息认证码可以用于鉴别或者认证消息在传输过程中是否有被篡改，或者可以用于网络认证终端是否为可信的终端。终端可生成随机数，并采用安全参数与随机数进行运算以获得消息认证码（也可以称为验证值或者 token）。其中，安全参数可以是密钥或者是 hash 算法。如果是密钥，则消息认证码可以是随机数利用该密钥加密后的值。如果是 hash 算法，则消息认证码可以是随机数经过该 hash 算法运算后得到的值。随机数与消息认证码可以包含于注册请求消息中。一种可能的实现方式中，注册请求消息为 NAS 消息（例如 NAS registration request）。

807、接入网设备选择支持 P-IoT 的 AMF。

步骤 807 是可选的。在一种可能的实现方式中，接入网设备可直接向任意 AMF 发送来自终端的注册请求消息，不必选择支持 P-IoT 的 AMF。

808、接入网设备向 AMF 发送来自终端的注册请求消息。

图 8 中的 AMF 为图 6A、图 6B 和图 7 中的第一核心网设备的示例，AMF 接收注册请求消息为第一核心网设备接收来自终端的第一消息的示例。

809、AMF 根据数量信息确定是否允许终端接入网络。

步骤 809 一种可能的实现方式如下：当操作请求方对应的终端中接入网络的终端数量小于或者等于数量阈值时，AMF 确定允许所述终端接入所述网络；否则，AMF 确定不允许所述终端接入所述网络。若 AMF 确定允许终端接入网络，则执行步骤 810；若 AMF 确定不允许终端接入网络，则执行步骤 816，即向终端发送注册拒绝消息。AMF 可统计并记录属于同一操作请求方的终端接入网络的数量。举例来说，AMF 在一个或多个终端通过认证或鉴权之后，更新该一个或多个终端所属的操作请求方已使用的终端的数量。AMF 可根据统计的操作请求方接入网络的终端的数量，确定该操作请求接入网络的终端的数量是否超过数量阈值。

在一种可能的实现方式中，AMF 根据数量信息确定允许终端接入网络之后，可以根据注册请求消息中的终端的应用标识获知需要选择支持 P-IoT 的 AUSF；然后，向该 AUSF 发送鉴权请求消息。一种可能的实现方式中，终端的应用标识不同于第三代合作伙伴（3rd Generation Partnership Project, 3GPP）终端的标识如用户隐藏标识（subscription concealed identifier, SUCI）、用户永久标识（subscription permanent identifier, SUPI）、5G 全球唯一临时标识（5G globally unique temporary identity, 5G-GUTI）、临时移动台标识（temporary mobile subscriber identity, TMSI）等，AMF 根据终端的应用标识获知该终端为无源物联终端或者为 P-IoT 终端，需要选择支持 P-IOT 的 AUSF。在一种可能的实现方式中，AMF 可以不选择支持 P-IoT 的 AUSF，而是向任意 AUSF 发送第一鉴权请求消息。

810、AMF 向 AUSF 发送第一鉴权请求消息。

第一鉴权请求消息（例如 Nausf_UEAuthentication_Authenticate Request）中可包括终端的应用标识。步骤 810 一种可能的实现方式如下：AMF 选择支持 P-IoT 的 AUSF，并向其选择的 AUSF 发送第一鉴权请求消息。步骤 810 另一种可能的实现方式如下：AMF 向任意 AUSF 发送第一鉴权请求消息。若终端发送的注册请求消息中包含终端标识、加密的终端标识、随机数、消息认证码中的一个或多个，则 AMF 向 AUSF 发送的第一鉴权请求消息中可以包括终端标识、加密的终端标识、随机数、消息认证码中的一个或多个。在一种可能的实现方式中，AMF 向 AUSF 发送指示信息 1（例如 P-IoT 指示信息），用于指示第一鉴权请求消息对应的鉴权为应用于无源物联网的鉴权，或者为对无源物联网终端的鉴权。举例来说，第一鉴权请求消息中可包含指示信息 1，该指示信息 1 指示该第一鉴权请求消息用于执行应用于无源物联网的鉴权或者用于对无源物联网终端的鉴权。又举例来说，AMF 通过第一鉴权请求消息之外的消息向 AUSF 发送指示信息 1，该指示信息 1 指示第一鉴权请求消息对应的鉴权为应用于无源物联网的鉴权，或者为用于对无源物联网终端的鉴权。一种可能的实现方式中，指示信息 1 用于指示该认证流程为单向认证、双向认证、终端对网络或者操作请求方的认证，或者，网络或者操作请求方对终端的认证中的一项或多项。

811、AUSF 选择支持 P-IoT 的 UDM。

在一种可能的实现方式中，AUSF 根据 AMF 发送的指示信息 1 或者根据终端的应用标识获知需要选择支持 P-IoT 的 UDM。一种可能的实现方式中，终端的应用标识不同于 3GPP 终端的标识如 SUCI、SUPI、5G-GUTI、TMSI 等，AUSF 根据终端的应用标识获知该终端为无源物联终端或者为 P-IoT 终端，需要选择支持 P-IOT 的 UDM。举例来说，第一鉴权请求消息中包含指示 AUSF 选择支持 P-IoT 的 UDM 的指示信息 1，AUSF 根据该指示信息 1 选择支持 P-IoT 的 UDM。

步骤 811 是可选的。在一种可能的实现方式中，AUSF 可以不选择 UDM，而是直接向任意 UDM 发送第二鉴权请求消息。

812、AUSF 向 UDM 发送第二鉴权请求消息。

第二鉴权请求消息(例如 Nudm_UEAuthentication GetRequest)中可包括终端的应用标识。如果 AMF 向 AUSF 发送的第一鉴权请求消息中包括终端标识、加密的终端标识、随机数、消息认证码中的一个或多个,则 AUSF 向 UDM 发送的第二鉴权请求消息中可以包括终端标识、加密的终端标识、随机数、消息认证码中的一个或多个。一种可能的实现方式, AUSF 向 UDM 发送的第二鉴权请求消息中包含指示信息 2 (例如 P-IoT 指示信息), 该指示信息 2 用于指示第二鉴权请求消息对应的鉴权为应用于无源物联网的鉴权, 或者为用于对无源物联网终端的鉴权。一种可能的实现方式中, 指示信息 2 用于指示该认证流程为单向认证、双向认证、终端对网络或者操作请求方的认证, 或者, 网络或者操作请求方对终端的认证中的一项或多项。

813、UDM 根据第二鉴权请求消息对终端进行认证。

在一种可能的实现方式中, 第二鉴权请求消息中包括终端的应用标识、随机数和消息认证码; UDM 可以根据终端的应用标识检索安全参数, 并根据安全参数和随机数验证消息认证码; 若一致, 则可以认为终端通过认证 (或者认为终端为可信的终端); 若不一致, 则可以认为终端不通过认证 (或者认为终端不为可信的终端)。安全参数可以是密钥或者是 hash 算法。如果是密钥, 则消息认证码可以是随机数利用该密钥加密后的值。如果是 hash 算法, 则消息认证码可以是随机数经过该 hash 算法运算后得到的值。在另一种可能的实现方式中, 若任意终端通过认证, 则 UDM 标记该应用标识已用; 若第二鉴权请求消息中的消息认证码通过验证且终端的应用标识未标记已用, 则认为终端的应用标识通过认证。

在一种可能的实现方式中, UDM 可以根据 AUSF 向 UDM 发送的指示信息 2 选择对终端进行认证的方法 (即选择适用于无源物联网或者无源物联网终端的鉴权方法)。

在一种可能的实现方式中, 若 AUSF 向 UDM 发送的第二鉴权请求消息中包括终端标识, 则 UDM 可以记录终端的应用标识与终端标识的对应关系。若 AUSF 向 UDM 发送的第二鉴权请求消息中包括加密的终端标识, 则 UDM 可以将加密的终端标识进行解密, 获取终端标识。UDM 可以记录终端的应用标识与终端标识的对应关系, 或者, 记录终端的应用标识与加密的终端标识的对应关系, 或者, 记录终端的应用标识、加密的终端标识、终端标识的对应关系。UDM 可以根据记录的终端应用标识或者对应关系统计已使用的终端数量。举例来说, 第二鉴权请求消息包括终端应用标识 1、终端标识 1; 若 UDM 已记录有终端应用标识 1 与终端标识 2 的对应关系, 则判定终端不通过认证, 并且统计的操作请求方已使用的终端数量保持不变。在该举例中, UDM 已记录有终端应用标识 1 与终端标识 2 的对应关系, 说明终端应用标识 1 已被其他终端使用, 即终端应用标识 1 被盗用。可见, UDM 可以根据记录的终端应用标识与终端标识 (或加密的终端标识) 的对应关系, 可确定终端应用标识是否被多个终端使用。在一种可能的实现方式中, UDM 在终端应用标识已被其他终端使用的情况下, 确定终端不通过认证。也就是说, 若终端的应用标识被盗用, 则确定终端不通过认证。又举例来说, 第二鉴权请求消息包括终端应用标识 1、终端标识 1; 若 UDM 已记录有终端应用标识 1, 则确定终端不通过认证, 并且统计的操作请求方已使用的终端数量保持不变。在该举例中, UDM 已记录有终端应用标识 1, 说明终端应用标识 1 已被其他终端使用, 即终端应用标识 1 被盗用。又举例来说, 第二鉴权请求消息包括终端应用标识 1、终端标识 1; 若 UDM 未记录有终端应用标识 1 与其他终端标识的对应关系且未记录有终端应用标识 1, 则 UDM 记录终端应用标识 1 和终端标识 1 的对应关系, 并将操作请求方已使用的终端的数量加一。在该举例中, UDM 未记录有终端应用标识 1 与其他终端标识的对应关系且未记录有终端应用标识 1, 说明

终端应用标识 1 未被使用。UDM 可以根据记录的终端应用标识或者对应关系统计已使用的终端数量。

814、UDM 向 AUSF 发送第一鉴权响应消息。

第一鉴权响应消息（例如 Nudm_UEAuthentication_Get Response）中可以包括认证结果，例如该认证结果可以包括认证通过或者认证不通过。认证通过是指终端通过认证。认证不通过是指终端未通过认证。

一种可能的实现方式中，若认证流程对应于网络对终端的单向认证，或者终端与网络之间的双向认证，则在 UDM 向 AUSF 发送的第一鉴权响应消息中，可以包括由 UDM 生成的随机数与 MAC 值（或者校验值或 token）。示例性的，MAC 值可以是 UDM 根据终端对应的安全参数与该随机数生成 MAC 值（或者校验值或 token）；或者，MAC 值可以是 UDM 根据终端发送的随机数以及 UDM 生成的随机数与终端对应的安全参数生成 MAC 值（或者校验值或 token）。该 MAC 值（或者校验值或 token）通过核心网向终端发送。终端根据预配置的安全参数以及 MAC 值（或者校验值或 token）解析随机数，并根据解析后的随机数认证网络是否为可信的网络。例如，当解析后的随机数包括终端生成的随机数时，网络为可信的网络。

815、AUSF 向 AMF 发送第二鉴权响应消息。

第二鉴权响应消息（例如 Nausf_UEAuthentication_Authenticate Response）中可以包括认证结果，例如该认证结果可以包括认证通过或者认证不通过。第二鉴权响应消息中包括的认证结果与第一鉴权响应消息中包括的认证结果相同。

816、AMF 向终端发送注册接受消息或者注册拒绝消息。

在一种可能的实现方式中，若终端通过认证，则 AMF 向终端发送注册接受消息（例如 registrationaccept）；若终端没有通过认证，则 AMF 向终端发送注册拒绝消息（例如 registrationreject）。在一种可能的实现方式中，注册接受消息或者注册拒绝消息可以是 NAS 消息（例如 NAS Registration Accept 或者 NAS Registration Reject）。若终端具有记录注册状态的能力，终端在接收到注册接受消息之后，可以记录其已注册，这样该终端就可判断自身的注册状态。也就是说，终端在未接收到注册接受消息之前，处于未注册状态，表示其未注册；终端在接收到注册接受消息之后，从未注册状态调整为注册状态，表示其已注册。

817、终端向 AMF 发送 NAS 消息。

当终端注册成功后，若终端需要向操作请求方（P-IoT AF 或者 P-IoT 服务器）发送信息（例如终端的应用标识），且终端发送的信息是通过控制面通道向 P-IoT AF 发送的，则可以通过 NAS 消息发给 AMF，由 AMF 向 P-IoT AF 发送（或者由 AMF 通过 NEF 向 P-IoT AF 发送），如图 8 所示。

在一种可能的实现方式中，若终端与 AMF 之间要采用 NAS 加密机制，则在执行步骤 817 之前，AMF 还需要与终端交互安全参数从而执行 NAS 安全机制。

在另一种可能的实现方式中，若终端发送的信息是通过用户面通道向 P-IoT 服务器发送的，则可以通过 RRC 消息发给接入网设备，由接入网设备通过用户面通道向 P-IoT 服务器发送（例如接入网设备通过 UPF 网元向 P-IoT 服务器发送）。

818、AMF 通过 NEF 向操作请求方发送来自终端的数据。

若终端通过控制面通道向 P-IoT AF 发送信息，则 AMF 可以通过 NEF 向 P-IoT AF 发送来自终端的数据。例如终端的数据可以包含终端的应用标识、存储于终端的存储区的信息。步骤 818 可替换为：AMF 通过 NEF 向操作请求方发送来自终端的数据。若终端通过用户面通道向 P-IoT 服务器发送信息，则终端可通过 RRC 消息发给接入网设备，由接入网设备通过用

户面通道向 P-IoT 服务器发送。

819、操作请求方向 UDM 发送失效信息。

失效信息指示一个或多个失效的终端。若操作请求方有一个或多个终端（例如标签）失效，需要替换失效的终端，则操作请求方可以（通过 NEF）向 UDM 发送失效终端的终端标识（或者加密的终端标识）。失效信息可以包含一个或多个失效的终端的终端标识（或者加密的终端标识）。

820、UDM 更新或者删除失效终端的标识信息。

失效终端的标识信息可以包括以下信息中的一项或多项：失效终端的应用标识、网络标识、终端标识、加密的终端标识、第二对应关系，所述第二对应关系包含失效终端的应用标识、网络标识、终端标识、加密的终端标识中的两个或两个以上的对应关系。

步骤 820 一种可能的实现方式如下：UDM 根据失效信息，更新或者删除失效终端的标识信息。举例来说，失效信息指示终端 1 和终端 5 失效，UDM 删除终端 1 的应用标识、网络标识、终端标识、加密的终端标识，或者，删除或更新终端 1 的应用标识、网络标识、终端标识、加密的终端标识中的两个或两个以上的对应关系以及删除终端 5 的应用标识、网络标识、终端标识、加密的终端标识中的两个或两个以上的对应关系。

可理解，步骤 806 至步骤 816 为终端注册或接入至网络（例如核心网）的步骤。

在一种可能的实现方式中，UDM 执行的步骤 813 和步骤 814 可由 AMF 实现，步骤 810 至步骤 815 可替换为：AMF 根据终端的应用标识检索安全参数，并根据安全参数和随机数验证消息认证码；若一致，则可以认为终端通过认证（或者认为终端为可信的终端）；若不一致，则可以认为终端不通过认证（或者认为终端不为可信的终端）。若 AMF 认为终端通过认证，则向终端发送注册接收消息；若 AMF 认为终端未通过认证，则向终端发送注册拒绝消息。

本申请实施例中，AMF 根据数量信息确定是否允许终端接入网络。若 AMF 根据数量信息确定不允许终端接入网络，则不必发送用于请求对该终端执行认证流程的消息，这样可以减少信令开销。

本申请实施例中，通过运营商在终端注册至网络之前，UDM 获知终端的应用标识，采用终端的应用标识来对终端进行认证。通过统计终端数量，可以防止一个终端的应用标识被多个终端使用，有利于网络进行标签管理与计费。

本申请实施例中，采用终端的应用标识进行接入管理。若需要对终端进行认证，还可以在打印标签时或者打印标签之后或者对标签进行初始化时对终端写入或者配置安全参数，从而在终端注册网络时，向网络发送用于认证的信息（例如随机数和消息认证码）。同时，还可以根据终端标识防止一个终端的应用标识被多个终端使用，有利于运营商对终端进行管理与计费。

下面结合具体实施例图 9，对上述实施例图 6A、图 6B 以及图 7 中的终端管理方法进行详细的说明。图 9 为本申请实施例提供的另一种终端管理方法交互流程图。图 9 以阅读器为接入网设备为例进行阐述，该方法也适用于阅读器为终端设备（例如 UE）的场景。如图 9 所示，该方法包括：

901、操作请求方获取终端的应用标识，AMF 获取数量信息和/或标识信息。

步骤 901 一种可能的实现方式如下：操作请求方和运营商的 BOSS 系统按照方式一分配终端的应用标识。图 9 中的 UDM 为图 4 中的第二核心网设备的一种示例，图 9 中的 UDM 可替换为 UDR 或者其他核心网网元。参阅图 4 中的方式一可知，按照方式一分配终端的应用标

识，操作请求方可获取终端的应用标识，第二核心网设备（对应于图 9 中的 UDM）没有获取终端的应用标识。图 9 的方法实施例中，运营商无预配置终端的应用标识，操作请求方分配终端的应用标识。在一种可能的实现方式中，UDM、操作请求方、运营商的 BOSS 系统执行方式一中的方法流程，这样 UDM 可配置放号数量，操作请求方可获取终端的应用标识，第一核心网设备（图 9 中的 AMF）可获取数量信息和/或标识信息。

902、终端初始化。

步骤 902 可参阅步骤 802。步骤 901 和步骤 902 是可选的。步骤 901 和步骤 902 可以在执行后续步骤之前预先完成的操作。

903、操作请求方向接入网设备发送操作指令。

步骤 903 可参阅步骤 803。

904、接入网设备与终端交互消息。

步骤 904 可参阅步骤 804。

905、终端判断自身的注册状态。

步骤 905 可参阅步骤 805。

906、终端向接入网设备发送注册请求消息。

步骤 906 可参阅步骤 806。

907、接入网设备可以选择支持 P-IoT 的 AMF。

步骤 907 可参阅步骤 807。

908、接入网设备向 AMF 发送来自终端的注册请求消息。

步骤 908 可参阅步骤 808。

909、AMF 根据数量信息确定是否允许终端接入网络。

步骤 909 可参阅步骤 809。若 AMF 确定允许终端接入网络，则执行步骤 910；若 AMF 确定不允许终端接入网络，则执行步骤 916，即向终端发送注册拒绝消息。

910、AMF 向 AUSF 发送第一鉴权请求消息。

步骤 910 可参阅步骤 810。步骤 910 和步骤 810 的区别在于，第一鉴权请求消息中未包括终端的应用标识。

第一鉴权请求消息（例如 Nausf_UEAuthentication_Authenticate Request）中可包括终端标识（或者加密的终端标识）。在一种可能的实现方式中，第一鉴权请求消息中包括终端标识、加密的终端标识、随机数、消息认证码中的一个或多个。

911、AUSF 选择支持 P-IoT 的 UDM。

步骤 911 可参阅步骤 811。

912、AUSF 向 UDM 发送第二鉴权请求消息。

步骤 912 可参阅步骤 812。第二鉴权请求消息（例如 Nudm_UEAuthentication GetRequest）中可包括终端标识（TID）或者加密的终端标识（CTID）。步骤 912 和步骤 812 的区别在于，第二鉴权请求消息中未包括终端的应用标识。如果 AMF 向 AUSF 发送的第一鉴权请求消息中包括终端标识、加密的终端标识、随机数、消息认证码中的一个或多个，则 AUSF 向 UDM 发送的第二鉴权请求消息中可以包括终端标识、加密的终端标识、随机数、消息认证码中的一个或多个。

913、UDM 根据第二鉴权请求消息对终端进行认证。

步骤 913 可参阅步骤 813。

在一种可能的实现方式中，第二鉴权请求消息中包括终端的终端标识（或加密的终端标

识)、随机数和消息认证码; UDM 可以根据终端的终端标识或者加密的终端标识中的明文部分检索安全参数, 并根据安全参数和随机数验证消息认证码; 若一致, 则可以认为终端通过认证 (或者认为终端为可信的终端); 若不一致, 则可以认为终端不通过认证 (或者认为终端不为可信的终端)。

914、UDM 向 AUSF 发送第一鉴权响应消息。

步骤 914 可参阅步骤 814。

915、AUSF 向 AMF 发送第二鉴权响应消息。

步骤 915 可参阅步骤 815。

916、AMF 向终端发送注册接受消息或者注册拒绝消息。

步骤 916 可参阅步骤 816。

917、终端向 AMF 发送 NAS 消息。

步骤 917 可参阅步骤 817。

918、AMF 通过 NEF 向操作请求方发送来自终端的数据。

步骤 918 可参阅步骤 818。

919、操作请求方向 UDM 发送失效信息。

步骤 919 可参阅步骤 819。

920、UDM 更新或者删除失效终端的标识信息。

步骤 920 可参阅步骤 820。

在一种可能的实现方式中, UDM 执行的步骤 913 和步骤 914 可由 AMF 实现, 步骤 910 至步骤 915 可替换为: AMF 根据终端的终端标识或者加密的终端标识中的明文部分检索安全参数, 并根据安全参数和随机数验证消息认证码; 若一致, 则可以认为终端通过认证 (或者认为终端为可信的终端); 若不一致, 则可以认为终端不通过认证 (或者认为终端不为可信的终端)。若 AMF 认为终端通过认证, 则向终端发送注册接收消息; 若 AMF 认为终端不通过认证, 则向终端发送注册拒绝消息。

本申请实施例中, UDM 在不获取终端的应用标识的情况下, 对终端进行接入管理和认证。相比图 8 中的方法流程, 可以满足企业或者用户或者操作请求方的隐私安全需求, 即网络不获取终端的应用标识。同理, 根据终端标识, 网络 (即 UDM) 可以统计使用的终端数量以及防止终端标识盗用的情况。

本申请实施例中, UDM 采用终端标识进行接入管理。若需要对终端进行认证, 还可以在打印标签时或者打印标签之后对终端写入安全参数, 从而在终端注册网络时, 向网络发送用于认证的信息 (例如随机数和消息认证码)。同时, 还可以根据终端标识防止一个终端标识被多个终端使用, 有利于运营商对终端进行管理与计费。

下面结合具体实施例图 10, 对上述实施例图 6A、图 6B 以及图 7 中的终端管理方法进行详细的说明。图 10 为本申请实施例提供的另一种终端管理方法交互流程图。图 10 以阅读器为接入网设备为例进行阐述, 该方法也适用于阅读器为终端设备 (例如 UE) 的场景。如图 10 所示, 该方法包括:

1001、操作请求方获取终端的应用标识, UDM 获取终端的网络标识。

步骤 1001 一种可能的实现方式如下: 操作请求方、UDM (或 UDR)、运营商的 BOSS 系统按照方式二分配终端的应用标识以及网络标识。参阅图 4 中的方式二可知, 按照方式二分配终端的应用标识和网络标识, 操作请求方可获取终端的应用标识, 第二核心网设备可获取终端的网络标识。图 10 中的 UDM 为图 4 中的第二核心网设备的一种示例, 图 10 中的 UDM

可替换为 UDR 或者其他核心网网元，图 10 中的 AMF 为图 4 中的第一核心网设备的一种示例。图 10 的方法实施例中，运营商无预配置终端的应用标识，操作请求方分配终端的应用标识。在一种可能的实现方式中，第二核心网设备（例如 UDM 或者 UDR）、第一核心网设备（例如 AMF）操作请求方、运营商的 BOSS 系统执行方式二中的方法流程，这样第二核心网设备可获取终端的网络标识，操作请求方可获取终端的应用标识，第一核心网设备（图 10 中的 AMF）可获取数量信息和/或标识信息。

1002、终端初始化。

步骤 1002 可参阅步骤 802。步骤 1001 和步骤 1002 是可选的。步骤 1001 和步骤 1002 可以是在执行后续步骤之前预先完成的操作。

1003、操作请求方向接入网设备发送操作指令。

步骤 1003 可参阅步骤 803。

1004、接入网设备与终端交互消息。

步骤 1004 可参阅步骤 804。

1005、终端判断自身的注册状态。

步骤 1005 可参阅步骤 805。

1006、终端向接入网设备发送注册请求消息。

步骤 1006 可参阅步骤 806。注册请求消息可包括终端的网络标识。在一种可能的实现方式中，注册请求消息中还可以包括终端的应用标识、终端标识（或者加密的终端标识）、随机数、消息认证码中的一个或多个。其中，终端的网络标识为运营商为终端分配的用于实现接入管理或者认证的标识。

1007、接入网设备选择支持 P-IoT 的 AMF。

步骤 1007 可参阅步骤 807。

1008、接入网设备向 AMF 发送来自终端的注册请求消息。

步骤 1008 可参阅步骤 808。

1009、AMF 根据数量信息确定是否允许终端接入网络。

步骤 1009 可参阅步骤 809。若 AMF 确定允许终端接入网络，则执行步骤 1010；若 AMF 确定不允许终端接入网络，则执行步骤 1016，即向终端发送注册拒绝消息。

1010、AMF 向 AUSF 发送第一鉴权请求消息。

步骤 1010 可参阅步骤 810。

第一鉴权请求消息（例如 Nausf_UEAuthentication_Authenticate Request）中可包括终端的网络标识。步骤 1010 和步骤 810 的一个区别在于，第一鉴权请求消息中包括终端的网络标识。

1011、AUSF 选择支持 P-IoT 的 UDM。

步骤 1011 可参阅步骤 811。

1012、AUSF 向 UDM 发送第二鉴权请求消息。

步骤 1012 可参阅步骤 812。第二鉴权请求消息（例如 Nudm_UEAuthentication GetRequest）中可包括终端的网络标识。步骤 1012 和步骤 812 的区别在于，第二鉴权请求消息中包括终端的网络标识。如果 AMF 向 AUSF 发送的第一鉴权请求消息中包括终端的网络标识、终端标识、加密的终端标识、随机数、消息认证码中的一个或多个，则 AUSF 向 UDM 发送的第二鉴权请求消息中可以包括终端的网络标识、终端标识、加密的终端标识、随机数、消息认证码中的一个或多个。

1013、UDM 根据第二鉴权请求消息对终端进行认证。

步骤 1013 可参阅步骤 813。步骤 1013 和步骤 813 的一个区别在于，UDM 对终端进行认证或鉴权的方式不同。在一种可能的实现方式中，第二鉴权请求消息中包括终端的网络标识、随机数和消息认证码；UDM 可以根据终端的网络标识检索安全参数，并根据安全参数和随机数验证消息认证码；若一致，则可以认为终端通过认证（或者认为终端为可信的终端）；若不一致，则可以认为终端不通过认证（或者认为终端不为可信的终端）。

一种可能的实现方式中，若 AUSF 向 UDM 发送的第二鉴权请求消息中包括终端网络标识、终端应用标识、终端标识、加密的终端标识，则 UDM 可以记录对应关系。该对应关系包括终端网络标识、终端应用标识、终端标识和加密的终端标识中的两个或两个以上之间的对应关系。若 AUSF 向 UDM 发送的第二鉴权请求消息中包括加密的终端标识，则 UDM 可以将加密的终端标识进行解密，获取终端标识。UDM 可以根据该对应关系统计操作请求方已使用的终端数量。

步骤 1013 一种可能的实现如下：UDM 根据第二鉴权请求消息中的终端网络标识，检索安全参数，并根据安全参数和随机数验证消息认证码；若验证通过，则记录终端网络标识，并统计操作请求方已使用的终端数量。举例来说，第二鉴权请求消息中包括终端 1 的终端网络标识 1，UDM 在终端 1 通过验证之后，检查是否记录有该终端网络标识 1；若未记录该终端网络标识 1，则将操作请求方已使用的终端数量加一；若记录有该终端应用标识 1，则保持操作请求方已使用的终端数量不变。

步骤 1013 另一种可能的实现如下：UDM 根据第二鉴权请求消息中的终端网络标识，检索安全参数，并根据安全参数和随机数验证消息认证码；若验证通过，则 UDM 可以记录该终端网络标识和该终端网络标识的对应关系，该对应关系包括终端网络标识与加密的终端标识、终端标识、终端的应用标识中的一个或多个的对应关系。UDM 可以根据该对应关系统计操作请求方使用的终端数量。举例来说，第二鉴权请求消息中包括终端 1 的终端网络标识 1，UDM 在终端 1 通过验证之后，检查是否记录有该终端网络标识 1 和终端网络标识 1 的对应关系；若未记录该终端网络标识 1 且未记录终端网络标识 1 的对应关系，则将操作请求方已使用的终端数量加一；若记录有该终端应用标识 1 或者终端应用标识 1 的对应关系，则保持操作请求方已使用的终端数量不变。

1014、UDM 向 AUSF 发送第一鉴权响应消息。

步骤 1014 可参阅步骤 814。

1015、AUSF 向 AMF 发送第二鉴权响应消息。

步骤 1015 可参阅步骤 815。

1016、AMF 向终端发送注册接受消息或者注册拒绝消息。

步骤 1016 可参阅步骤 816。

1017、终端向 AMF 发送 NAS 消息。

步骤 1017 可参阅步骤 817。

1018、AMF 通过 NEF 向操作请求方发送来自终端的数据。

步骤 1018 可参阅步骤 818。

1019、操作请求方向 UDM 发送失效信息。

步骤 1019 可参阅步骤 819。

1020、UDM 更新或者删除失效终端的标识信息。

步骤 1020 可参阅步骤 820。

在一种可能的实现方式中，UDM 执行的步骤 1013 和步骤 1014 可由 AMF 实现，步骤 1010

至步骤 1015 可替换为：AMF 根据终端的网络标识检索安全参数，并根据安全参数和随机数验证消息认证码；若一致，则可以认为终端通过认证（或者认为终端为可信的终端）；若不一致，则可以认为终端不通过认证（或者认为终端不为可信的终端）。若 AMF 认为终端通过认证，则向终端发送注册接收消息；若 AMF 认为终端不通过认证，则向终端发送注册拒绝消息。

本申请实施例中，核心网能够在不获取终端的应用标识的情况下，对终端进行接入管理和认证。相比图 8 中的方法流程，可以满足企业的隐私安全需求，即网络不获取终端的应用标识。相比图 9 中的方法流程，网络采用终端的网络标识对终端进行接入管理和认证。该机制可以满足企业不将数据上报网络的需求（例如企业不上报终端的应用标识和终端标识的需求）。同理，根据终端标识，网络可以统计使用的终端数量以及防止终端标识盗用的情况。

下面结合具体实施例图 11，对上述实施例图 6A、图 6B 以及图 7 中的终端管理方法进行详细的说明。图 11 为本申请实施例提供的另一种终端管理方法交互流程图。图 11 以阅读器为接入网设备为例进行阐述，该方法也适用于阅读器为终端设备（例如 UE）的场景。如图 11 所示，该方法包括：

1101、操作请求方获取终端的应用标识，UDM 配置放号数量。

步骤 1001 一种可能的实现方式如下：操作请求方、第二核心网设备（例如 UDM 或者 UDR）、第一核心网设备（图 11 中的 AMF）、运营商的 BOSS 系统执行方式一的方法流程。参阅图 4 中的方式一可知，执行方式一的方法流程，操作请求方可获取终端的应用标识，第二核心网设备可配置放号数量，第一核心网设备（图 8 中的 AMF）可获取数量信息和/或标识信息。图 11 中的 UDM 为图 4 中的第二核心网设备的一种示例，图 11 中的 UDM 可替换为 UDR 或者其他核心网网元，图 11 中的 AMF 为图 4 中的第一核心网设备的一种示例。图 11 的方法实施例中，运营商无预配置终端的应用标识，操作请求方分配终端的应用标识。

1102、终端初始化。

步骤 1102 可参阅步骤 802。步骤 1101 和步骤 1102 是可选的。步骤 1101 和步骤 1102 可以是在执行后续步骤之前预先完成的操作。

1103、AMF 向接入网设备发送第一指令。

第一指令（可称为在线签约指令）用于执行在线签约或者用于触发终端执行在线签约。或者，第一指令指示终端执行在线签约。

1104、接入网设备接与终端交互消息。

一种可能的实现方式，接入网设备获知第一指令为在线签约指令，接入网设备根据该第一指令与终端交互消息，例如通知或者触发终端执行在线签约。另一种可能的实现方式，接入网设备向终端转发第一指令，接入网设备与终端交互消息，通知或者触发终端执行在线签约。

1105、终端判断签约状态。

在一种可能的实现方式中，终端接收接入网设备转发的第一指令后，可以判断自己的签约状态；若终端为未签约的状态或者未获取签约数据，则终端执行步骤 1106；若终端已获取签约数据或者终端为已签约的状态，则可以跳过步骤 1106 至步骤 1116。签约数据可包括终端的标识信息和/或认证信息。标识信息可包括终端网络标识。当终端获取到核心网设备（例如 UDM）分配的标识信息和/或认证信息之后，该终端从未签约的状态调整为己签约的状态。或者说，终端未获取到核心网设备（例如 UDM）分配的标识信息和/或认证信息之前，该终端未获取签约数据；终端获取到核心网设备（例如 UDM）分配的标识信息和/或认证信息之后，

该终端获取到签约数据。

在一种可能的实现方式中,终端通过与接入网设备交互消息获知需要执行在线签约之后,可以判断自己的签约状态;若终端为未签约的状态或者未获取签约数据,则终端执行步骤 1106;若终端已获取签约数据或者终端为已签约的状态,则可以跳过步骤 1106 至步骤 1116。

步骤 1105 是可选的。在一种可能的实现方式中,终端可不执行步骤 1105,而是在执行步骤 1104 之后,直接执行步骤 1106。

1106、终端向接入网设备发送第一请求消息。

第一请求消息(例如可以是在线签约请求消息或者注册请求消息,但该注册请求消息是用于指示注册网络执行在线签约),该第一请求消息用于请求执行在线签约。

在一种可能的实现方式中,第一请求消息可以包括企业标识(或者操作请求方标识或者用户标识)、一个为空集的终端的网络标识(即空的终端网络标识)、随机数、消息认证码中的一个或多个。其中,消息认证码可以是将随机数加密或者经过哈希算法后获得的值。在一种可能的实现方式中,若网络服务多个企业或者用户或者操作请求方,则网络可以根据终端发送的企业标识(或者用户标识或者操作请求方标识)分配网络标识。若网络只服务一个企业(或者用户或者操作请求方),则终端可以不发送企业标识(或者用户标识或者操作请求方标识)。另一种可能的实现方式中,终端发送的第一请求消息中包括随机数和消息认证码;网络可以在终端通过认证后,为终端分配终端的网络标识。

接入网设备选择支持 P-IoT 的 AMF。

接入网设备可以选择一个支持 P-IoT 在线签约的 AMF。支持 P-IoT 在线签约的 AMF 具备执行图 11 中的 AMF 执行的操作的功能。

1107、接入网设备选择支持 P-IoT 的 AMF。

接入网设备可以选择一个支持 P-IoT 在线签约的 AMF。支持 P-IoT 在线签约的 AMF 具备执行图 11 中的 AMF 执行的操作的功能。

1108、接入网设备向 AMF 发送来自终端的第一请求消息。

第一请求消息中可以包括企业标识(或者用户标识或者操作请求方标识)、空的终端网络标识、随机数、消息认证码中的一个或多个。

1109、AMF 根据数量信息确定是否允许终端接入网络。

若 AMF 确定允许终端接入网络,则执行步骤 1110;若 AMF 确定不允许终端接入网络,则执行步骤 1116,即向终端发送注册拒绝消息。

1110、AMF 向 AUSF 发送第二请求消息。

第二请求消息(例如可以是鉴权消息、Nausf_UEAuthentication_Authenticate Request)用于请求核心网设备(例如 UDM)执行在线签约。若终端发送的第一请求消息包括企业标识(或者用户标识或者操作请求方标识)、空的终端网络标识、随机数、消息认证码中的一个或多个,则 AMF 向 AUSF 发送的第二请求消息中可以包括企业标识(或者用户标识或者操作请求方标识)、空的终端网络标识、随机数、消息认证码中的一个或多个。在一种可能的实现方式中,AMF 向 AUSF 发送指示信息 3(例如 P-IoT 指示信息),用于指示为在线签约,或者,为无源物联网的在线签约,或者,为无源物联网终端的在线签约。AMF 向 AUSF 发送的指示信息 3 可包含于第二请求消息,也可以包含于其他消息。

AMF 向 AUSF 发送第二请求消息之前,可选择支持 P-IoT(或者支持 P-IoT 在线签约)的 AUSF。支持 P-IoT(或者支持 P-IoT 在线签约)的 AUSF 具备执行图 11 中的 AUSF 执行的操作的功能。在一种可能的实现方式中,AMF 可以根据第一请求消息或者根据接入网设备

获知需要选择支持 P-IoT（或者支持 P-IoT 在线签约）的 AUSF。一种可能的实现方式，第一请求消息的类型为特定的类型，AMF 可以根据第一请求消息的消息类型确定需要选择支持 P-IoT（或者支持 P-IoT 在线签约）的 AUSF；另一种可能的实现方式，接入网设备具有支持 P-IoT 能力的接入网设备，AMF 根据接入网设备或者根据接入网设备的能力获知需要选择支持 P-IoT（或者支持 P-IoT 在线签约）的 AUSF。

1111、AUSF 选择 UDM。

AUSF 选择支持 P-IoT（或者支持 P-IoT 在线签约）的 UDM。支持 P-IoT（或者支持 P-IoT 在线签约）的 UDM 具备执行图 11 中的 UDM 执行的操作的功能。一种可能的实现方式，AUSF 根据 AMF 发送的指示信息 3 或者根据第二请求消息获知需要选择支持 P-IoT（或者支持 P-IoT 在线签约）的 UDM。

1112、AUSF 向 UDM 发送第三请求消息。

第三请求消息（例如可以是鉴权请求消息、Nudm_UEAuthentication GetRequest）用于请求对终端做认证或鉴权。第三请求消息中可以包括企业标识（或者用户标识或者操作请求方标识）、空的终端网络标识、随机数、消息认证码中的一个或多个。举例来说，AMF 向 AUSF 发送的第二请求消息中包括企业标识（或者用户标识或者操作请求方标识）、空的终端网络标识、随机数、消息认证码中的一个或多个，AUSF 向 UDM 发送的第三请求消息中可以包括企业标识（或者用户标识或者操作请求方标识）、空的终端网络标识、随机数、消息认证码中的一个或多个。在一种可能的实现方式中，AUSF 向 UDM 发送指示信息 4（例如 P-IoT 指示信息），用于指示为在线签约，或者，为无源物联网的在线签约，或者，为无源物联网终端的在线签约。AUSF 向 UDM 发送的指示信息 4 可包含于第三请求消息，也可以包含于其他消息。

1113、UDM 根据企业标识（或者用户标识或者操作请求方标识）执行认证，并在认证通过后分配终端的网络标识。

UDM 在终端通过认证之后，还可为终端分配安全参数，该安全参数用于认证该终端。UDM 还可记录为终端分配的网络标识和安全参数的对应关系，以便根据该终端的网络标识检索该安全参数。举例来说，终端可利用 UDM 为其分配的安全参数处理随机数以得到消息认证码；该终端发送的注册请求消息中可包含该随机数和该消息认证码；UDM 可根据该终端的网络标识检索安全参数，并利用该安全参数验证该消息认证码。

在一种可能的实现方式中，第三请求消息中包括企业标识（或者用户标识或者操作请求方标识）、空的终端网络标识、随机数、消息认证码中的一个或多个，则 UDM 根据企业标识（或者用户标识或者操作请求方标识）检索安全参数。UDM 根据检索的安全参数和随机数验证消息认证码；若一致，则可以认为终端通过认证（或者认为终端为可信的终端，或者认为终端来自可信的操作请求方）。UDM 根据安全参数和随机数验证消息认证码；若不一致，则可以认为终端不通过认证（或者认为终端不为可信的终端）。在一种可能的实现方式中，UDM 可以根据 AUSF 向 UDM 发送的指示信息 4 选择鉴权方法（即选择适用于在线签约，或者，适用于无源物联网在线签约，或者，适用于无源物联网终端的在线签约方法）。

在一种可能的实现方式中，UDM 分配终端的网络标识之后，UDM 可以记录该终端的网络标识与企业标识（或者用户标识或者操作请求方标识）的对应关系。可选的，UDM 可以根据终端的网络标识或者该对应关系统计操作请求方使用的终端数量，UDM 也可以在后续终端注册的时候统计操作请求方使用的终端数量。UDM 可以根据终端的网络标识或者该对应关系统计使用的终端数量可参阅图 10 中的步骤 1013。

1114、UDM 向 AUSF 发送第一响应消息。

第一响应消息（例如可以是鉴权响应消息、Nudm_UEAuthentication_Get Response）中可以包括认证结果。该认证结果例如可以包括认证通过或者认证不通过。若第一响应消息包括的认证结果为认证通过，则该第一响应消息还可包括 UDM 为终端分配的网络标识和安全参数。若第一响应消息包括的认证结果为认证通过，则该第一响应消息可仅包括该认证结果。

1115、AUSF 向 AMF 发送第二响应消息。

第二响应消息（例如可以是鉴权响应消息、Nausf_UEAuthentication_Authenticate Response）中可以包括认证结果，例如可以包括认证通过或者认证不通过。若第二响应消息包括的认证结果为认证通过，则该第二响应消息还可包括 UDM 为终端分配的网络标识和安全参数。

1116、AMF 向终端发送注册接受消息或者注册拒绝消息。

注册接受消息（或者称为在线签约接收消息、在线签约完成消息）可包括为终端分配的网络标识。注册接收消息还可包括安全参数。注册接受消息指示终端的在线签约通过。或者说，注册接受消息指示终端完成在线签约。注册拒绝消息（或者称为在线签约不通过消息、在线签约失败消息等）指示终端的在线签约不通过。或者说，注册拒绝消息指示终端的在线签约失败或未完成。

一种可能的实现方式中，若终端通过认证，则 AMF 向终端发送在线签约接受消息，或者，在线签约完成消息，或者，注册接受消息（例如 registrationaccept）。在线签约接受消息、在线签约完成消息、注册接受消息均包含为终端分配的网络标识。若终端没有通过认证，则 AMF 向终端发送在线签约失败消息，或者，在线签约不通过消息，或者，注册拒绝消息（例如 Registration Reject）。在线签约失败消息、在线签约不通过消息、注册拒绝消息均指示在线签约不通过或终端没有通过认证。

一种可能的实现方式中，注册接受消息或者注册拒绝消息可以是 NAS 消息或者包含于 NAS 消息中发送（例如 NAS Registration Accept、NAS Onboarding Accept、NAS Onboarding complete、NAS Registration Reject、NAS Onboarding Reject、NAS Onboarding failed）。

1117、操作请求方向接入网设备发送操作指令。

步骤 1003 可参阅步骤 803。

操作指令中可以包括一个或多个终端的应用标识。操作请求方可以通过控制面通道或者用户面通道向接入网设备发送操作指令。图中以操作请求方通过控制面通道向接入网设备发送操作指令为例展示。操作请求方（例如 P-IoT AF）可以通过 NEF、AMF 向接入网设备发送操作指令，或者操作请求方可以通过 AMF 向接入网设备发送操作指令。若通过用户面通道发送，则操作请求方（P-IoT 服务器）可以通过 UPF 向接入网设备发送操作指令。

1118、接入网设备与终端交互消息。

步骤 1118 可参阅步骤 804。

1119、终端判断自身的注册状态。

步骤 1119 可参阅步骤 805。

1120、终端向 AMF 发送注册请求消息。

注册请求消息可包括终端的网络标识。一种可能的实现方式中，注册请求消息中还可以包括终端的应用标识、终端标识（或者加密的终端标识）、随机数、消息认证码中的一个或多个。其中，终端的网络标识为运营商为终端分配的用于接入管理或者认证的标识。

步骤 1120 可替换为：终端通过接入网设备向 AMF 发送注册请求消息。在一种可能的实现方式中，注册请求消息为 NAS 消息（例如 NAS Registration Request）；终端向接入网设备发送注册请求消息，该接入网设备可以选择支持 P-IoT 的 AMF，并向选择的 AMF 发送来自

终端的注册请求消息。

1121、AMF 向 AUSF 发送第一鉴权请求消息。

步骤 1121 可参阅步骤 810。

第一鉴权请求消息（例如 Nausf_UEAuthentication_Authenticate Request）中可包括终端的网络标识。第一鉴权请求消息用于请求对终端进行认证或鉴权。若终端发送的注册请求消息中包括终端的应用标识、终端标识（或者加密的终端标识）、随机数、消息认证码中的一个或多个，则 AMF 向 AUSF 发送的第一鉴权请求消息中可以包括终端的应用标识、终端标识（或者加密的终端标识）、随机数、消息认证码中的一个或多个。在一种可能的实现方式，AMF 向 AUSF 发送指示信息 1（例如 P-IoT 指示信息），用于指示该鉴权为无源物联网的鉴权，或者为无源物联网终端的鉴权。

可选的，AMF 选择支持 P-IoT 的 AUSF。在一种可能的实现方式中，AMF 可以根据注册请求消息中的终端的网络标识或者根据指示信息 1 获知需要选择支持 P-IoT 的 AUSF。一种可能的实现方式中，终端的网络标识不同于 3GPP 终端的标识如 SUCI、SUPI、5G-GUTI、TMSI 等，AMF 根据终端的应用标识获知该终端为无源物联终端或者为 P-IoT 终端，需要选择支持 P-IOT 的 AUSF。

1122、AUSF 向 UDM 发送第二鉴权请求消息。

步骤 1122 可参阅步骤 812。

第二鉴权请求消息（例如 Nausf_UEAuthentication_Authenticate Request）中可包括终端的网络标识。第二鉴权请求消息用于请求对终端进行认证或鉴权。如果 AMF 向 AUSF 发送的第一鉴权请求消息中包括终端的应用标识、终端标识（或者加密的终端标识）、随机数、消息认证码中的一个或多个，则 AUSF 向 UDM 发送的第二鉴权请求消息中可以包括终端的应用标识、终端标识（或者加密的终端标识）、随机数、消息认证码中的一个或多个。一种可能的实现方式，AMF 向 AUSF 发送指示信息 2（例如 P-IoT 指示信息），用于指示该鉴权为应用于无源物联网的鉴权，或者为无源物联网终端的鉴权。一种可能的实现方式中，指示信息 2 用于指示该认证流程为单向认证、双向认证、终端对网络或者操作请求方的认证，或者，网络或者操作请求方对终端的认证中的一项或多项。

可选的，AUSF 选择支持 P-IoT 的 UDM。在一种可能的实现方式中，AUSF 根据 AMF 发送的指示信息或者根据终端的网络标识获知需要选择支持 P-IoT 的 UDM。

1123、UDM 根据第二鉴权请求消息对终端进行认证。

步骤 1123 可参阅步骤 1013。

1124、UDM 向 AUSF 发送第一鉴权响应消息。

步骤 1124 可参阅步骤 814。

1125、AUSF 向 AMF 发送第二鉴权响应消息。

步骤 1125 可参阅步骤 815。

1126、AMF 向终端发送注册接受消息或者注册拒绝消息。

步骤 1126 可参阅步骤 816。

1127、终端向 AMF 发送 NAS 消息。

步骤 1127 可参阅步骤 817。

1128、AMF 通过 NEF 向操作请求方发送来自终端的数据。

步骤 1128 可参阅步骤 818。

1129、操作请求方向 UDM 发送失效信息。

步骤 1129 可参阅步骤 819。

1130、UDM 更新或者删除失效终端的标识信息。

步骤 1130 可参阅步骤 820。

在一种可能的实现方式中,UDM 执行的步骤 1113 和步骤 1114 可由 AMF 实现,步骤 1110 至步骤 1115 可替换为:AMF 根据企业标识执行认证,并在认证通过后分配终端的网络标识。应理解,若终端通过认证,则向终端发送注册接受消息;否则,向终端发送注册拒绝消息。

图 11 的方法流程中,步骤 1101 至步骤 1116 为执行在线签约以获取终端的网络标识的流程,步骤 1107 至步骤 1130 为执行注册流程的步骤。

图 11 中的方法流程与图 10 中的方法流程相比,终端的网络标识是通过在线签约流程向终端发送的。其有益效果在于,终端的网络标识可以无需提前配置于企业中,可以防止企业将一个终端的网络标识用于多个终端中,即终端获取终端的网络标识可以流程化,更安全。另外,AMF 根据数量信息确定是否允许终端接入网络。若操作请求方对应的终端接入网络的终端设备小于或等于数量阈值,则不必为请求执行在线签约的终端(属于该操作请求方)分配网络标识,这样可以减少不必要的操作。

图 12 示出了一种通信装置 1200 的结构示意图。该通信装置 1200 可以对应实现上述各个方法实施例中由核心网设备(例如图 4 和图 6B 中的第一核心网设备和第二核心网设备)实现的功能或者步骤,也可实现上述各个方法实施例中由操作请求方实现的功能或者步骤。该通信装置可以包括处理模块 1210 和收发模块 1220。可选的,还可以包括存储单元,该存储单元可以用于存储指令(代码或者程序)和/或数据。处理模块 1210 和收发模块 1220 可以与该存储单元耦合,例如,处理模块 1210 可以读取存储单元中的指令(代码或者程序)和/或数据,以实现相应的方法。上述各个单元可以独立设置,也可以部分或者全部集成。例如收发模块 1220 可包括发送模块和接收模块。

在一些可能的实施方式中,通信装置 1200 能够对应实现上述方法实施例中第一核心网设备的操作和功能。例如通信装置 1200 可以为第一核心网设备,也可以为应用于第一核心网设备中的部件(例如芯片或者电路)。收发模块 1220 例如可以用于执行图 4、图 6A、图 6B、图 7、图 8、图 9、图 10、图 11 的实施例中的由第一核心网设备或 AMF 所执行的全部接收或发送操作,例如图 4 所示的实施例中的步骤 405、步骤 417、步骤 427、步骤 435 以及图 6A 所示实施例中的步骤 601A、步骤 602A,和/或用于支持本文所描述的技术的其它过程。处理模块 1210 用于执行图 6A、图 6B、图 7、图 8、图 9、图 10、图 11 的实施例中的由第一核心网设备或 AMF 所执行的除了收发操作之外的全部操作,例如图 6A 所示的实施例中的步骤 602A,图 7 所示的实施例中的步骤 702,图 8 所示的实施例中的步骤 809。

在一些可能的实施方式中,通信装置 1200 能够对应实现上述方法实施例中第二核心网设备的操作和功能。例如通信装置 1200 可以为第二核心网设备,也可以为应用于第二核心网设备中的部件(例如芯片或者电路)。收发模块 1220 例如可以用于执行图 4、图 6B、图 8、图 9、图 10、图 11 的实施例中的由第二核心网设备所执行的全部接收或发送操作,例如图 4 所示的实施例中的步骤 401、步骤 405、步骤 411、步骤 417、步骤 421、步骤 425、步骤 427、步骤 432、步骤 435,图 6B 所示实施例中的步骤 602B、步骤 603B,图 8 所示实施例中的步骤 812、步骤 814、步骤 819,和/或用于支持本文所描述的技术的其它过程。处理模块 1210 用于执行图 4、图 8、图 9、图 10、图 11 的实施例中的由第二核心网设备所执行的除了收发操作之外的全部操作,例如图 4 所示的实施例中的步骤 402、步骤 412、步骤 415、步骤 422、步骤 426、步骤 433,以及图 8 所示的实施例中的步骤 813 和步骤 820。

在一些可能的实施方式中，通信装置 1200 能够对应实现上述方法实施例中操作请求方的操作和功能。例如通信装置 1200 可以为操作请求方，也可以为应用于操作请求方中的部件（例如芯片或者电路）。收发模块 1220 例如可以用于执行图 4、图 5、图 6A、图 6B、图 8、图 9、图 10、图 11 的实施例中的由操作请求方所执行的全部接收或发送操作，例如图 4 所示的实施例中的步骤 403、步骤 413、步骤 416、步骤 423、步骤 425、步骤 434，以及图 5 所示实施例中的步骤 501，图 6A 所示实施例中的步骤 602A，图 8 所示实施例中的步骤 803、步骤 818、步骤 819，和/或用于支持本文所描述的技术的其它过程。处理模块 1210 用于执行图 4、图 5、图 8、图 9、图 10、图 11 的实施例中的由操作请求方所执行的除了收发操作之外的全部操作，例如图 4 所示的实施例中的步骤 401、步骤 414、步骤 424，图 5 所示的实施例中的步骤 502，以及图 8 所示的实施例中的步骤 801。

图 13 为本申请实施例提供的另一种通信装置 130 的结构示意图。图 13 中的通信装置可以是上述第一核心网设备。图 13 中的通信装置可以是上述第二核心网设备。图 13 中的通信装置可以是上述操作请求方。

如图 13 所示，该通信装置 130 包括至少一个处理器 1320 和收发器 1310。

在本申请的另一些实施例中，处理器 1320 和收发器 1310 可以用于执行上述第一核心网设备执行的功能或操作等。处理器 1320 例如可执行如下一项多项操作：图 6A 所示的实施例中的步骤 602A，图 7 所示的实施例中的步骤 702，图 8 所示的实施例中的步骤 809。收发器 1310 例如可执行如下一项或多项操作：图 4 所示的实施例中的步骤 405、步骤 417、步骤 427、步骤 435，图 6A 所示实施例中的步骤 601A、步骤 602A。

在本申请的一些实施例中，处理器 1320 和收发器 1310 可以用于执行上述第二核心网设备执行的功能或操作等。处理器 1320 例如可执行如下一项多项操作：图 4 所示的实施例中的步骤 402、步骤 412、步骤 415、步骤 422、步骤 426、步骤 433，以及图 8 所示的实施例中的步骤 813 和步骤 820。收发器 1310 例如可执行如下一项或多项操作：图 4 所示的实施例中的步骤 401、步骤 405、步骤 411、步骤 417、步骤 421、步骤 425、步骤 427、步骤 432、步骤 435，图 6B 所示实施例中的步骤 602B、步骤 603B，图 8 所示实施例中的步骤 812、步骤 814、步骤 819。

在本申请的一些实施例中，处理器 1320 和收发器 1310 可以用于执行上述操作请求方执行的功能或操作等。处理器 1320 例如可执行如下一项或多项操作：图 4 所示的实施例中的步骤 401、步骤 414、步骤 424，图 5 所示的实施例中的步骤 502，以及图 8 所示的实施例中的步骤 801。收发器 1310 可执行如下一项或多项操作：图 4 所示的实施例中的步骤 403、步骤 413、步骤 416、步骤 423、步骤 425、步骤 434，以及图 5 所示实施例中的步骤 501，图 6A 所示实施例中的步骤 602A，图 8 所示实施例中的步骤 803、步骤 818、步骤 819。

收发器 1310 用于通过传输介质和其他设备/装置进行通信。处理器 1320 利用收发器 1310 收发数据和/或信令，并用于实现上述方法实施例中的方法。处理器 1320 可实现处理模块 1210 的功能，收发器 1310 可实现收发模块 1220 的功能。

可选的，通信装置 130 还可以包括至少一个存储器 1330，用于存储程序指令和/或数据。存储器 1330 和处理器 1320 耦合。本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。处理器 1320 可能和存储器 1330 协同操作。处理器 1320 可能执行存储器 1330 中存储的程序指令。该至少一个存储器中的至少一个可以包括于处理器中。

本申请实施例中不限定上述收发器 1310、处理器 1320 以及存储器 1330 之间的具体连接

介质。本申请实施例在图 13 中以存储器 1330、处理器 1320 以及收发器 1310 之间通过总线 1340 连接，总线在图 13 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。该总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 13 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

在本申请实施例中，处理器可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件，可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

图 14 为本申请实施例提供的另一种通信装置 140 的结构示意图。如图 14 所示，图 14 所示的通信装置包括逻辑电路 1401 和接口 1402。图 12 中的处理模块 1210 可以用逻辑电路 1401 实现，图 12 中的收发模块 1220 可以用接口 1402 实现。其中，该逻辑电路 1401 可以为芯片、处理电路、集成电路或片上系统（system on chip, SoC）芯片等，接口 1402 可以为通信接口、输入输出接口等。本申请实施例中，逻辑电路和接口还可以相互耦合。对于逻辑电路和接口的具体连接方式，本申请实施例不作限定。

在本申请的一些实施例中，该逻辑电路和接口可用于执行上述第一核心网设备执行的功能或操作等。

在本申请的另一些实施例中，该逻辑电路和接口可用于执行上述第二核心网设备执行的功能或操作等。

在本申请的另一些实施例中，该逻辑电路和接口可用于执行上述操作请求方执行的功能或操作等。

在本申请的一些实施例中，该逻辑电路和接口可用于执行上述接入网设备 2 执行的功能或操作等。

本申请还提供一种计算机可读存储介质，该计算机可读存储介质中存储有计算机代码，当计算机代码在计算机上运行时，使得计算机执行上述实施例的方法。

本申请还提供一种计算机程序产品，该计算机程序产品包括计算机代码或计算机程序，当该计算机代码或计算机程序在计算机上运行时，使得上述实施例中的认证鉴权方法被执行。

本申请还提供一种通信系统，包括终端设备、接入网设备 1、第二接入网设备以及第三接入网设备。

本申请还提供一种通信系统，包括终端设备、接入网设备 2。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以上述权利要求的保护范围为准。

权 利 要 求 书

1.一种终端管理方法，其特征在于，包括：

第一核心网设备接收来自终端的第一消息，所述第一消息用于请求接入网络；

所述第一核心网设备在根据数量信息确定允许所述终端接入所述网络时，向所述终端所属的操作请求方发送第二消息；所述数量信息包括所述操作请求方允许使用的终端数量，所述第二消息包含第一标识信息，所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

2.根据权利要求1所述的方法，其特征在于，所述根据数量信息确定允许所述终端接入所述网络包括：

当所述操作请求方对应的终端中接入所述网络的终端数量小于数量阈值时，所述第一核心网设备确定允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

3.根据权利要求1或2所述的方法，其特征在于，所述方法还包括：

所述第一核心网设备在根据所述数量信息确定不允许所述终端接入所述网络的情况下，向所述终端发送第三消息；所述第三消息指示拒绝所述终端接入所述网络。

4.根据权利要求3所述的方法，其特征在于，所述根据所述数量信息确定不允许所述终端接入所述网络包括：

当所述操作请求方对应的终端中接入所述网络的终端数量大于或等于数量阈值时，所述第一核心网设备确定不允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

5.根据权利要求1至4任一项所述的方法，其特征在于，所述方法还包括：

所述第一核心网设备向第二核心网设备发送第四消息；所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息和所述认证信息用于执行所述认证流程；所述第二标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

6.根据权利要求5所述的方法，其特征在于，所述第二消息还包括指示信息，所述指示信息指示所述认证流程为单向认证、双向认证、所述终端对所述网络或者所述操作请求方的单向认证、所述网络或者所述操作请求方对所述终端的单向认证中的任一种。

7.根据权利要求1至4任一项所述的方法，其特征在于，所述方法还包括：

所述第一核心网设备根据所述第一消息对所述终端执行认证流程；所述第一消息包括第三标识信息和认证信息，所述第三标识信息和所述认证信息用于执行所述认证流程；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

8.根据权利要求1至7任一项所述的方法，其特征在于，所述方法还包括：

所述第一核心网设备根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

9.根据权利要求5或6或7所述的方法，其特征在于，所述方法还包括：

所述第一核心网设备接收第五消息；

所述第一核心网设备向所述终端，发送第六消息；所述第五消息指示所述认证流程通过，

所述第六消息指示接受所述终端接入所述网络；或者，所述第五消息指示所述认证流程不通过，所述第六消息指示拒绝所述终端接入所述网络。

10.根据权利要求 1 至 9 任一项所述的方法，其特征在于，所述方法还包括：

所述核心网设备获取所述数量信息和/或所述第一标识信息。

11.一种通信装置，其特征在于，包括：

收发模块，用于接收来自终端的第一消息，所述第一消息用于请求接入网络；

所述收发模块，还用于在处理模块根据数量信息确定允许所述终端接入所述网络时，向所述终端所属的操作请求方发送第二消息；所述数量信息包括所述操作请求方允许使用的终端数量，所述第二消息包含第一标识信息，所述第一标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

12.根据权利要求 11 所述的装置，其特征在于，

所述处理模块，具体用于当所述操作请求方对应的终端中接入所述网络的终端数量小于数量阈值时，确定允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

13.根据权利要求 11 或 12 所述的装置，其特征在于，

所述收发模块，还用于在所述处理模块根据所述数量信息确定不允许所述终端接入所述网络的情况下，向所述终端发送第三消息；所述第三消息指示拒绝所述终端接入所述网络。

14.根据权利要求 13 所述的装置，其特征在于，

所述处理模块，具体用于当所述操作请求方对应的终端中接入所述网络的终端数量大于或等于数量阈值时，确定不允许所述终端接入所述网络；所述数量阈值为所述操作请求方允许使用的终端数量。

15.根据权利要求 11 至 14 任一项所述的装置，其特征在于，

所述收发模块，还用于向第二核心网设备发送第四消息；所述第四消息用于请求对所述终端执行认证流程；所述第四消息包括第二标识信息和认证信息，所述第二标识信息和所述认证信息用于执行所述认证流程；所述第二标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

16.根据权利要求 15 所述的装置，其特征在于，所述第四消息还包括指示信息，所述指示信息指示所述认证流程为单向认证、双向认证、所述终端对所述网络或者所述操作请求方的单向认证、所述网络或者所述操作请求方对所述终端的单向认证中的任一种。

17.根据权利要求 11 至 14 任一项所述的装置，其特征在于，

所述处理模块，还用于根据所述第一消息对所述终端执行认证流程；所述第一消息包括第三标识信息和认证信息，所述第三标识信息和所述认证信息用于执行所述认证流程；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

18.根据权利要求 11 至 17 任一项所述的装置，其特征在于，

所述处理模块，还用于根据所述第一消息包括的第三标识信息，确定所述终端所属的所述操作请求方；所述第三标识信息包括所述终端的终端标识、加密的终端标识、终端应用标识、终端网络标识、操作请求方标识中的一项或多项。

19.根据权利要求 15 或 16 或 17 所述的装置，其特征在于，

所述收发模块，还用于接收第五消息；向所述终端，发送第六消息；所述第五消息指示所述认证流程通过，所述第六消息指示接受所述终端接入所述网络；或者，所述第五消息指

示所述认证流程不通过，所述第六消息指示拒绝所述终端接入所述网络。

20.根据权利要求 11 至 19 任一项所述的装置，其特征在于，
所述处理模块，还用于获取所述数量信息和/或所述第一标识信息。

21.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行权利要求 1 至 10 任意一项所述的方法。

22.一种通信装置，其特征在于，包括处理器和存储器，
所述存储器，用于存储计算机程序或指令；
所述处理器，用于执行存储器中的计算机程序或指令，使得权利要求 1-10 任一项所述的方法被执行。

23. 一种通信系统，其特征在于，包括用于执行如权利要求 1-10 中任一项所述的方法的设备。

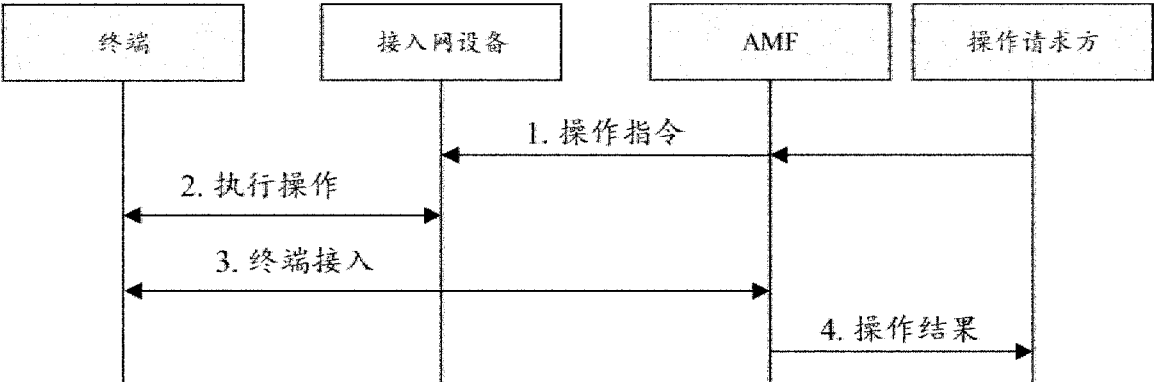


图 1

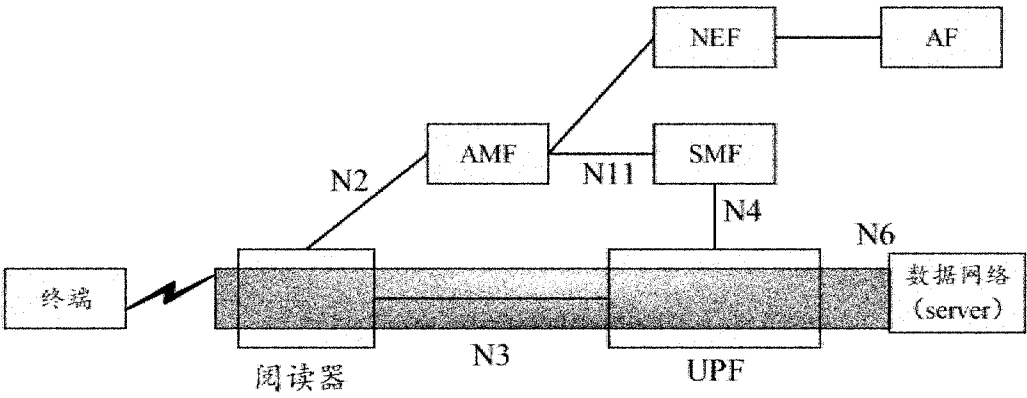


图 2A

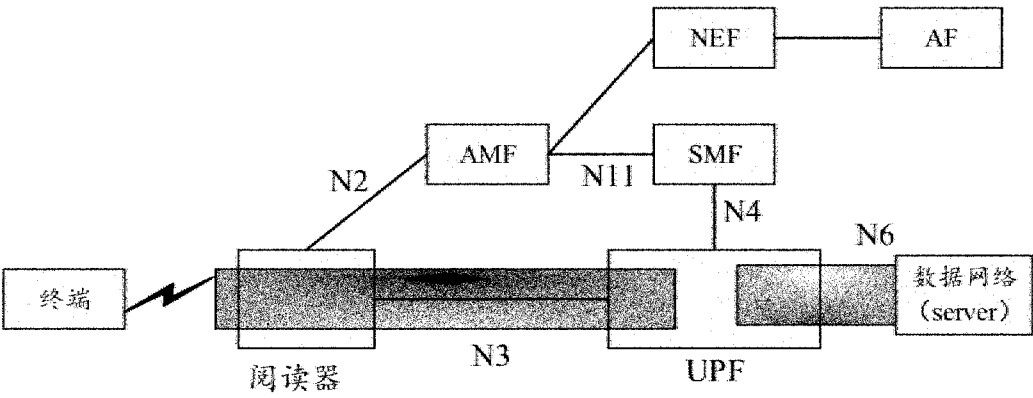


图 2B

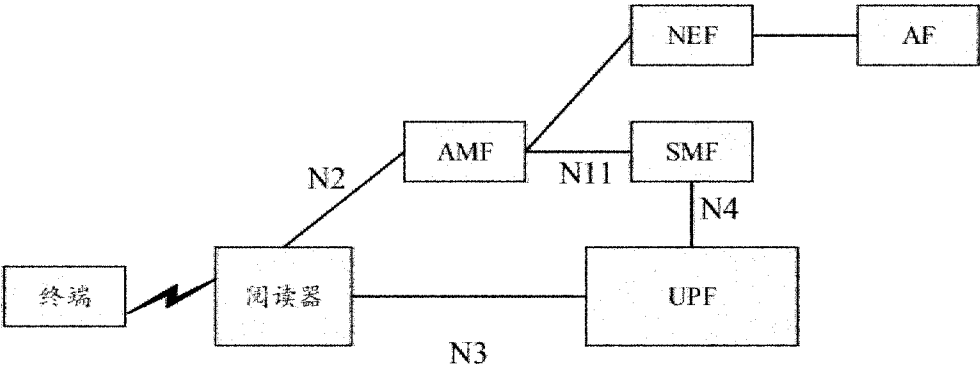


图 2C

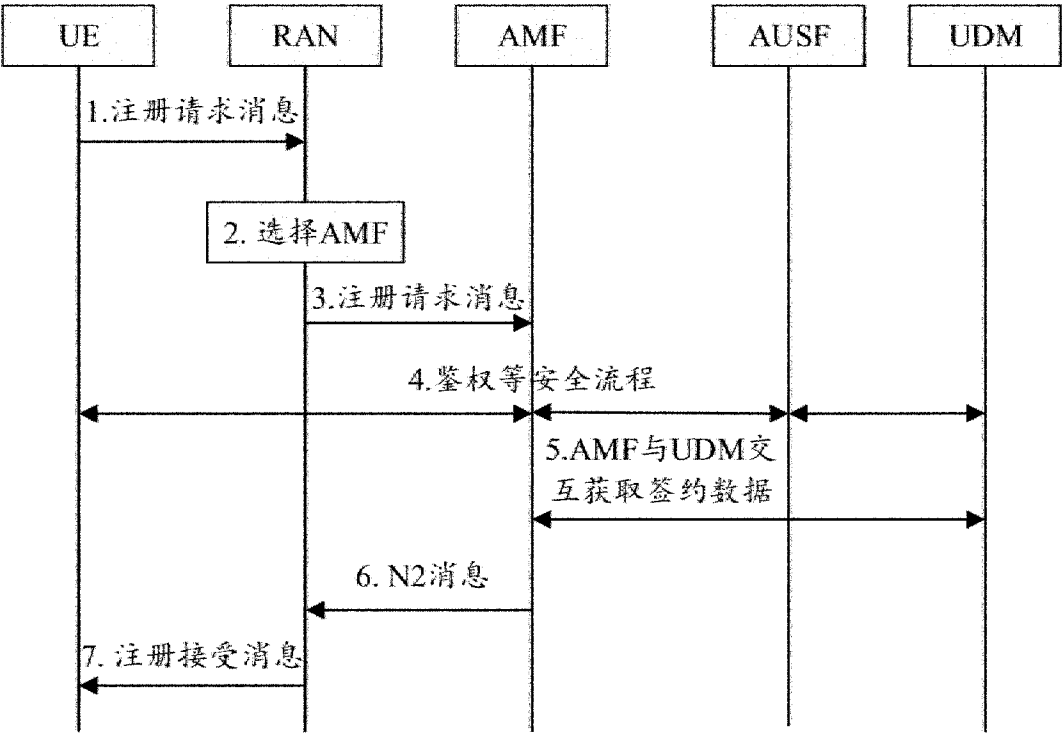


图 3

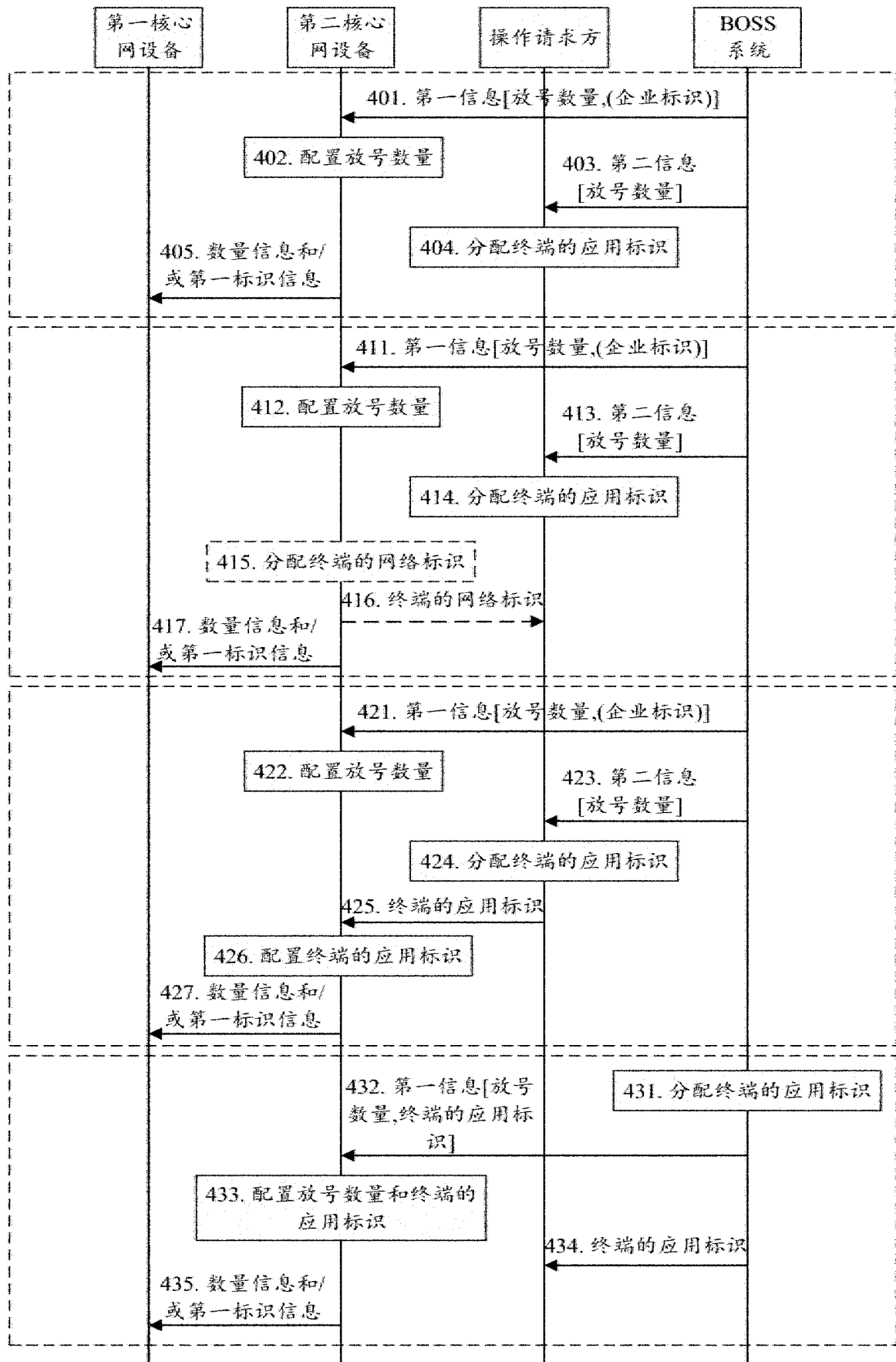


图 4

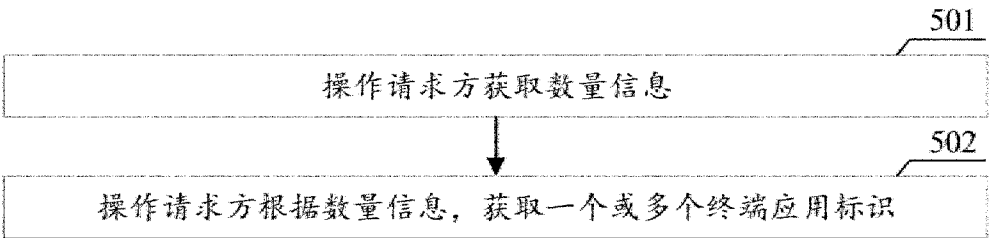


图 5

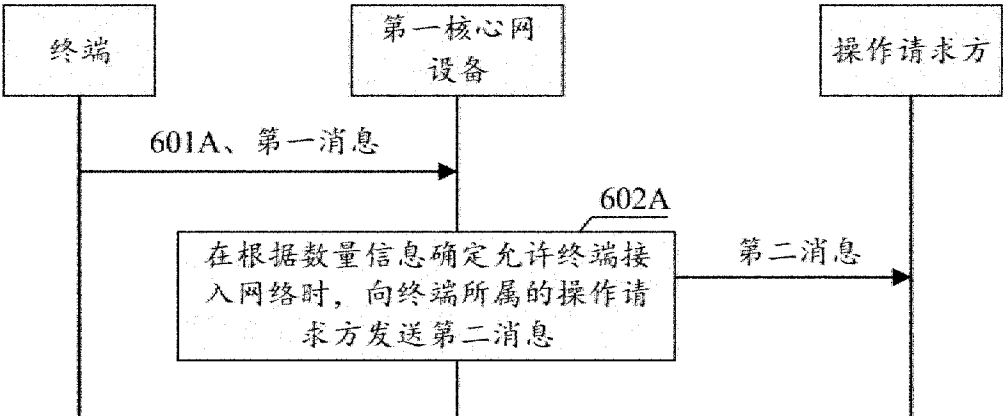


图 6A

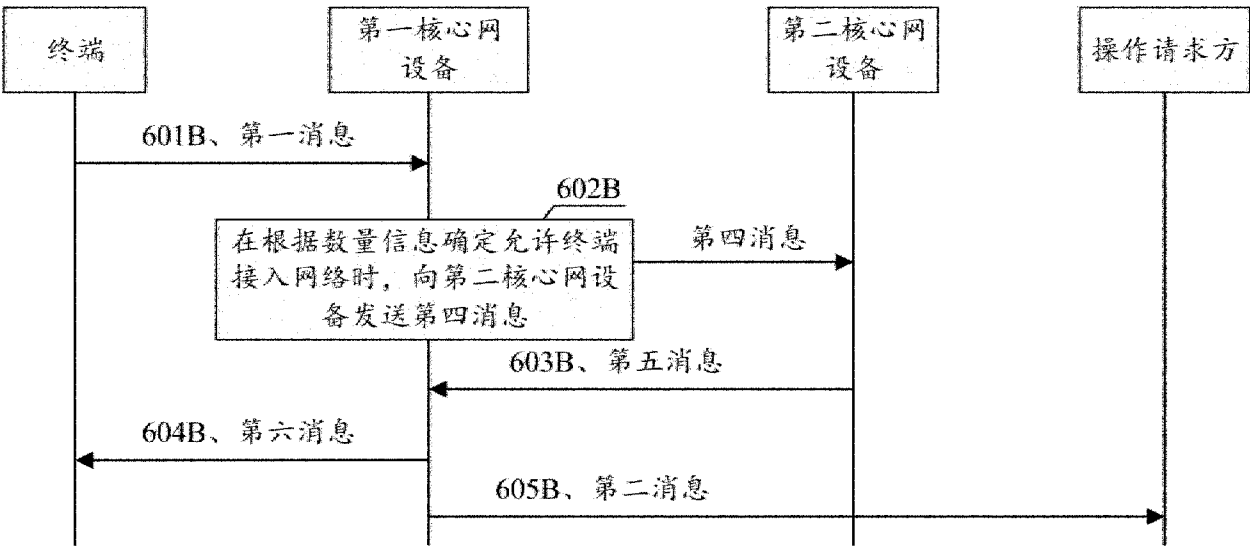


图 6B

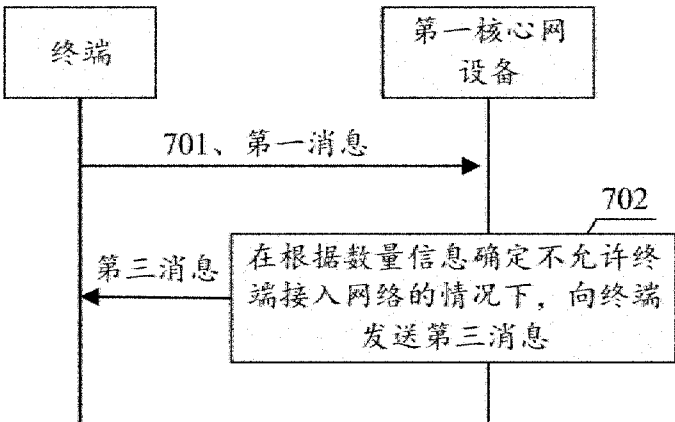


图 7

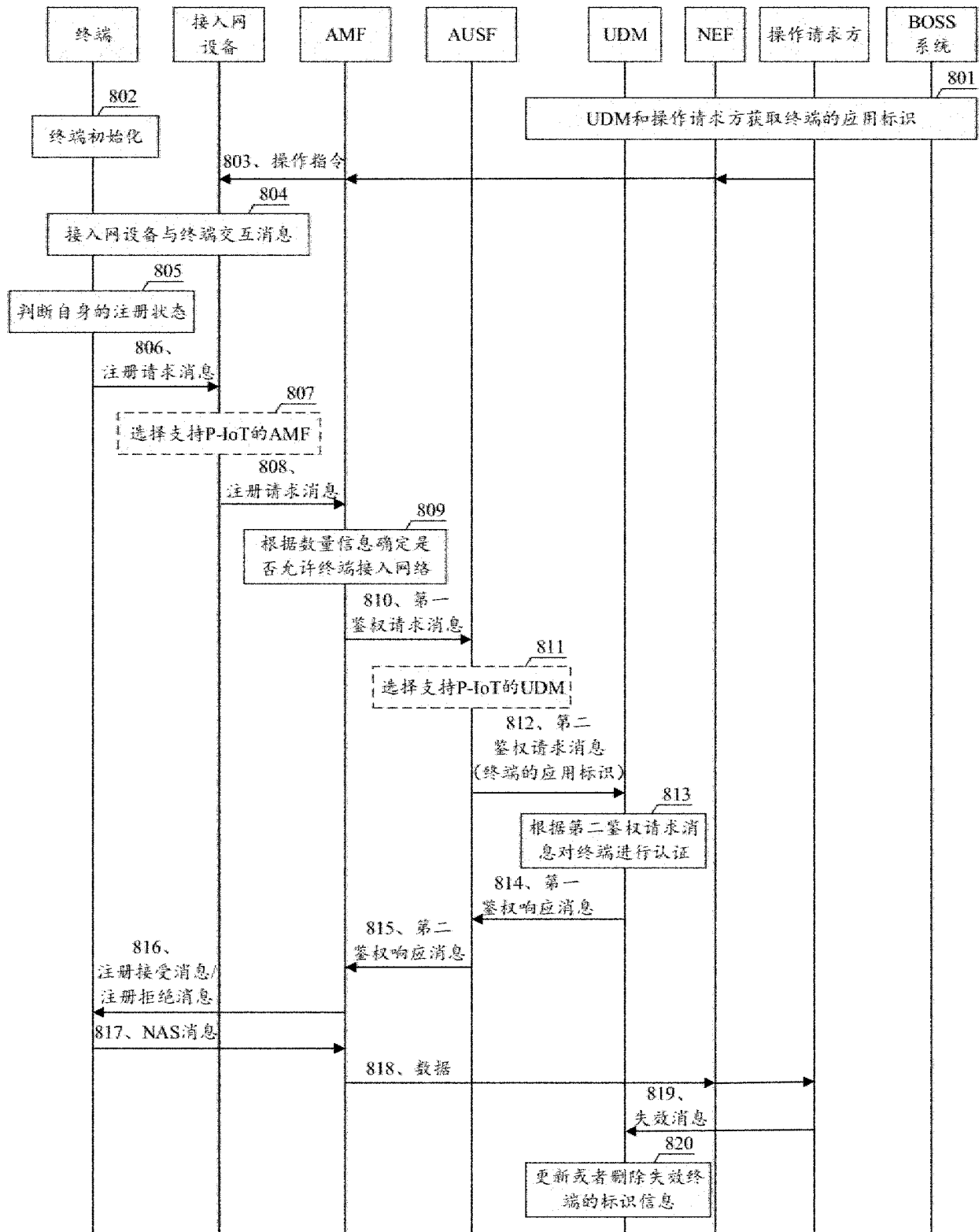


图 8

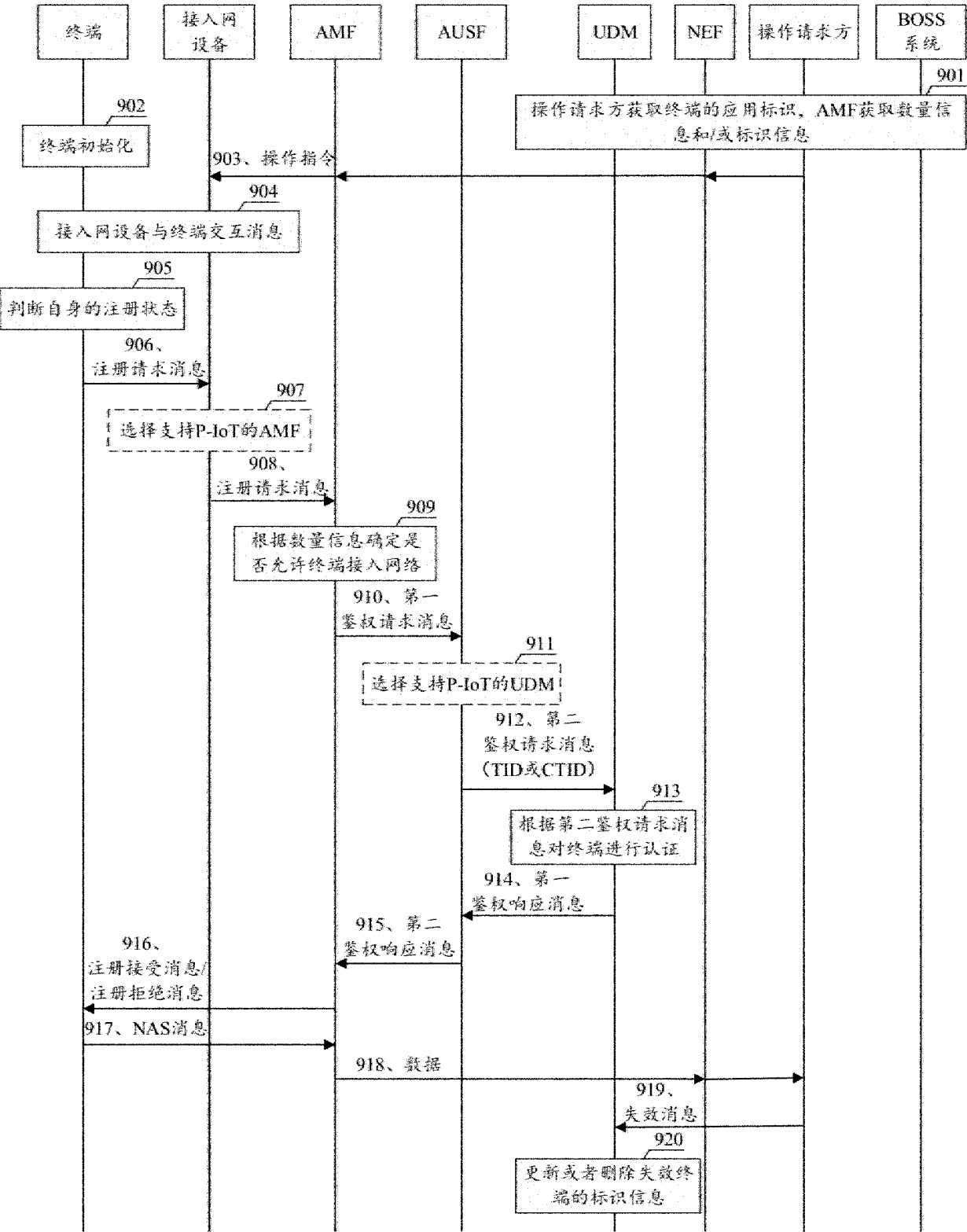


图 9

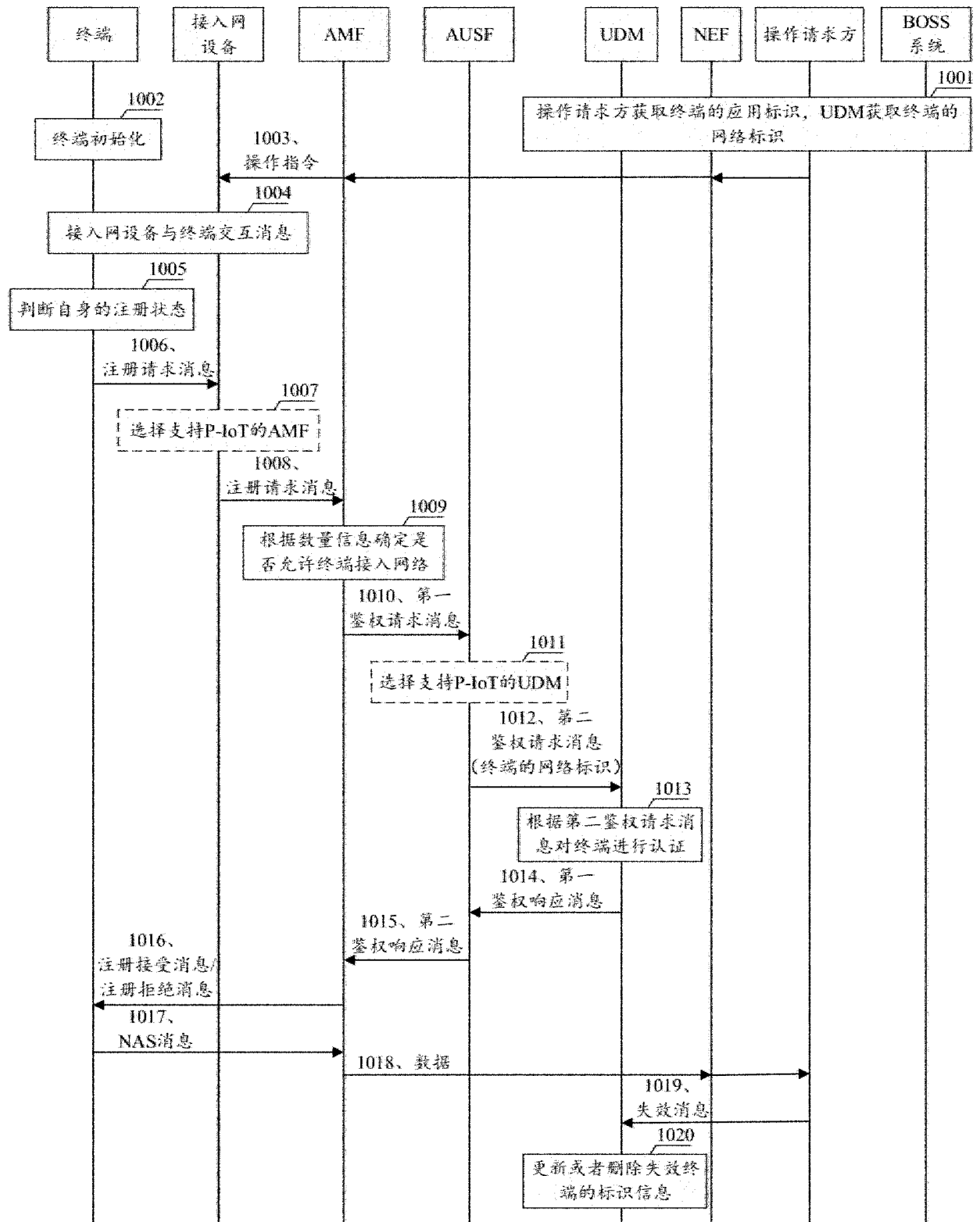


图 10

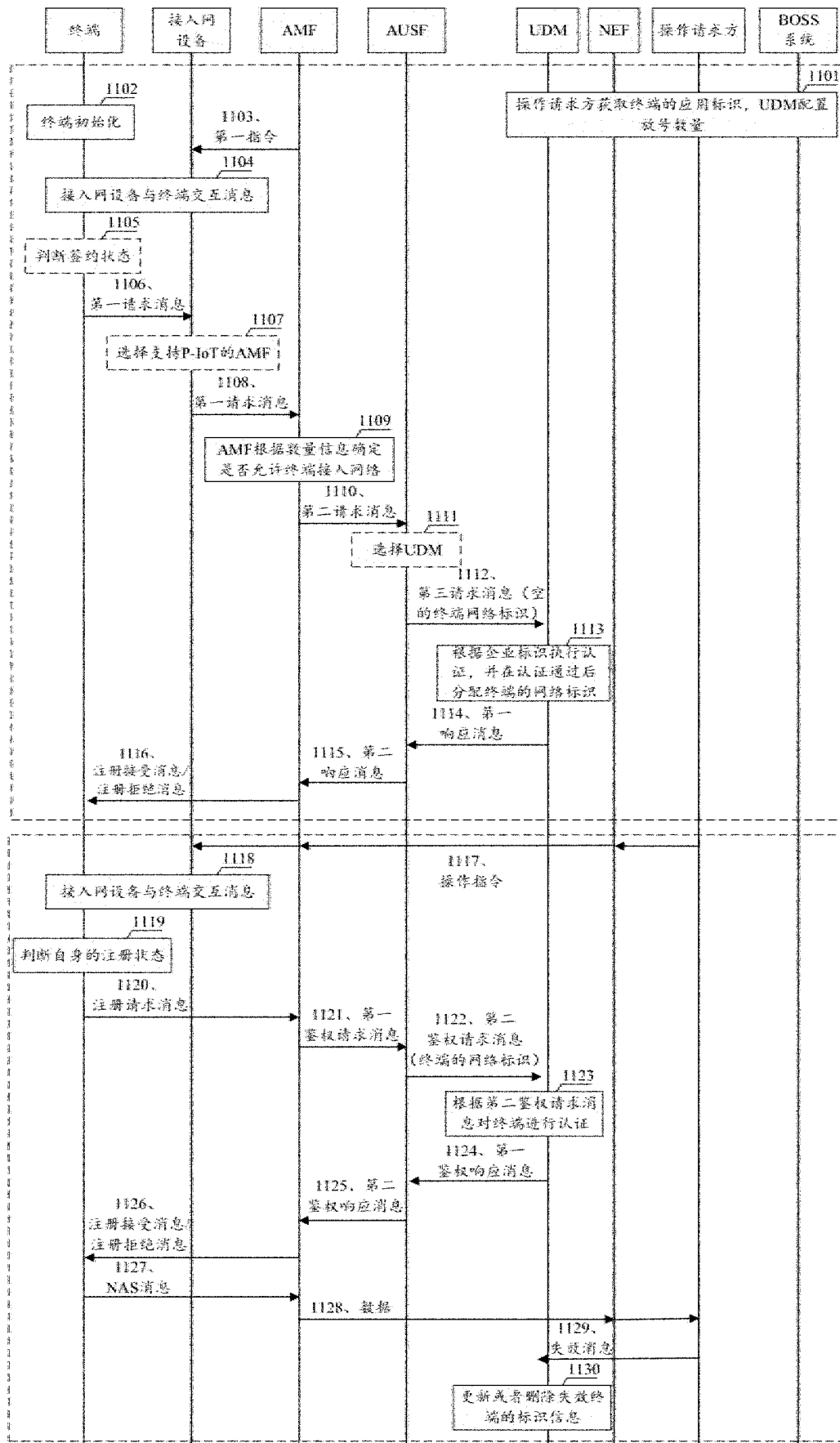


图 11

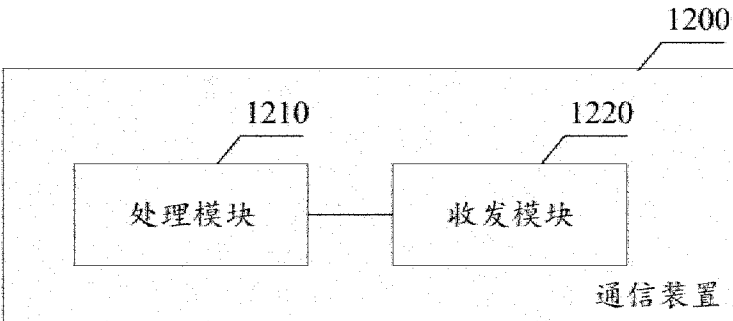


图 12

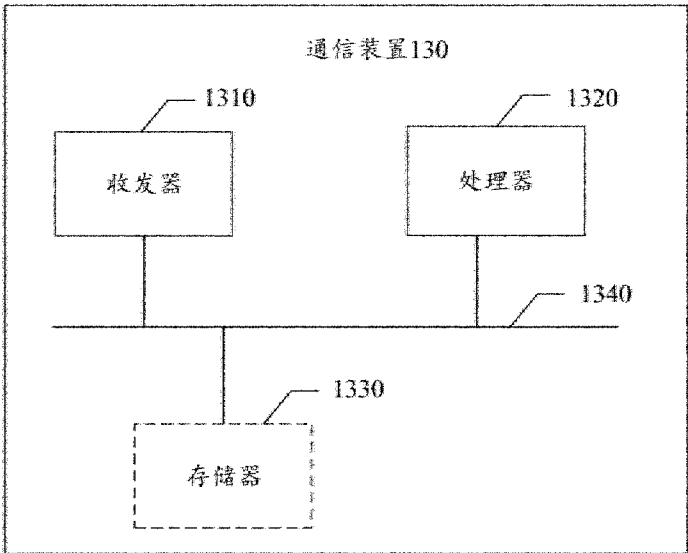


图 13

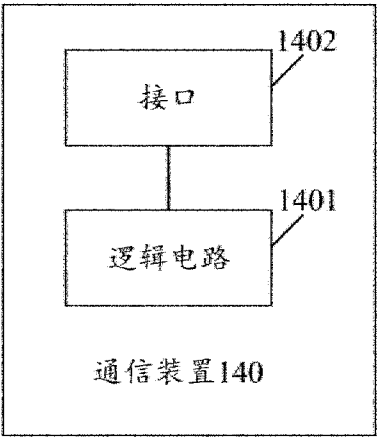


图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/072596

A. CLASSIFICATION OF SUBJECT MATTER

H04W8/22(2009.01)i;H04W 48/16(2009.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:H04W

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

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

CNABS; CNTXT; CNKI; VEN; USTXT; WOTXT; EPTXT; 3GPP: 电子标签, 读卡器, 阅读器, 终端, 物联网, 无源, 标识, 允许, 接入, 数量, 数目, 请求, 指示, 认证, tag, RFID, reader, passive, IoT, P-IoT, number, request, indicate, ID, authentic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2020155021 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 06 August 2020 (2020-08-06) description, page 16, paragraph 29-page 21, paragraph 33, page 30, paragraph 21-page 32, paragraph 2, and figure 13	1-23
X	CN 105723797 A (MEDIATEK INC.) 29 June 2016 (2016-06-29) description, paragraphs [0030]-[0051]	1-23
A	CN 110583036 A (HUAWEI INTERNATIONAL PTE LTD.) 17 December 2019 (2019-12-17) entire document	1-23
A	CN 108073955 A (ZTE CORP.) 25 May 2018 (2018-05-25) entire document	1-23
A	US 2014204736 A1 (RESEARCH IN MOTION LTD.) 24 July 2014 (2014-07-24) entire document	1-23



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

02 March 2023

Date of mailing of the international search report

14 March 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/072596

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2020155021	A1	06 August 2020	CN	112771903	A	07 May 2021
				CN	112771903	B	28 June 2022
CN	105723797	A	29 June 2016	US	2016113054	A1	21 April 2016
				US	10117279	B2	30 October 2018
				WO	2016058558	A1	21 April 2016
				IN	201727004137	A	03 March 2017
				CN	105723797	B	05 July 2019
				CN	110267362	A	20 September 2019
				CN	110267362	B	04 November 2022
CN	110583036	A	17 December 2019	WO	2018222132	A2	06 December 2018
				WO	2018222132	A3	31 January 2019
				US	2020100105	A1	26 March 2020
				US	11432157	B2	30 August 2022
				CN	110583036	B	25 November 2022
CN	108073955	A	25 May 2018	None			
US	2014204736	A1	24 July 2014	US	9554300	B2	24 January 2017
				EP	2946580	A1	25 November 2015
				EP	2946580	B1	04 July 2018
				WO	2014111510	A1	24 July 2014

国际检索报告

国际申请号

PCT/CN2023/072596

A. 主题的分类 H04W8/22(2009.01)i;H04W 48/16(2009.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) IPC:H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNABS; CNTXT; CNKI; VEN; USTXT; WOTXT; EPTXT; 3GPP; 电子标签, 读卡器, 阅读器, 终端, 物联网, 无源, 标识, 允许, 接入, 数量, 数目, 请求, 指示, 认证, tag, RFID, reader, passive, IoT, P-IoT, number, request, indicate, ID, authentic		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	WO 2020155021 A1 (华为技术有限公司) 2020年8月6日 (2020 - 08 - 06) 说明书第16页第29段-第21页第33段, 第30页第21段-第32页第2段以及图13	1-23
X	CN 105723797 A (联发科技股份有限公司) 2016年6月29日 (2016 - 06 - 29) 说明书第[0030]-[0051]段	1-23
A	CN 110583036 A (华为国际有限公司) 2019年12月17日 (2019 - 12 - 17) 全文	1-23
A	CN 108073955 A (中兴通讯股份有限公司) 2018年5月25日 (2018 - 05 - 25) 全文	1-23
A	US 2014204736 A1 (RESEARCH IN MOTION LTD) 2014年7月24日 (2014 - 07 - 24) 全文	1-23
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “D” 申请人在国际申请中引证的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2023年3月2日		国际检索报告邮寄日期 2023年3月14日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 刘婧 电话号码 (+86) 020-28950457

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2023/072596

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
WO	2020155021	A1	2020年8月6日	CN	112771903	A	2021年5月7日
				CN	112771903	B	2022年6月28日
CN	105723797	A	2016年6月29日	US	2016113054	A1	2016年4月21日
				US	10117279	B2	2018年10月30日
				WO	2016058558	A1	2016年4月21日
				IN	201727004137	A	2017年3月3日
				CN	105723797	B	2019年7月5日
				CN	110267362	A	2019年9月20日
				CN	110267362	B	2022年11月4日
CN	110583036	A	2019年12月17日	WO	2018222132	A2	2018年12月6日
				WO	2018222132	A3	2019年1月31日
				US	2020100105	A1	2020年3月26日
				US	11432157	B2	2022年8月30日
				CN	110583036	B	2022年11月25日
CN	108073955	A	2018年5月25日	无			
US	2014204736	A1	2014年7月24日	US	9554300	B2	2017年1月24日
				EP	2946580	A1	2015年11月25日
				EP	2946580	B1	2018年7月4日
				WO	2014111510	A1	2014年7月24日