(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
2018 年 3 月 22 日 (22.03.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/050007 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/100636

(22) 国际申请日: 2017 年 9 月 6 日 (06.09.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610822884.8 2016年9月13日 (13.09.2016) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 翟来国 (ZHAI, Laiguo); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦由中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 徐法禄 (XU, Falu); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦由中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 林愈银 (LIN, Yuyin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦由中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 李睿 (LI, Rui); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦由中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: 隆天知识产权代理有限公司 (LUNG TIN INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路5号远大中心B座18层, Beijing 100101 (CN)。

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

(54) **Title:** METHOD AND APPARATUS FOR ACCESSING LOCAL NETWORK BY USER TERMINAL AND COMPUTER STORAGE MEDIUM

(54) **发明名称**: 用户终端访问本地网络的方法和装置和计算机存储介质

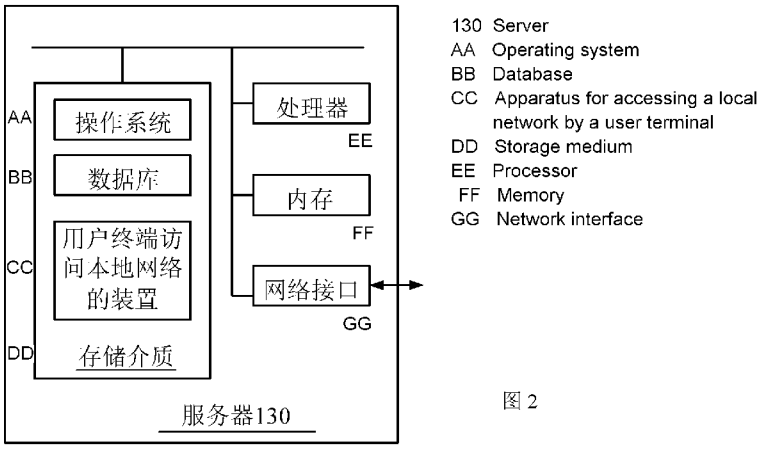

图 2

(57) **Abstract:** The disclosure relates to a method and an apparatus for accessing a local network by a user terminal and a computer storage medium, comprising: receiving a user plane S1-U uplink packet, and identifying and intercepting a local network access packet in the S1-U uplink packet; determining a user type of a user terminal corresponding to the local network access packet, and verifying a local network access permission of the user terminal according to the user type and a destination address in the local network access packet; and if the verification succeeds, disassembling the S1-U uplink packet, converting a source IP address and a source port number in a user IP packet to a device IP address and a mapped port number, re-encapsulating the packet into a local network packet, and forwarding the local network packet to a next hop address of a subnet to which the destination address belongs. In this way, a local network can be securely accessed directly from a base station side of a mobile network, so that nodes on an access path are greatly reduced, network latency is decreased, and transmission rate is increased.

WO 2018/050007 A1

[见续页]

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

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

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本公开涉及一种用户终端访问本地网络的方法和装置和计算机存储介质，包括：接收用户平面S1-U上行报文，识别并拦截所述S1-U上行报文中的本地网络访问报文；确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限；如果验证通过，则将所述S1-U上行报文拆解，将用户IP报文中的源IP地址和源端口号转换为设备IP地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址，能从移动网基站侧直接安全地访问本地网络，使得访问路径结点大幅减少，降低网络时延，提高传输速率。(图2)

用户终端访问本地网络的方法和装置和计算机存储介质

技术领域

本公开涉及通信技术领域，特别是涉及一种用户终端访问本地网络的方法和装置和计算机存储介质。

背景技术

随着移动通信技术的发展，使用移动网终端访问企业网普遍存在，如使用智能手机随时随地移动办公。移动网基站的部署位置也越来越靠近企业网络，尤其是室内部署场景，在一些大型企业、商业场所和中央商务区（CBD，Central Business District）等场所，运营商为满足室内高容量要求而部署了室内型基站，如室内分布系统，这些移动网室内基站和企业网络部署在同一个建筑里。与运营商移动网基站就近部署的私有网络（非因特网）统称为本地网络。

传统的用户终端访问本地网络时，用户终端（UE，User Equipment）发往移动网的上行报文经过 LTE（Long Term Evolution，通用移动通信技术的长期演进）移动网基站 eNB、回传网络（Backhaul），以及核心网 EPC 后，进入因特网，如骨干网和城域网等，然后从因特网上进入企业防火墙，经过 VPN 网关认证后，访问企业内网的服务器，移动网发给用户终端的下行报文的路径则相反。这种用户终端访问本地网络的方式，在进入企业网络时是从用公网，即因特网进入的，存在访问路径结点多，网络时延大的问题。

发明内容

基于此，有必要针对上述技术问题，提供一种用户终端访问本地网络的方法和装置，能从移动网基站侧直接安全地访问本地网络，使得访问路径结点大幅减少，降低网络时延，提高传输速率。

一种用户终端访问本地网络的方法，所述方法包括：

接收用户平面 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络访问报文；

确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所

述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限；

如果验证通过，则将所述 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址。

一种用户终端访问本地网络的装置，所述装置包括：

本地网络报文识别模块，用于接收用户平面 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络访问报文；

本地网络访问处理模块，用于确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限，如果验证通过，则将所述 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址。

一种用户终端访问本地网络的装置，其中，包括处理器以及存储有所述处理器可执行指令的存储器，当所述指令被处理器执行时，执行如下操作：

接收用户平面 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络访问报文；

确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限；

如果验证通过，则将所述 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址。

一种计算机存储介质，所述计算机存储介质中存储有计算机可执行的一个或多个程序，所述一个或多个程序被所述计算机执行时使所述计算机执行前述方法。

上述用户终端访问本地网络的方法和装置，通过接收 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络访问报文，拦截的本地网络访问报文不会发送至核心网减少了访问路径结点，确定本地网络访问报文对应的用户终端的用户类型，根据用户类型和本地网络访问报文中的目的地址验证用户终端的本地网络访问权限；如果验证通过，则将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至所

述目的地址所在子网的下一跳地址，只有验证通过的本地网络访问报文才会进行转发，保证了本地网络信息的安全性，使得用户终端能快速安全的访问本地网络。

附图说明

图 1 为一个实施例中用户终端访问本地网络的方法运行的应用环境图；

图 2 为一个实施例中图 1 中服务器的内部结构图；

图 3 为一个实施例中用户终端访问本地网络的方法的流程图；

图 4 为一个实施例中 DNS 查询响应的流程图；

图 5 为一个实施例中本地网络访问权限验证的流程图；

图 6 为一个实施例中判断用户访问权限是否符合目的子网类型对应的访问权限的流程图；

图 7 为一个实施例中发起用户类型修改申请的流程图；

图 8 为一个实施例中根据判决算法修改用户类型的流程图；

图 9 为一个具体的实施例中用户终端查询本地网络域名时序图；

图 10 为一个具体的实施例中用户终端访问本地网络 DMZ 子网的上行报文的时序图；

图 11 为一个具体的实施例中用户终端访问本地网络 DMZ 下行报文时序图；

图 12 为一个具体的实施例中本地网络 DMZ 访客授权时序图；

图 13 为一个具体的实施例中用户终端访问本地网络内网上行报文时序图；

图 14 为一个具体的实施例中用户终端访问本地网络内网下行报文时序图；

图 15 为一个具体的实施例中本地网络内网授权时序图；

图 16 为一个实施例中用户终端访问本地网络的装置的结构框图；

图 17 为另一个实施例中用户终端访问本地网络的装置的结构框图；

图 18 为一个实施例中本地网络访问处理模块的结构框图；

图 19 为再一个实施例中用户终端访问本地网络的装置的结构框图；

图 20 为又一个实施例中用户终端访问本地网络的装置的结构框图；

图 21 为一个实施例中第一验证单元的结构框图；

图 22 为一个实施例中本地网络访问处理模块的结构框图；

图 23 为一个实施例中本地网络访问授权模块的结构框图；

图 24 为又一个实施例中用户终端访问本地网络的装置的结构框图；

图 25 为一个实施例中移动网基站部署了用户终端访问本地网络的装置后的内部结构示意图；

图 26 为一个实施例中用户终端访问本地网络的系统结构框图；

图 27 为一个实施例中用户终端访问本地网络的系统的内部结构示意图；

图 28 为另一个实施例中用户终端访问本地网络的系统的内部结构示意图。

具体实施方式

图 1 为一个实施例中用户终端访问本地网络的方法运行的应用环境图，如图 1 所示，该应用环境包括终端 110、基站 eNB（evolved Node B）120、服务器 130、企业 DMZ 区 140 和企业内网 150，其中企业 DMZ 区 140 包括 VPN 网关 141、反向代理服务器 142 和防火墙 143，企业内网 150 包括阻塞 choke 路由器 151、公共服务器 152 和 APP 应用服务器 153，此应用环境中的设备可根据实际部署相应的增加或减少。其中终端 110 为可使用移动通信网进行通信的设备，包括但不限于智能终端、移动通信工业设备、物联网（IoT，Things Of Internet）设备等。用户终端访问本地网络时，从移动网基站侧经过用户终端权限验证后直接访问企业网络，上行报文和下行报文都不需要经过回传网络 Backhaul、核心网 EPC 和因特网，可快速安全地接入访问本地网络。此应用环境可应用于多种场景，如手机移动办公的内网访问场景，工业设备之间通过无线互联，工业设备数据属于企业私有数据，数据量大，实时性要求高，无线传输数据到企业网络的场景。商用场所无线传输到商场网络服务器的场景，如大型购物商城，商家推出的 VR（虚拟现实）、AR（增强现实）推广活动，传输数据量大，实时性要求高，存在无线传输数据到商场网络服务器的需求。大型赛事或展会，大量视频无线传输到场馆内服务器的场景等。

在一个实施例中，图 1 中的服务器 130 的内部结构如图 2 所示，该服务器 130 包括通过系统总线连接的处理器、存储介质、内存和网络接口。其中，该服务器 130 的存储介质存储有操作系统、数据库和一种用户终端访问本地网络的装置，数据库用于存储数据，如用户记录表等，该装置用于实现一种适用于服务器 130 的用户终端访问本地网络的方法。该服务器 130 的处理器用于提供计算和控制能力，支撑整个服务器 130 的运行。该服务器 130 的内存为存储介质中的用户终端访问本地网络的装置的

运行提供环境。该服务器 130 的网络接口用于与基站 eNB120、企业网络、运营商 Backhaul 通过网络连接通信，比如接收基站 eNB120 发送的上行报文等。服务器 130 一般采用高性能网络服务器。

如图 3 所示，在一个实施例中，提供了一种用户终端访问本地网络的方法，应用于上述应用环境，包括如下步骤：

步骤 S110，接收用户平面 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络访问报文。

具体的，终端需要访问本地网络时，向基站发送封装了用户报文的空口报文，其中用户报文即 IP 报文的源 IP 地址就是 UE PDN IP，UE PDN IP 是用户终端 UE 在移动网完成登记后，由移动网分配的 IP 地址。基站接收到空口报文后，提取其中的用户报文，并打包在 S1-U 隧道报文中进行发送。本方案需要得到源 IP 地址作为用户标识，通过源 IP 地址区分识别不同的用户终端。移动网基站和核心网之间采用隧道方式传输用户报文，移动网基站和核心网为每个用户终端各自分配唯一的 S1-U 隧道标识 TEID（Tunnel Endpoint Identifier），基站分配的隧道标识称为移动网基站隧道标识，核心网分配的隧道标识可称为核心网隧道标识。发给移动网基站的下行报文，需打包成携带移动网基站 TEID 的 S1-U（S1 User Plane）用户平面报文，移动网基站收到后通过移动网基站隧道标识 TEID 区分出不同的用户，打包成空口报文中发送至对应的用户终端。同理，移动网基站 eNB 发给核心网的上行报文，需打包成携带核心网隧道标识的 S1-U 报文，核心网收到根据核心网隧道标识区分用户，通过处理后发往因特网。可通过部署在基站或服务器的本地网络报文识别模块识别并拦截用户平面 S1-U 上行报文中的本地网络访问报文。如果本地网络报文识别模块部署在基站中，则在基站发送 S1-U 上行报文之前，就能识别并拦截本地网络访问报文，从而只将识别出的本地网络访问报文发给后续的处理模块，减轻后续处理模块的压力。如果本地网络报文识别模块部署在服务器中，则在基站将 S1-U 上行报文发送至核心网的过程中，由服务器识别并拦截本地网络访问报文，从而本地网络访问报文不会发送至核心网。

本地网络访问报文是符合本地网络访问报文特征规则的报文，使用配置的本地网络访问报文特征列表，对 S1-U 上行报文中的用户报文逐个进行比对和分析，识别出本地网络访问报文。配置的本地网络访问报文特征列表中，每条记录包含子网段、协

议号、端口号等信息，允许协议号和端口号字段可选。如一条本地网络访问报文特征列表记录为：“地址：10.1.0.0，子网掩码：255.255.0.0，协议号：6，端口号：443，上述“地址：10.1.0.0，子网掩码：255.255.0.0”，在描述时经常使用子网 10.1.0.0/16 来替代。通过从 S1-U 上行报文中用户报文提取出目的地址、协议号、目的端口号然后与本地网络访问报文特征列表进行对比，只有特征匹配才为本地网络访问报文。如用户访问 hr.ttt.com.cn（ip 地址为 10.1.2.1）的 https 报文，目的地址 10.1.2.1 匹配 10.1.0.0/16 子网，https 即协议号 6，端口号 443，则匹配上述特征记录。拦截的本地网络访问报文不会发送至核心网，只有非本地网络访问报文才会发送至核心网。

步骤 S120，确定本地网络访问报文对应的用户终端的用户类型，根据用户类型和本地网络访问报文中的目的地址验证用户终端的本地网络访问权限。

具体的，不同的用户类型具有不同的访问权限，具体的用户类型的种类和对应的权限可根据需要自定义，定义时可根据本地网络区域的划分为不同的区域设置不同种类的用户类型。可根据用户终端所在的网络段确定用户终端的用户类型，如可设置固定 IP 地址的高权限用户，为不同的用户终端分配不同的固定权限。也可设置默认用户类型为无权限用户，需要实时的向本地网络访问授权模块申请有权限的用户类型，本地网络访问授权模块根据用户类型申请请求，实时的根据授权判决算法，授权判决算法可依据当前网络通信状态参数、访问的本地网络的区域等多种参考因子为用户终端授权相应的动态的有不同权限的用户类型，根据当前网络通信状态实时更新用户类型，可实时控制用户终端访问本地网络的数量。也可先通过查找用户记录表获取用户终端的用户类型，在用户记录表中不存在用户终端对应的用户记录时，才需要向本地网络访问授权模块申请有权限的用户类型。

只有用户终端的本地网络访问权限与其访问的本地网络访问报文中的目的地址要求的权限相匹配，才算验证通过。可将本地网络分为不同的区域，如 DMZ 区（Demilitarized Zone，非军事化区，也称隔离区）和内部网络，访问不同的区域需要不同的访问权限。用户终端访问的目的地址在不同的区域时，本地网络访问授权模块可根据用户类型申请请求，采用不同的授权判决算法，从而使得不同的区域的访问根据其内容的私密性设置不同的访问规则，灵活方便。授权判决时，可通过 VPN 网关协助认证用户身份，只有用户通过认证确认为内部用户，才有申请特定用户类型的权限，进一步保证用户类型授权的安全性。

步骤 S130，如果验证通过，则将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至目的地址所在子网的下一跳地址。

具体的，只有验证通过的本地网络访问报文才会进行转发，如果没有验证通过，则丢弃报文，保证了本地网络信息的安全性，向本地网络转发前，需要先拆解 S1-U 报文，提取用户报文，获取用户报文携带的源 IP 地址和源端口号，转换为设备 IP 地址和映射端口号。设备 IP 地址为实现上述方法的设备在本地网络中的 IP 地址，设备 IP 地址的数量可根据设备的网卡个数相应的设定，每个网卡也可设置多个设备 IP 地址。将移动网为用户终端分配的源 IP 地址统一转换为设备 IP 地址，保证在本地网络中传输的正确 IP 地址。同时，用户报文携带的源端口号也需要转换为映射端口号，由于之前用户报文携带的源端口号对于不同的用户终端可能携带相同的端口号，需要在一个本地网络地址下重新分配端口号，保证每个设备 IP 地址+映射端口号的组合在传输过程中是不重复的，从而保证数据传输的正确性。

如一个具体的实施例中，用户终端 110 访问 APP 应用服务器 153 的访问路径如图 1 中路线 160 所示，经过访问路径结点基站 eNB120、服务器 130、VPN 网关 141、防火墙 143、choke 路由器 151 后到达 APP 应用服务器 153，中途不需要经过回传网络 Backhaul、核心网 EPC 和因特网，使得访问路径结点大幅减少，降低网络时延，提高传输速率。

本实施例中，通过接收 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络访问报文，拦截的本地网络访问报文不会发送至核心网减少了访问路径结点，确定本地网络访问报文对应的用户终端的用户类型，根据用户类型和本地网络访问报文中的目的地址验证用户终端的本地网络访问权限；如果验证通过，则将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至所述目的地址所在子网的下一跳地址，只有验证通过的本地网络访问报文才会进行转发，保证了本地网络信息的安全性，使得用户终端能快速安全的访问本地网络。

在一个实施例中，如图 4 所示，步骤 S110 之前，还包括：

步骤 S210，接收 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络域名的域名系统 DNS 查询报文。

具体的，终端需要访问本地网络服务时，需要先获取本地网络服务器域名（如hr.ttt.com.cn）对应的本地网络 IP 地址，如果需要访问的本地网络服务器的 IP 地址已经提前获取，如对于经常访问一个固定的本地网络，可预存其本地网络 IP 地址，发送网络访问报文中直接携带预存的本地网络 IP 地址。但一般情况下，需要通过 DNS 查询报文获取网络域名对应的 IP 地址。可通过部署在基站或服务器的本地网络报文识别模块识别并拦截 S1-U 上行报文中的本地网络域名的 DNS 查询报文。

本地网络域名查询报文，为标准 DNS 查询报文，由用户终端发往公网 DNS 服务器。本地网络报文识别模块在用户终端发往公网 DNS 服务器之前，分析 DNS 查询报文中的域名，与配置的本地网络域名列表的每条域名记录进行匹配，检查是否匹配成功，如果匹配成功，则识别到本地网络域名查询报文。配置的本地网络域名列表中，每条记录符合 FQDN（Fully Qualified Domain Name，完全合格域名/全称域名）规则。如 ttt.com.cn 为本地网络域名列表中的一个记录，则如果 DNS 查询报文中的域名为 hr.ttt.con.cn 或 ims.ttt.com.cn 都算匹配成功。

步骤 S220，根据本地网络域名的 DNS 查询报文构造携带本地网络 IP 地址的 DNS 响应报文，将 DNS 响应报文返回至终端，本地网络 IP 地址作为目的地址携带在本地网络访问报文中。

具体的，可根据本地网络域名配置信息获取域名对应的本地网络 IP 地址，构造 DNS 查询响应消息，也可转发到外置的专用本地网络域名 DNS 服务器获取域名对应的本地网络 IP 地址，完成构造 DNS 查询响应消息。本地网络域名配置信息中配置了每个本地网络域名对应的本地网络 IP 地址，如 hr.ttt.com.cn 对应地址 10.1.2.1，ims.tt.com.cn 对应地址 10.1.3.2。另外，还需要配置域名记录的生存时间，即 TTL（Time To Live），超过 TTL 时间后域名记录应失效，需重新获取。将 DNS 响应报文返回至终端，其中 DNS 响应报文携带本地网络域名和对应的本地网络 IP 地址，则后续终端发送本地网络域名对应的本地网络访问报文时使用这个本地网络 IP 地址作为目的地址。

在一个实施例中，如图 5 所示，步骤 S120 包括：

步骤 S121，提取本地网络访问报文携带的用户标识，确定用户标识对应的用户类型，确定目的地址所在子网和子网类型。

具体的，用户标识为源 IP 地址，可根据源 IP 地址与用户类型的对应关系得到对

应的用户类型。源 IP 地址与用户类型的对应关系可通过表格、文本等形式预先存储，从而通过查表或查字符串的形式获得对应的用户类型。根据目的地址所在的 IP 地址段确定对应的子网，不同的子网对应了各自的子网类型。子网类型可根据本地网络的信息安全重要程度进行划分，如分为 DMZ 子网和内网子网，内网子网需要更高的访问权限才能访问。且不同的子网类型有对应的具有访问权限的用户类型，可自定义子网类型和具有访问权限的用户类型之间的对应关系。通过为不同的子网类型分配不同的具有访问权限的用户类型，提高了访问权限的灵活控制性。

步骤 S122，判断用户类型对应的用户访问权限是否符合目的地址所在子网类型对应的访问权限，如果符合，则进入步骤 S123。

具体的，只有用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限，才会进入下一步，否则丢弃本地网络访问报文。

步骤 S123，判断目的地址所在子网是否为允许访问的子网，如果是，则本地网络访问权限通过验证，否则本地网络访问权限未通过验证。

具体的，当用户类型符合用户访问权限后，进一步判断目的地址所在子网是否为允许访问的子网，可通过预先为不同类型的用户分配不同的子网列表，通过查表的方式确定本地网络访问报文中的目的地址所在子网是否为允许访问的子网，如果是，则本地网络访问权限通过验证，否则本地网络访问权限未通过验证。

本实施例中，通过访客权限和子网权限双重验证，灵活方便的控制不同用户类型的访问权限，保证本地网络访问的安全性。

在一个实施例中，方法还包括：如果用户类型对应的用户访问权限不符合目的地址所在子网类型对应的访问权限，则根据授权判决算法更新用户终端的用户类型。

具体的，如果用户类型对应的用户访问权限不符合目的地址所在子网类型对应的访问权限，可向本地网络访问授权模块申请用户类型的变更，本地网络访问授权模块接收到用户类型变更请求，可根据用户类型变更请求和授权判决算法更新用户终端的用户类型。在发送用户类型变更请求时，可根据目的地址所在子网类型和当前用户类型生成不同的用户类型变更请求。不同的用户类型变更请求可对应不同的授权判决算法，授权判决算法的确定可根据需要自定义，如根据配置的不同子网类型对应的授权人数和当前在线人数，以及总流量门限和当前在线流量等因素确定是否给予用户类型变更请求授予相应的用户类型。本实施例中，如果用户类型对应的用户访问权限不符

合目的地址所在子网类型对应的访问权限，可申请具有相应权限的用户类型，达到动态的权限变更。

还可根据授权判决算法，将符合目的地址所在子网类型对应的访问权限的用户的类型修改为无权限用户，灵活的控制访问权限。

在一个实施例中，步骤 S130 中则将 S1-U 上行报文拆解的步骤之前，还包括：根据当前访问状态判断是否为本地网络访问报文提供转发许可，如果本地网络访问报文获得转发许可，则进入将所述 S1-U 上行报文拆解的步骤，如果本地网络访问报文未获得转发许可，则丢弃本地网络访问报文。

具体的，当前访问状态包括用户的上下行访问速率限制、访问时长和访问总流量等信息，根据当前访问状态判断是否为本地网络访问报文提供转发许可。只有获得转发许可才能转发报，不同的子网类型可对应不同的转发许可授予策略。通过转发许可进一步灵活控制本地网络的访问流量、访问时长等。对 DMZ 授权访客用户访问 DMZ 子网，根据访客用户的上下行访问速率限制、访问时长和访问总流量等信息，为本地网络访问处理模块提供访客转发许可。对授权内网用户访问内部网络子网，根据用户的上下行访问速率限制，为本地网络访问处理模块提供授权转发许可。对受控授权用户访问本地网络 VPN 网关，根据受控授权用户的上下行访问速率限制、访问时长和访问总流量等为本地网络访问处理模块提供受控转发许可。

在一个实施例中，步骤 S120 中确定本地网络访问报文对应的用户终端的用户类型的步骤包括：根据本地网络访问报文携带的用户终端的用户标识查询用户记录表，如果用户标识在所述用户记录表中，则得到用户记录表中记录的用户类型，如果用户标识不在用户记录表中，则用户类型为无权限用户。

具体的，可根据用户类型生成不同类型的用户记录表，通过记录表标识进行区分。如果更新了用户类型，则同步更新用户记录表。从而如果上次获得了有权限的用户类型，在下次访问时，可直接通过用户记录表得到有权限的用户类型记录，不必重新申请有权限的用户类型，快速获得访问权限。在一个实施例中，获取用户记录表中的用户记录对应的有效时间，判断在有效时间范围内用户没有访问本地网络，则删除用户记录。在一个实施例中，如果用户访问权限到期，则设置此用户对应的禁用期，在禁用期期内，此用户不具有申请用户类型更新的权限，只有禁用期过后，才具有申请资格。在一个实施例中，本地网络分为 DMZ 区和内网，子网类型分为 DMZ 子网和内

网子网，用户类型包括 DMZ 授权访客用户、受控授权用户和授权内网用户，如图 6 所示，步骤 S122 包括以下步骤中的至少一个：

步骤 S122a，如果目的地址所在子网类型为 DMZ 子网，且用户类型为 DMZ 授权访客用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

具体的，DMZ 区，提供外部网络和内部网络的隔离，并由外部路由器和防火墙提供一定防护。部署在 DMZ 区的设备大都也要具备一定的防攻击能力，也称为堡垒主机。内部网络，由内部路由器，图 1 中即 choke 路由器（阻塞路由器），和防火墙提供防护。内部网络不允许外部直接访问，只允许 DMZ 区的部分堡垒主机访问，外网用户必须通过 VPN 网关认证后才可访问。VPN 网关，可作为堡垒主机，大都部署在 DMZ 区，也可租用运营商的 VPN 网关，可通过 DMZ 区的堡垒主机中转再访问内部网络。DMZ 区服务器还可部署反向代理服务器，对外公共服务器也大多部署在内部网络，用户访问对外公共服务时，通过 DMZ 的反向代理服务器，再去访问部署于内部网络的对外公共服务器，为对外公共服务器提供更好的防护。DMZ 授权访客用户，表示具有 DMZ 子网访问权限的用户，如果目的地址所在子网类型为 DMZ 子网，且用户类型为 DMZ 授权访客用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

步骤 S122b，如果目的地址所在子网类型为内网子网，用户类型为受控授权用户，则判断用户类型对应的用户访问权限不符合目的地址所在子网类型对应的访问权限，将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至 VPN 网关。

具体的，受控授权用户表示对本地网络的 VPN 网关有权限访问，如果用户类型为受控授权用户，在获得内部用户身份前，需要向 VPN 网关申请用户身份认证，将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至 VPN 网关。

步骤 S122c，如果目的地址所在子网类型为内网子网，用户类型为授权内网用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

具体的，授权内网用户表示具有内网子网访问权限的用户，只有内部用户且通过内网授权判决算法得到授权才能对本地网络内网子网进行访问。本方案不限定用户通

过本地网络内部用户认证的方式。

本实施例中，将子网类型分为 DMZ 子网和内网子网，用户类型包括 DMZ 授权访客用户、受控授权用户和授权内网用户，通过目的地址所在子网类型和用户类型具体判断是否符合目的地址所在子网类型对应的访问权限，达到对各个不同子网的灵活访问控制。

在一个实施例中，如图 7 所示，方法还包括以下步骤中的至少一个：

步骤 S310，如果目的地址所在子网类型为 DMZ 子网，且用户类型为非 DMZ 授权访客用户，则发起 DMZ 授权访客用户申请。

步骤 S320，如果目的地址所在子网类型为内网子网，获知用户身份为内部用户前，则发起受控授权用户申请。

具体的，没有通过 VPN 认证的用户，无法确认用户身份，只能发往 VPN 网关进行认证，则只能发起受控授权用户申请，不能发起授权内网用户申请。

步骤 S330，如果目的地址所在子网类型为内网子网，获知用户身份为内部用户且用户类型为受控授权用户，则发起授权内网用户申请。

具体的，只有获知到用户身份为内部用户后，才能发起授权内网用户申请。

本实施例中，通过目的地址所在子网类型、当前用户类型和当前用户身份控制发送的用户类型申请请求，使得用户类型申请请求能分层次的正确的生成。

在一个实施例中，如图 8 所示，如果用户类型对应的用户访问权限不符合所述目的地址所在子网类型对应的访问权限，则根据授权判决算法更新用户终端的用户类型的步骤包括以下步骤中的至少一个：

步骤 S410，如果接收到 DMZ 授权访客用户申请，则根据 DMZ 访客授权判决算法给予 DMZ 访客授权，并根据配置生成 DMZ 访客授权信息，修改通过 DMZ 访客授权的用户类型为 DMZ 授权访客用户。

具体的，DMZ 访客授权信息可包括用户标识和对应的用户类型。在用户记录表分为 DMZ 授权访客用户记录表、受控授权用户记录表和内网授权用户记录表的情况下，可将 DMZ 访客授权信息传递至 DMZ 授权访客用户记录表，更新 DMZ 授权访客用户记录表，新增或变更用户记录，并将用户记录的用户类型设置为 DMZ 授权访客用户。在更新用户记录的同时发送启动访客用户访问控制消息，携带启动的策略和相关信息。其中上行速率控制和下行速率控制为必选策略，访问时长和访问总流量为可

选。

步骤 S420，如果接收到受控授权用户申请，则根据受控授权判决算法，给予受控授权，并根据配置生成受控授权信息，修改通过受控授权的用户类型为受控授权用户。

具体的，受控授权信息可包括用户标识和对应的用户类型。可将受控授权信息传递至受控授权用户记录表，更新受控授权用户记录表，新增或变更用户记录，并将用户记录的用户类型设置为受控授权用户。向本地网络访问控制模块发送启动受控授权用户访问控制消息，携带启动的策略和相关信息。其中上行速率控制和下行速率控制为必选策略，访问时长和访问总流量为可选。

步骤 S430，如果接收到授权内网用户申请，则根据内网授权判决算法，给予内网授权，并根据配置生成内网授权信息，修改通过内网授权的用户类型为内网授权用户。

具体的，内网授权信息可包括用户标识和对应的用户类型。可将内网授权信息传递至内网授权用户记录表，更新内网授权用户记录表，新增或变更用户记录，并将用户记录的用户类型设置为内网授权用户。启动内网授权用户的访问控制功能，本地网络访问控制模块停止原来的受控授权用户访问控制功能。

本实施例中，对于不同用户类型的用户申请，采取了不同的授权判决算法。且存在多个不同类型的表，进行相应的更新，使得用户类型的授权灵活有序。通过不同的授权判决算法对允许访问子网、访问速率、访问时长和访问总流量进行授权限制。

在一个实施例中，用户记录表分为 DMZ 授权访客用户记录表、受控授权用户记录表和内网授权用户记录表，方法还包括：根据用户类型的更新修改对应类型的用户记录表的用户记录。

具体的，DMZ 授权访客用户记录表包括用户标识、用户移动网基站信息和访客授权信息。访客授权信息，包含允许访问的子网列表及下一跳地址、用户上行访问速率、用户下行访问速率、用户访问时长、用户访问总流量配额等信息。受控授权用户记录表包括用户标识、用户移动网基站信息和受控授权信息。受控授权信息，包含用户上行访问速率、用户下行访问速率、用户访问时长、用户访问总流量配额等信息。内网授权用户记录表包括用户标识、用户移动网基站信息和内网授权信息。内网授权信息，包含允许访问的子网列表及下一跳地址、用户上行访问速率、用户下行访问速

率等信息。

在一个实施例中，用户记录表记录了移动网基站 IP 地址和移动网基站用户信息，所述移动网基站用户信息包括所述移动网基站 IP 地址和移动网基站隧道标识 TEID。

具体的，用户记录表中的用户标识即为用户终端在移动网的 IP 地址，即移动网基站 IP 地址，移动网基站用户信息包含移动网基站 eNB 的 IP 地址和用户终端的移动网基站隧道标识 TEID，两者进行了关联。对于用户记录表分为 DMZ 授权访客用户记录表、受控授权用户记录表和内网授权用户记录表时，DMZ 授权访客用户记录表，包括用户标识、用户移动网基站信息和 DMZ 访客授权信息。DMZ 访客授权信息，包含允许访问的子网列表及下一跳地址、用户上行访问速率、用户下行访问速率、用户访问时长、用户访问总流量配额等信息。受控授权用户记录表，包括用户标识、用户移动网基站信息和受控授权信息。受控授权信息，包含用户上行访问速率、用户下行访问速率、用户访问时长、用户访问总流量配额等信息。内网授权用户记录表，包括用户标识、用户移动网基站信息和内网授权信息。内网授权信息，包含允许访问的子网列表及下一跳地址、用户上行访问速率、用户下行访问速率等信息。

在一个实施例中，所述方法还包括：接收本地网络下行报文，将本地网络下行报文中携带的设备 IP 地址和映射端口号还原为用户终端的源 IP 地址和源端口号，根据用户终端的移动网基站隧道标识打包成 S1-U 下行报文发送至移动网基站。

具体的，本地网络下行报文是本地网络发给用户终端的回应报文，其中携带了设备 IP 地址和映射端口号，需要转换为用户终端的源 IP 地址和源端口号才能转发至用户终端。

在一个实施例中，接收本地网络下行报文的步骤之后，还包括：

根据本地网络下行报文对应的用户类型申请对应类型的下行转发许可，如果申请成功，则进入将本地网络下行报文中携带的设备 IP 地址和映射端口号还原为用户终端的源 IP 地址和源端口号的步骤，否则丢弃本地网络下行报文。

具体的，申请对应类型的下行转发许可时申请请求携带待转发字节数，如果申请成功，则将本地网络下行报文拆解，获取其中携带的设备 IP 地址和映射端口号，转换为用户源 IP 地址和源端口号，并重新封装成 S1-U 下行报文，并转发至基站 eNB。基站 eNB 收到 S1-U 下行报文后，转化为空口报文发送至用户终端。如果没有申请成功，则丢弃本地网络下行报文，达到对本地网络下行报文的控制管理。

在一个实施例中，步骤 S110 之前还包括：预先进行各个参数和规则的配置。

具体的，如配置的参数和规则包括：本地网络访问报文特征、本地网络域名规则、本地网络子网及路由规则、VPN 网关配置、本地网络访问控制规则等，为其他模块提供参数配置接口功能。

在一个具体的实施例中，上述用户终端访问本地网络的方法由新增模块实现，其中新增模块包括本地网络报文识别模块、本地网络域名代理模块、本地网络访问处理模块、本地网络访问控制模块、本地网络访问授权模块和用户信息管理模块。用户终端查询本地网络域名时序图如图 9 所示，由本地网络域名代理模块构造 DNS 查询响应，具体描述如下：

401UE 发送空口报文携带用户报文即 DNS 查询报文给 eNB，查询本地网络域名；

402eNB 收到后提取用户报文，打包成 S1-U 上行报文发送至本地网络报文识别模块；

403 本地网络报文识别模块逐包分析 S1-U 报文内容，识别出 DNS 查询报文；

404 本地网络报文识别模块根据配置的本地网络域名规则，识别出本地网络域名的 DNS 查询报文；

405 本地网络报文识别模块，将本地网络域名的 DNS 查询报文向本地网络域名代理模块转发，其他 DNS 查询报文继续发往核心网；

406 本地网络域名代理模块构造 DNS 查询响应报文，携带本地网络 IP 地址；

407 本地网络域名代理模块向用户信息管理模块获取用户移动网基站信息；

408 本地网络域名代理模块将 DNS 查询响应报文打包成 S1-U 报文，发给 eNB；

409eNB 收到 S1-U 报文，提取出用户报文即 DNS 查询响应报文，打包成空口报文发给 UE。

在一个具体的实施例中，用户终端访问本地网络 DMZ 子网的上行报文的时序图 10 示例，具体描述如下：

501UE 从空口发送用户上行报文；

502eNB 收到后提取用户报文，打包成 S1-U 上行报文发送；

503 本地网络报文识别模块，根据配置的本地网络访问报文特征，逐包比对，识别出本地网络访问报文；

504 本地网络报文识别模块转发本地网络访问报文至本地网络访问处理模块；

505 本地网络访问处理模块检查目的子网，识别出是 DMZ 子网；

506本地网络访问处理模块检查是否在 DMZ 授权访客用户记录表中；

507本地网络访问处理模块，对不在 DMZ 授权访客用户记录表中的访客，可向用户信息管理模块发起携带用户标识的 DMZ 授权访客用户申请，获取 DMZ 访客授权信息；

508 本地网络访问处理模块对 DMZ 授权访客用户检查目的地址所在子网是否在允许访问的子网列表中，对于未授权的访客或者未授权的子网访问，报文直接丢弃；

509本地网络访问处理模块向本地网络访问控制模块获取访客上行转发许可，携带待转发字节数；

510 本地网络访问处理模块，将报文拆包，进行端口地址转换，并重新封装成本地网络报文。如果未获转发许可，则报文直接丢弃。

511本地网络访问处理模块将打包好的本地网络报文，发给目的地址所在子网对应的下一跳地址。

在一个具体的实施例中，本地网络 DMZ 服务器返回给 UE 的回应报文，转发时也需要申请访客下行转发许可，图 11 为 用户终端访问本地网络 DMZ 下行报文时序图示例，具体描述如下：

601本地网络访问处理模块收到本地网络 DMZ 的报文，即用户下行报文；

602本地网络访问处理模块向本地网络访问控制模块获取访客下行转发许可，携带待转发字节数；

603 本地网络访问处理模块，将报文拆包，进行端口地址转换并重新封装成 S1-U 下行用户报文。未获转发许可，报文直接丢弃；

604本地网络访问处理模块将打包好的 S1-U 下行用户报文，发给 eNB；

605eNB 收到 S1-U 报文，将用户下行报文从空口发送给 UE。

用户终端访问本地网络 DMZ，需要申请访客授权，申请过程可以在本地网络域名响应过程中触发，也可以本地网络 DMZ 访问过程中触发，在一个具体的实施例中，本地网络 DMZ 访客授权时序图 12 示例，具体描述如下：

701用户信息管理模块向本地网络访问授权模块发起 DMZ 授权访客用户申请；

702本地网络访问授权模块根据 DMZ 访客授权判决算法，给予 DMZ 访客授权，并根据配置生成 DMZ 访客授权信息；

703 本地网络访问授权模块返回 DMZ 授权访客用户申请响应；

704用户信息管理模块检查授权结果，保存 DMZ 访客授权信息，加入到授权访客用户记录表；

705用户信息管理模块向本地网络访问控制模块发送启动 DMZ 授权访客用户访问控制消息，携带启动的策略和相关信息，其中上行速率控制和下行速率控制为必选策略，访问时长和访问总流量为可选。

用户终端访问本地网络内网子网，需要进行内网身份认证，内网身份认证的具体过程可根据需要自定义，本方案不作限定。内网身份认证成功前，本地网络访问授权模块给予受控授权，报文转发至 VPN 网关，称为受控转发，此时用户为受控授权用户；本地网络访问授权模块获知用户身份为内部用户时，根据内网授权判决算法给予内网授权，报文允许转发到授权子网，称为授权转发，此时用户变更为授权内网用户。在一个具体的实施例中，用户终端访问本地网络内网上行报文时序图如图 13 所示，具体描述如下：

801UE 从空口发送用户上行报文；

802eNB 收到后打包成 S1-U 上行报文发送；

803本地网络报文识别模块，根据配置的本地网络访问报文特征，逐包比对，识别出本地网络访问报文；

804本地识别模块转发本地网络访问报文给本地网络访问处理模块；

805 本地网络访问处理模块检查目的子网，识别出是内网子网；

806本地网络访问处理模块检查受控授权用户记录表和内网授权用户记录表；

807本地网络访问处理模块，对不存在上述记录表中的用户，向用户信息管理模块发送携带用户标识的用户类型更新申请，获取用户授权信息；

808 本地网络访问处理模块确认用户类型是受控授权用户还是授权内网用户，以便后续执行不同的策略处理；

809 本地网络访问处理模块对授权内网用户，检查目的地址所在子网是否属于授权子网列表，如果不属于，直接丢弃报文，如果属于，则进入下一步；

810本地网络访问处理模块，对受控授权用户，向本地网络访问控制模块获取受控上行转发许可，携带转发字节数，对授权内网用户，向本地网络访问控制模块获取授权上行转发许可，携带转发字节数。

811 本地网络访问处理模块，将报文拆包，进行端口地址转换，并重新封装成本地网络报文，未获转发许可，则报文直接丢弃。

812本地网络访问处理模块将打包好的本地网络报文，对于受控授权用户，发给VPN 网关，对于授权内网用户，发给目的地址所在子网对应的下一跳地址。

本地网络内网子网服务器或者 VPN 网关返回给 UE 的回应报文，转发时也需要申请下行转发许可，根据不同的用户类型，过程略有区别，用户终端访问本地网络内网下行报文时序图如图 14 所示，具体描述如下：

901本地网络访问处理模块收到来自本地网络内网或者 VPN 网关的本地网络报文，即用户下行报文；

902本地网络访问处理模块检查用户记录类型是受控授权用户还是授权内网用户；

903本地网络访问处理模块，对受控授权用户，向本地网络访问控制模块获取受控下行转发许可，携带转发字节数，对授权内网用户，向本地网络访问控制模块获取授权下行转发许可，携带转发字节数。

904 本地网络访问处理模块，将报文拆包，进行端口地址转换并重新封装成 S1-U 下行用户报文。未获转发许可，报文直接丢弃。

905本地网络访问处理模块将打包好的 S1-U 下行用户报文，发给 eNB。

906eNB 收到 S1-U 报文，将用户下行报文从空口发送给 UE。

本地网络访问授权模块根据内网授权判决算法，对内部身份用户进行判决给予授权，内网授权判决算法可结合当前的授权内网访问人数、配置的授权内网访问人数门限和当前的授权内网访问总速率、配置的授权内网访问总速率门限等因素。

对于判决为不给予内网授权的用户，仍保持受控授权用户记录类型；判决为授予内网授权的用户，将由原来的受控授权用户类型变更为授权内网用户类型。即使经过本地网络认证过的内网身份用户，如果本地网络访问授权模块未给予内网授权，仍为受控授权用户类型。

图 15 为本地网络内网授权时序图，用户终端将用户终端标识，即用户终端在移动网的 IP 地址，通知 VPN 网关，VPN 网关通知给本地网络访问授权模块，具体描述如下：

1001 用户初始访问本地网络内网时，用户信息管理模块向本地网络访问授权模

块发起受控授权用户申请；

1002 本地网络访问授权模块根据受控授权判决算法，给予受控授权，并根据配置生成受控授权信息；

1003 本地网络访问授权模块返回受控授权用户申请响应；

1004 用户信息管理模块检查受控授权结果，保存为受控授权用户信息，加入到受控授权用户记录表；

1005 用户信息管理模块向本地网络访问控制模块发送启动受控授权用户访问控制消息，携带启动的策略和相关信息，其中上行速率控制和下行速率控制为必选策略，访问时长和访问总流量为可选；

1006 用户终端与本地网络内网认证系统进行内网认证，本步骤不作限定。

1007 用户终端将用户标识发给 VPN 网关，本步骤可选；

1008 VPN 网关通知本地网络访问授权模块，携带用户标识，本步骤可选；

1009 本地网络访问授权模块获知该用户已通过内网认证，用户身份为内部用户；

1010 本地网络访问授权模块根据内网授权判决算法，给予内网授权，并根据配置生成内网授权信息；

1011 本地网络访问授权模块向用户信息管理模块发送授权内网用户通知，携带授权信息；

1012 用户信息管理模块将用户从受控授权用户记录修改为授权内网用户记录，保存授权信息，并加入到内网授权用户记录表，同时从受控授权用户记录表中删除；

1013 用户信息管理模块通知本地网络访问控制模块启动内网授权用户的访问控制功能，本地网络访问控制模块停止原来的受控授权用户访问控制功能。

在一个实施例中，如图 16 所示，提供了一种用户终端访问本地网络的装置，包括：

本地网络报文识别模块 520，用于接收 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络访问报文。

本地网络访问处理模块 530，用于确定本地网络访问报文对应的用户终端的用户类型，根据用户类型和所述本地网络访问报文中的目的地址验证用户终端的本地网络访问权限，如果验证通过，则将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地

网络报文转发至目的地址所在子网的下一跳地址。

在一个实施例中，本地网络报文识别模块 520 还用于接收 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络域名的 DNS 查询报文。如图 17 所示，所述装置还包括：

本地网络域名代理模块 540，用于根据本地网络域名的 DNS 查询报文构造携带本地网络 IP 地址的 DNS 响应报文，将 DNS 响应报文返回至终端，本地网络 IP 地址作为目的地址携带在本地网络访问报文中。

在一个实施例中，如图 18 所示，本地网络访问处理模块 530 包括：

信息确定单元 531，用于提取本地网络访问报文携带的用户标识，确定用户标识对应的用户类型，确定目的地址所在子网和子网类型。

第一验证单元 532，用于判断用户类型对应的用户访问权限是否符合目的地址所在子网类型对应的访问权限，如果符合，则进入第二验证单元。

第二验证单元 533，用于判断目的地址所在子网是否为允许访问的子网，如果是，则本地网络访问权限通过验证，否则本地网络访问权限未通过验证。

在一个实施例中，如图 19 所示，装置还包括：

本地网络访问控制模块 550，用于根据当前访问状态判断是否为本地网络访问报文提供转发许可，如果本地网络访问报文获得转发许可，则进入本地网络访问处理模块中将所述 S1-U 上行报文拆解，如果本地网络访问报文未获得转发许可，则丢弃本地网络访问报文。

在一个实施例中，如图 20 所示，装置还包括：

本地网络访问授权模块 560，用于如果用户类型对应的用户访问权限不符合目的地址所在子网类型对应的访问权限，则根据授权判决算法更新用户终端的用户类型。

在一个实施例中，本地网络访问处理模块 530 还用于根据本地网络访问报文携带的所述用户终端的用户标识查询用户记录表，如果用户标识在所述用户记录表中，则得到用户记录表中记录的用户类型，如果用户标识在用户记录表中，则用户类型为无权限用户。

在一个实施例中，本地网络分为 DMZ 区和内网，子网类型分为 DMZ 子网和内网子网，用户类型包括 DMZ 授权访客用户、受控授权用户和授权内网用户，如图 21 所示，第一验证单元 532 包括以下单元中的至少一个：

DMZ 子网验证单元 532a，用于如果目的地址所在子网类型为 DMZ 子网，且用户类型为 DMZ 授权访客用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

内网子网第一验证单元 532b，用于如果目的地址所在子网类型为内网子网，用户类型为受控授权用户，则判断用户类型对应的用户访问权限不符合所述目的地址所在子网类型对应的访问权限，将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至 VPN 网关。

内网子网第二验证单元 532c，用于如果目的地址所在子网类型为内网子网，用户类型为授权内网用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

在一个实施例中，如图 22 所示，本地网络访问处理模块 530 还包括：

授权申请单元 534，所述授权申请单元包括以下单元中的至少一个：

DMZ 授权申请单元 534a，用于如果目的地址所在子网类型为 DMZ 子网，且所述用户类型为非 DMZ 授权访客用户，则发起 DMZ 授权访客用户申请。

受控授权申请单元 534b，用于如果目的地址所在子网类型为内网子网，获知用户身份为内部用户前，则发起受控授权用户申请。

授权内网申请单元 534c，用于如果目的地址所在子网类型为内网子网，获知用户身份为内部用户且所述用户类型为受控授权用户，则发起授权内网用户申请。

在一个实施例中，如图 23 所示，本地网络访问授权模块 560 包括以下单元中的至少一个：

DMZ 授权单元 560a，用于如果接收到 DMZ 授权访客用户申请，则根据 DMZ 访客授权判决算法给予 DMZ 访客授权，并根据配置生成 DMZ 访客授权信息，修改通过 DMZ 访客授权的用户类型为 DMZ 授权访客用户。

受控授权单元 560b，用于如果接收到受控授权用户申请，则根据受控授权判决算法，给予受控授权，并根据配置生成受控授权信息，修改通过受控授权的用户类型为受控授权用户。

授权内网单元 560c，用于如果接收到授权内网用户申请，则根据内网授权判决算法，给予内网授权，并根据配置生成内网授权信息，修改通过内网授权的用户类型

为内网授权用户。

在一个实施例中，用户记录表分为 DMZ 授权访客用户记录表、受控授权用户记录表和内网授权用户记录表，如图 24 所示，所述装置还包括：

用户信息管理模块 570，用于根据用户类型的更新修改对应类型的用户记录表的用户记录。

在一个实施例中，提供了一种用户终端访问本地网络的装置，包括处理器以及存储有所述处理器可执行指令的存储器，当指令被处理器执行时，执行如下操作：

接收用户平面 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络访问报文。

确定本地网络访问报文对应的用户终端的用户类型，根据用户类型和本地网络访问报文中的目的地址验证用户终端的本地网络访问权限。

如果验证通过，则将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至目的地址所在子网的下一跳地址。

在一个实施例中，当所述指令被处理器执行时，还执行如下操作：

接收 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络域名的 DNS 查询报文。

根据本地网络域名的 DNS 查询报文构造携带本地网络 IP 地址的 DNS 响应报文，将 DNS 响应报文返回至终端，本地网络 IP 地址作为目的地址携带在本地网络访问报文中。

在一个实施例中，处理器所执行的确定所述本地网络访问报文对应的用户终端的用户类型，根据用户类型和所述本地网络访问报文中的目的地址验证用户终端的本地网络访问权限的操作包括：

提取本地网络访问报文携带的用户标识，确定用户标识对应的用户类型；

确定目的地址所在子网和子网类型；

判断用户类型对应的用户访问权限是否符合目的地址所在子网类型对应的访问权限，如果符合，则判断目的地址所在子网是否为允许访问的子网；

如果是允许访问的子网，则本地网络访问权限通过验证，否则本地网络访问权限

未通过验证。

在一个实施例中，本地网络分为 DMZ 区和内网，目的地址所在子网类型分为 DMZ 子网和内网子网，用户类型包括 DMZ 授权访客用户、受控授权用户和授权内网用户，处理器所执行的判断用户类型对应的用户访问权限是否符合目的地址所在子网类型对应的访问权限的操作包括以下操作中的至少一个：

如果目的地址所在子网类型为 DMZ 子网，且用户类型为 DMZ 授权访客用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

如果目的地址所在子网类型为内网子网，用户类型为受控授权用户，则判断用户类型对应的用户访问权限不符合所述目的地址所在子网类型对应的访问权限，将 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至 VPN 网关。

如果目的地址所在子网类型为内网子网，用户类型为授权内网用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限。

在一个实施例中，提供了一种移动网基站，移动网基站包括上述任一实施例所述的用户终端访问本地网络的装置。

具体的，将用户终端访问本地网络的装置部署在移动网基站上，不需要新增设备，只需要对移动网基站 eNB 进行软件升级。如图 25 所示，为一个具体的实施例中移动网基站部署了用户终端访问本地网络的装置后的内部结构示意图。

在一个实施例中，如图 26 所示，提供了一种用户终端访问本地网络的系统，所述系统包括基站 eNB610 和服务器 620，服务器包括上述任一实施例所述的用户终端访问本地网络的装置 621。

具体的，将用户终端访问本地网络的装置部署在服务器上，对现有的基站不需要做任何改动，做到透明部署。如图 27 所示，为本实施例中用户终端访问本地网络的系统的内部结构示意图。

在一个实施例中，提供了一种用户终端访问本地网络的系统，系统包括基站 eNB 和服务器，基站 eNB 用于接收 S1-U 上行报文，识别并拦截 S1-U 上行报文中的本地网络访问报文，将本地网络访问报文发送至服务器，服务器用于确定本地网络访问报文对应的用户终端的用户类型，根据用户类型确定用户终端的本地网络访问权限，如

果本地网络访问权限为允许访问本地网络访问报文中的目的地址所在子网，则将S1-U上行报文拆解，将用户IP报文中的源IP地址和源端口号转换为设备IP地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至目的地址所在子网的下一跳地址。

具体的，本地网络报文识别模块部署在移动网基站上，其他模块部署在一个服务器，则只有符合本地网络报文特征和本地网络域名特征的报文才转给服务器处理，可以降低新增设备的处理开销。如图28所示，为本实施例中用户终端访问本地网络的系统的内部结构示意图。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述程序可存储于一计算机可读取存储介质中，如本发明实施例中，该程序可存储于计算机系统的存储介质中，并被该计算机系统中的至少一个处理器执行，以实现包括如上述各方法的实施例的流程。其中，所述存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

工业实用性

本发明实施例提供的技术方案可以应用于通信技术领域。在本发明的实施例中，通过接收S1-U上行报文，识别并拦截S1-U上行报文中的本地网络访问报文，拦截的本地网络访问报文不会发送至核心网减少了访问路径结点，确定本地网络访问报文对应的用户终端的用户类型，根据用户类型和本地网络访问报文中的目的地址验证用户终端的本地网络访问权限；如果验证通过，则将S1-U上行报文拆解，将用户IP

报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至所述目的地址所在子网的下一跳地址，只有验证通过的本地网络访问报文才会进行转发，保证了本地网络信息的安全性，使得用户终端能快速安全的访问本地网络。

权利要求

1、一种用户终端访问本地网络的方法，所述方法包括：

接收用户平面 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络访问报文；

确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限；

如果验证通过，则将所述 S1-U 上行报文拆解，将用户网络协议 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址。

2、根据权利要求 1 所述的方法，其中，所述方法还包括：

接收 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络域名的域名系统 DNS 查询报文；

根据所述本地网络域名的 DNS 查询报文构造携带本地网络 IP 地址的 DNS 响应报文，将所述 DNS 响应报文返回至终端，所述本地网络 IP 地址作为目的地址携带在本地网络访问报文中。

3、根据权利要求 1 所述的方法，其中，所述确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限的步骤包括：

提取所述本地网络访问报文携带的用户标识，确定所述用户标识对应的用户类型；

确定所述目的地址所在子网和子网类型；

判断所述用户类型对应的用户访问权限是否符合所述目的地址所在子网类型对应的访问权限，如果符合，则判断所述目的地址所在子网是否为允许访问的子网；

如果是允许访问的子网，则所述本地网络访问权限通过验证，否则所述本地网络访问权限未通过验证。

4、根据权利要求 1 所述的方法，其中，所述则将所述 S1-U 上行报文拆解的步骤之前，还包括：

根据当前访问状态判断是否为所述本地网络访问报文提供转发许可，如果所述

本地网络访问报文获得转发许可，则进入所述将所述 S1-U 上行报文拆解的步骤；

如果所述本地网络访问报文未获得转发许可，则丢弃所述本地网络访问报文。

5、根据权利要求 3 所述的方法，其中，本地网络分为隔离区 DMZ 区和内网，所述目的地址所在子网类型分为 DMZ 子网和内网子网，所述用户类型包括 DMZ 授权访客用户、受控授权用户和授权内网用户，所述判断所述用户类型对应的用户访问权限是否符合所述目的地址所在子网类型对应的访问权限的步骤包括以下步骤中的至少一个：

如果所述目的地址所在子网类型为 DMZ 子网，且所述用户类型为 DMZ 授权访客用户，则判断所述用户类型对应的用户访问权限符合所述目的地址所在子网类型对应的访问权限；

如果所述目的地址所在子网类型为内网子网，所述用户类型为受控授权用户，则判断所述用户类型对应的用户访问权限不符合所述目的地址所在子网类型对应的访问权限，将所述 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至虚拟专用网络 VPN 网关；

如果所述目的地址所在子网类型为内网子网，所述用户类型为授权内网用户，则判断所述用户类型对应的用户访问权限符合所述目的地址所在子网类型对应的访问权限。

6、根据权利要求 1 所述的方法，其中，所述方法还包括：

接收本地网络下行报文，将所述本地网络下行报文中携带的设备 IP 地址和映射端口号还原为用户终端的源 IP 地址和源端口号，根据用户终端的移动网基站隧道标识打包成 S1-U 下行报文发送至移动网基站。

7、根据权利要求 6 所述的方法，其中，所述接收本地网络下行报文的步骤之后，还包括：

根据本地网络下行报文对应的用户类型申请对应类型的下行转发许可，如果申请成功，则进入所述将所述本地网络下行报文中携带的设备 IP 地址和映射端口号还原为用户终端的源 IP 地址和源端口号的步骤，否则丢弃所述本地网络下行报文。

8、一种用户终端访问本地网络的装置，其中，所述装置包括：

本地网络报文识别模块，设置为接收用户平面 S1-U 上行报文，识别并拦截所述

S1-U 上行报文中的本地网络访问报文；

本地网络访问处理模块，设置为确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限，如果验证通过，则将所述 S1-U 上行报文拆解，将用户网络协议 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址。

9、根据权利要求 8 所述的装置，其中，所述本地网络报文识别模块还设置为接收 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络域名的域名系统 DNS 查询报文；

所述装置还包括：

本地网络域名代理模块，设置为根据所述本地网络域名的 DNS 查询报文构造携带本地网络 IP 地址的 DNS 响应报文，将所述 DNS 响应报文返回至终端，所述本地网络 IP 地址作为目的地址携带在本地网络访问报文中。

10、根据权利要求 8 所述的装置，其中，所述本地网络访问处理模块包括：

信息确定单元，设置为提取所述本地网络访问报文携带的用户标识，确定所述用户标识对应的用户类型，确定所述目的地址所在子网和子网类型；

第一验证单元，设置为判断所述用户类型对应的用户访问权限是否符合所述目的地址所在子网类型对应的访问权限，如果符合，则进入第二验证单元；

第二验证单元，设置为判断所述目的地址所在子网是否为允许访问的子网，如果是，则所述本地网络访问权限通过验证，否则所述本地网络访问权限未通过验证。

11、根据权利要求 8 所述的装置，其中，所述装置还包括：

本地网络访问控制模块，设置为根据当前访问状态判断是否为所述本地网络访问报文提供转发许可，如果所述本地网络访问报文获得转发许可，则进入所述本地网络访问处理模块中将所述 S1-U 上行报文拆解，如果所述本地网络访问报文未获得转发许可，则丢弃所述本地网络访问报文。

12、一种用户终端访问本地网络的装置，其中，包括处理器以及存储有所述处理器可执行指令的存储器，当所述指令被处理器执行时，执行如下操作：

接收用户平面 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络访

问报文；

确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限；

如果验证通过，则将所述 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至所述目的地址所在子网的下一跳地址。

13、根据权利要求 12 所述的装置，其中，当所述指令被处理器执行时，还执行如下操作：

接收 S1-U 上行报文，识别并拦截所述 S1-U 上行报文中的本地网络域名的域名系统 DNS 查询报文；

根据所述本地网络域名的 DNS 查询报文构造携带本地网络 IP 地址的 DNS 响应报文，将所述 DNS 响应报文返回至终端，所述本地网络 IP 地址作为目的地址携带在本地网络访问报文中。

14、根据权利要求 12 所述的装置，其中，所述处理器所执行的确定所述本地网络访问报文对应的用户终端的用户类型，根据所述用户类型和所述本地网络访问报文中的目的地址验证所述用户终端的本地网络访问权限的操作包括：

提取所述本地网络访问报文携带的用户标识，确定所述用户标识对应的用户类型；

确定所述目的地址所在子网和子网类型；

判断所述用户类型对应的用户访问权限是否符合所述目的地址所在子网类型对应的访问权限，如果符合，则判断所述目的地址所在子网是否为允许访问的子网；

如果是允许访问的子网，则所述本地网络访问权限通过验证，否则所述本地网络访问权限未通过验证。

15、根据权利要求 14 所述的装置，其中，本地网络分为隔离区 DMZ 区和内网，所述目的地址所在子网类型分为 DMZ 子网和内网子网，所述用户类型包括 DMZ 授权访客用户、受控授权用户和授权内网用户，所述处理器所执行的判断所述用户类型对应的用户访问权限是否符合所述目的地址所在子网类型对应的访问权限的操作包括以下操作中的至少一个：

如果所述目的地址所在子网类型为 DMZ 子网，且所述用户类型为 DMZ 授权访

客用户，则判断所述用户类型对应的用户访问权限符合所述目的地址所在子网类型对应的访问权限；

如果所述目的地址所在子网类型为内网子网，所述用户类型为受控授权用户，则判断所述用户类型对应的用户访问权限不符合所述目的地址所在子网类型对应的访问权限，将所述 S1-U 上行报文拆解，将用户 IP 报文中的源 IP 地址和源端口号转换为设备 IP 地址和映射端口号，并重新封装成本地网络报文，将所述本地网络报文转发至虚拟专用网络 VPN 网关；

如果所述目的地址所在子网类型为内网子网，所述用户类型为授权内网用户，则判断所述用户类型对应的用户访问权限符合所述目的地址所在子网类型对应的访问权限。

16. 一种计算机存储介质，所述计算机存储介质中存储有计算机可执行的一个或多个程序，所述一个或多个程序被所述计算机执行时使所述计算机执行如根据权利要求 1-7 中任一项所述的用户终端访问本地网络的方法。

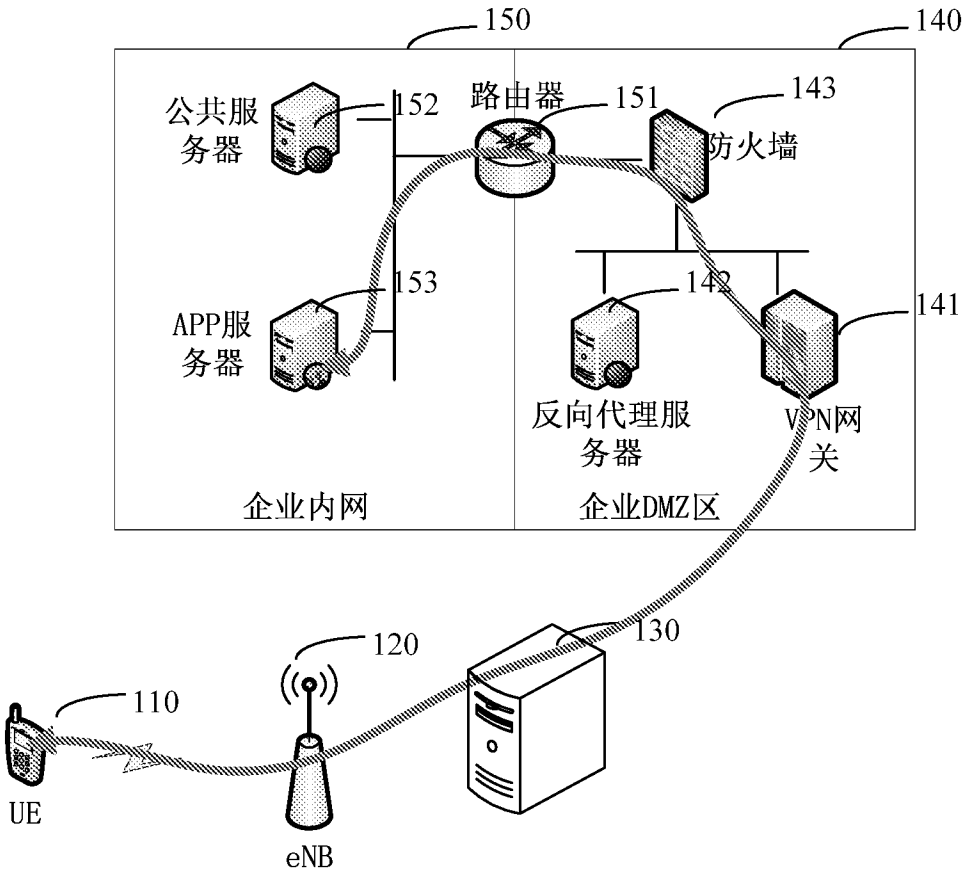
150
140
公共服务器
152
路由器
151
143
防火墙
153
142
141
APP服务器
反向代理服务器
VPN网关
企业内网
企业DMZ区
120
130
110
UE
eNB

图 1

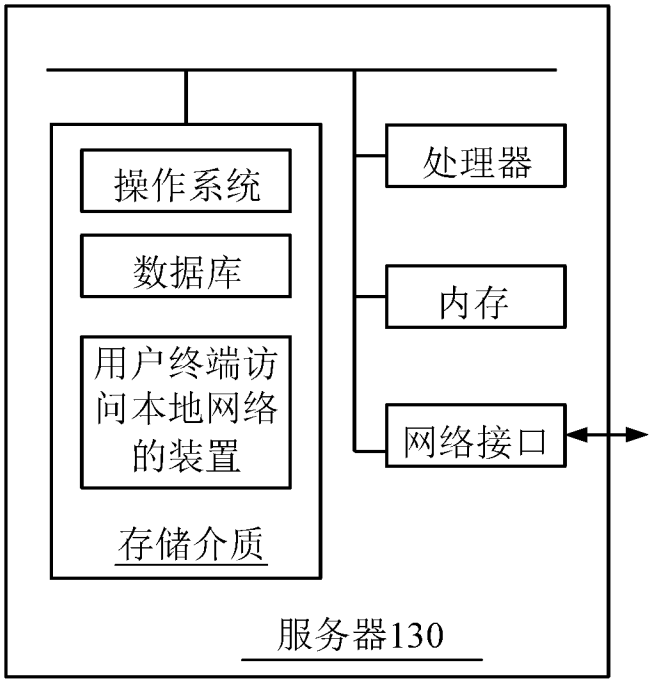

图 2

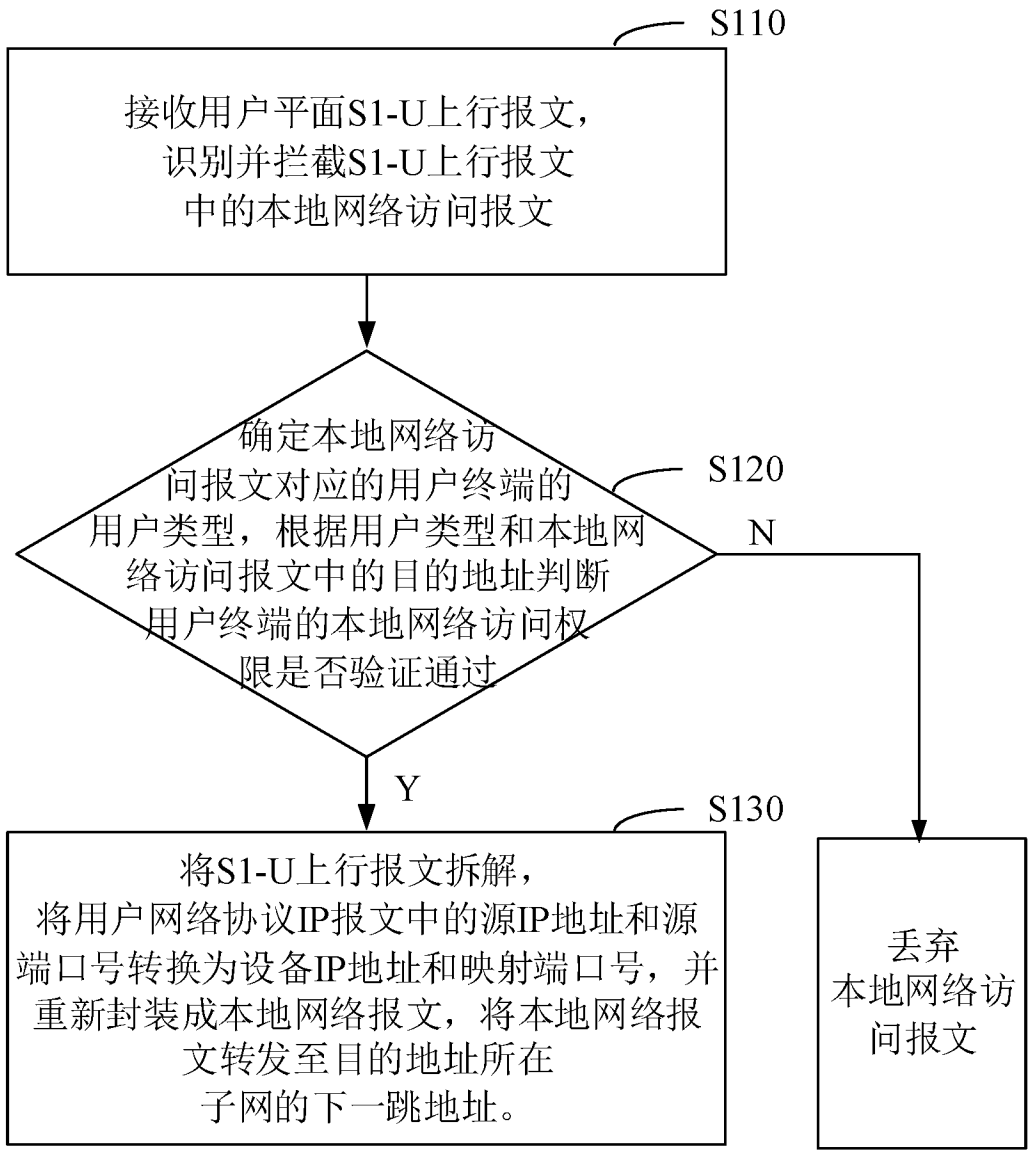
S110
接收用户平面S1-U上行报文，
识别并拦截S1-U上行报文
中的本地网络访问报文
确定本地网络访
问报文对应的用户终端的
用户类型，根据用户类型和本地网
络访问报文中的目的地址判断
用户终端的本地网络访问权
限是否验证通过
S120
N
Y
S130
将S1-U上行报文拆解，
将用户网络协议IP报文中的源IP地址和源
端口号转换为设备IP地址和映射端口号，并
重新封装成本地网络报文，将本地网络报
文转发至目的地址所在
子网的下一跳地址。
丢弃
本地网络访
问报文

图 3

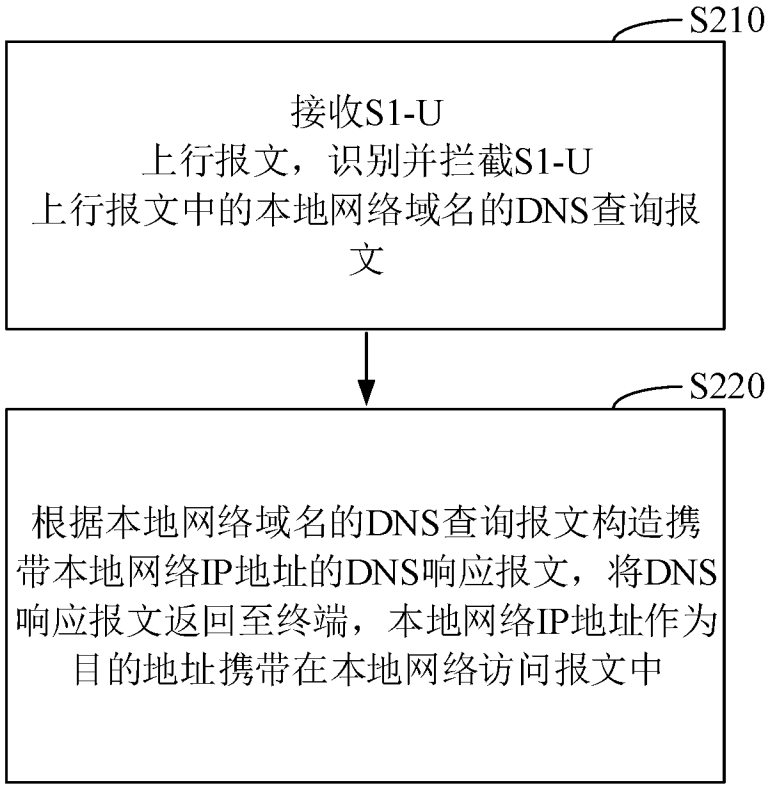
S210
接收S1-U
上行报文，识别并拦截S1-U
上行报文中的本地网络域名的DNS查询报
文
S220
根据本地网络域名的DNS查询报文构造携
带本地网络IP地址的DNS响应报文，将DNS
响应报文返回至终端，本地网络IP地址作为
目的地址携带在本地网络访问报文中

图 4

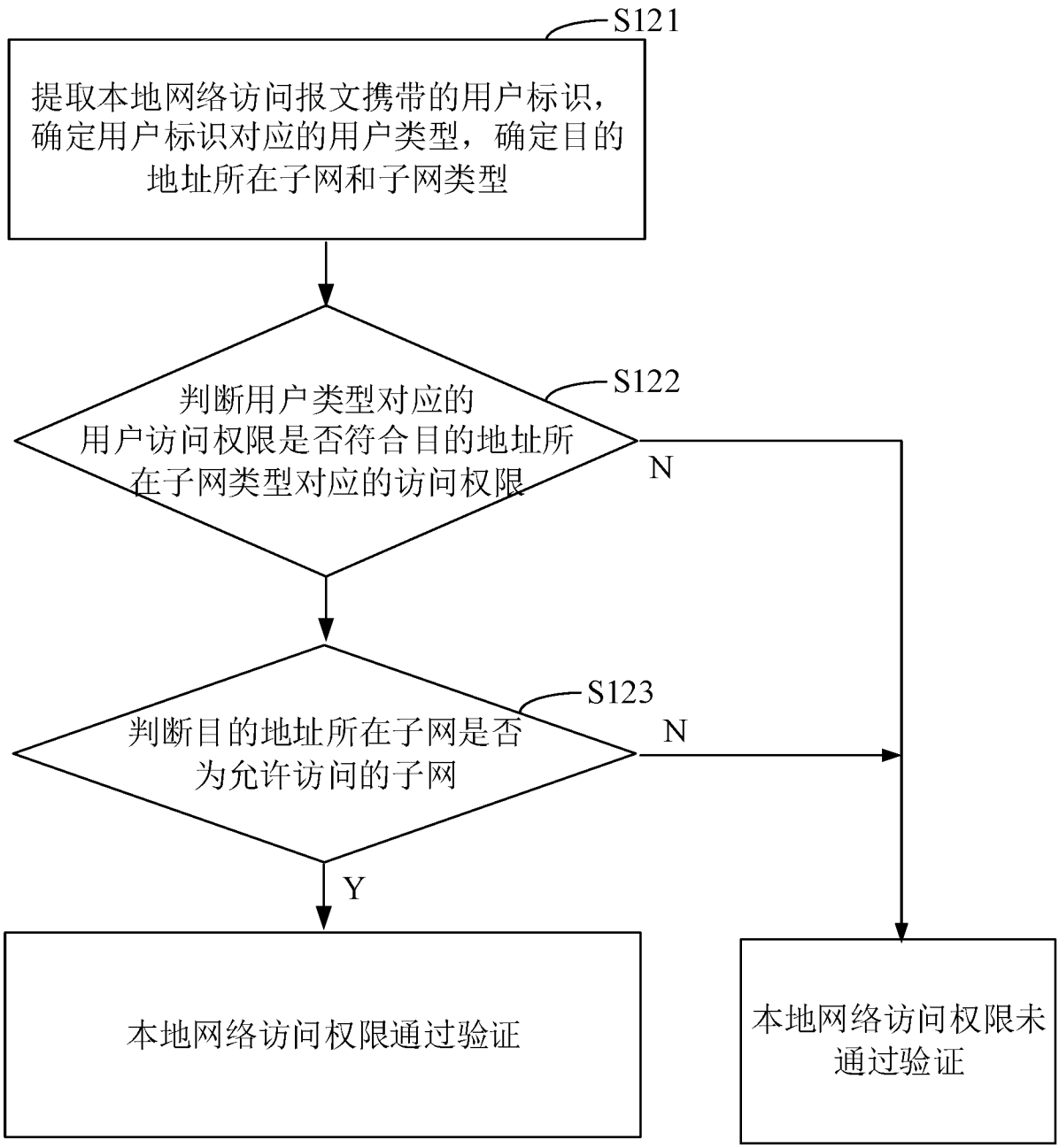
S121
提取本地网络访问报文携带的用户标识，确定用户标识对应的用户类型，确定目的地址所在子网和子网类型
S122
判断用户类型对应的用户访问权限是否符合目的地址所在子网类型对应的访问权限
N
S123
判断目的地址所在子网是否为允许访问的子网
N
Y
本地网络访问权限通过验证
本地网络访问权限未通过验证

图 5

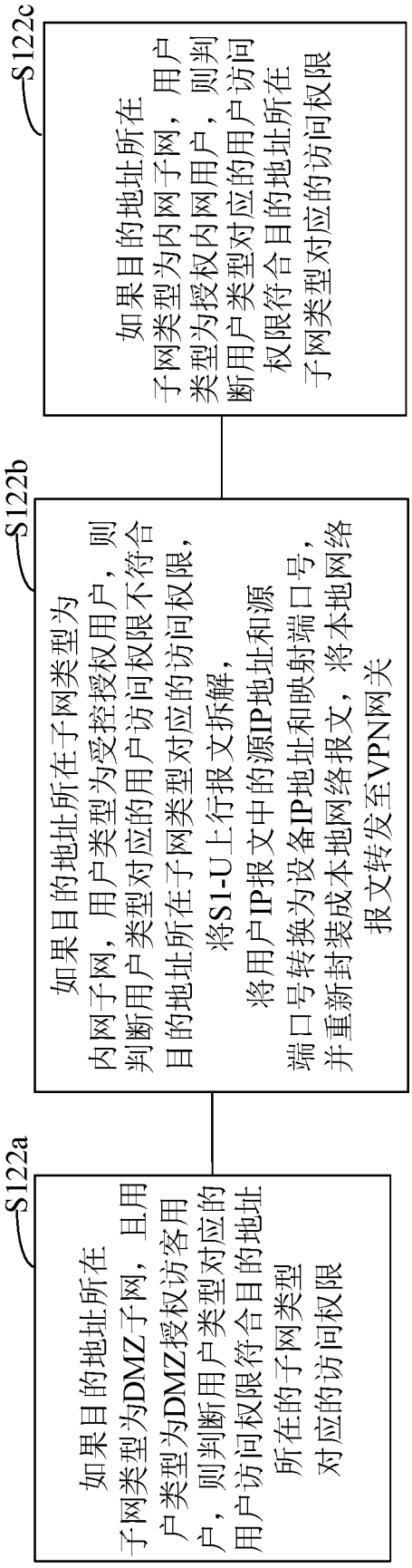
S122a
如果目的地址所在子网类型为DMZ子网，且用户类型为DMZ授权访客用户，则判断用户类型对应的用户访问权限符合目的地址所在的子网类型对应的访问权限
S122b
如果目的地址所在子网类型为内网子网，用户类型为受控授权用户，则判断用户类型对应的用户访问权限不符合目的地址所在子网类型对应的访问权限，将S1-U上行报文拆解，将用户IP报文中的源IP地址和源端口号转换为设备IP地址和映射端口号，并重新封装成本地网络报文，将本地网络报文转发至VPN网关
S122c
如果目的地址所在子网类型为内网子网，用户类型为授权内网用户，则判断用户类型对应的用户访问权限符合目的地址所在子网类型对应的访问权限

图6

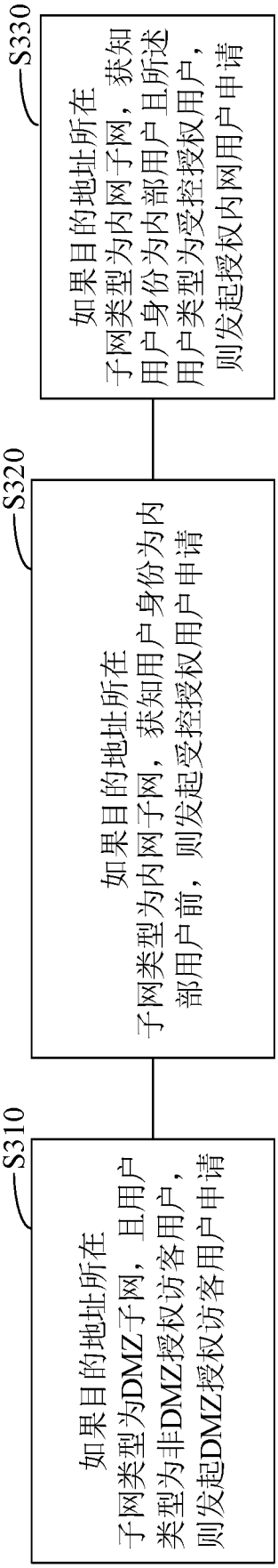
S310
如果目的地址所在子网类型为DMZ子网，且用户类型为非DMZ授权访客用户，则发起DMZ授权访客用户申请
S320
如果目的地址所在子网类型为内网子网，获知用户身份为内部用户前，则发起受控授权用户申请
S330
如果目的地址所在子网类型为内网子网，获知用户身份为内部用户且所述用户类型为受控授权用户，则发起授权内网用户申请

图7

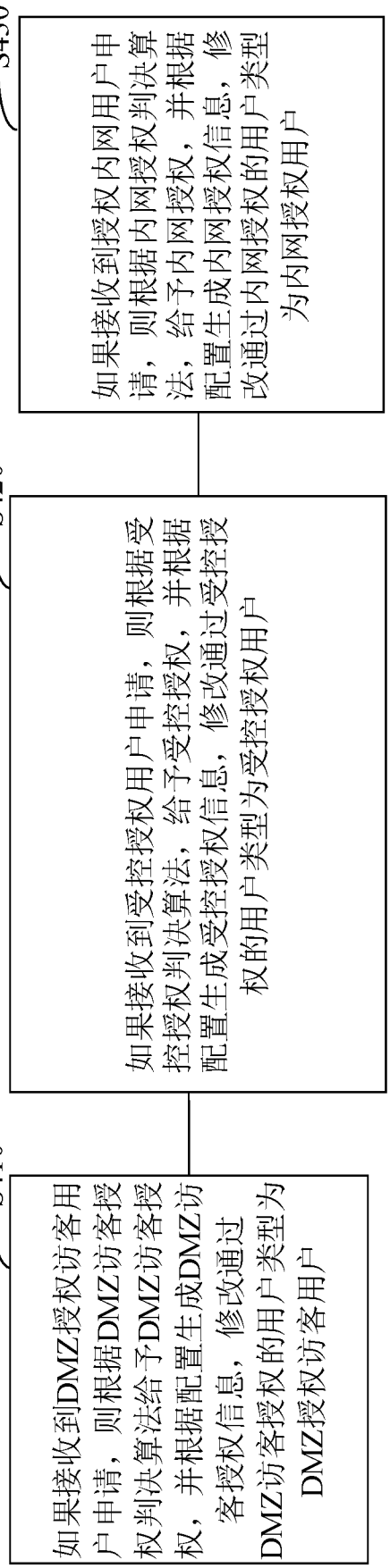
S410
如果接收到DMZ授权访客用户申请，则根据DMZ访客授权判决算法给予DMZ访客授权，并根据配置生成DMZ访客授权信息，修改通过DMZ访客授权的用户类型为DMZ授权访客用户
S420
如果接收到受控授权用户申请，则根据受控授权判决算法，给予受控授权，并根据配置生成受控授权信息，修改通过受控授权的用户类型为受控授权用户
S430
如果接收到授权内网用户申请，则根据内网授权判决算法，给予内网授权，并根据配置生成内网授权信息，修改通过内网授权的用户类型为内网授权用户

图8

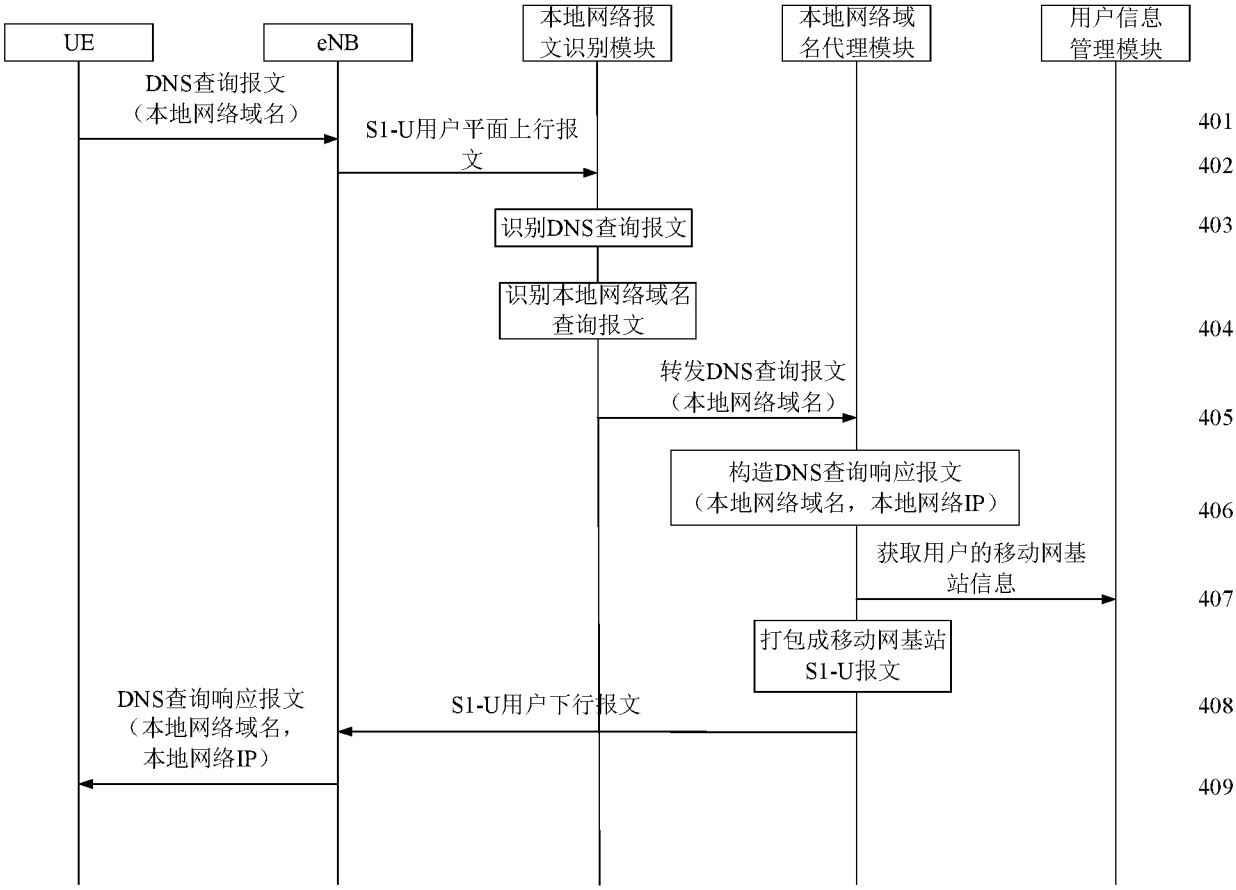
UE
eNB
本地网络报文识别模块
本地网络域名代理模块
用户信息管理模块
DNS查询报文（本地网络域名）
S1-U用户平面上行报文
识别DNS查询报文
识别本地网络域名查询报文
转发DNS查询报文（本地网络域名）
构造DNS查询响应报文（本地网络域名，本地网络IP）
获取用户的移动网基站信息
打包成移动网基站S1-U报文
S1-U用户下行报文
DNS查询响应报文（本地网络域名，本地网络IP）
401
402
403
404
405
406
407
408
409

图 9

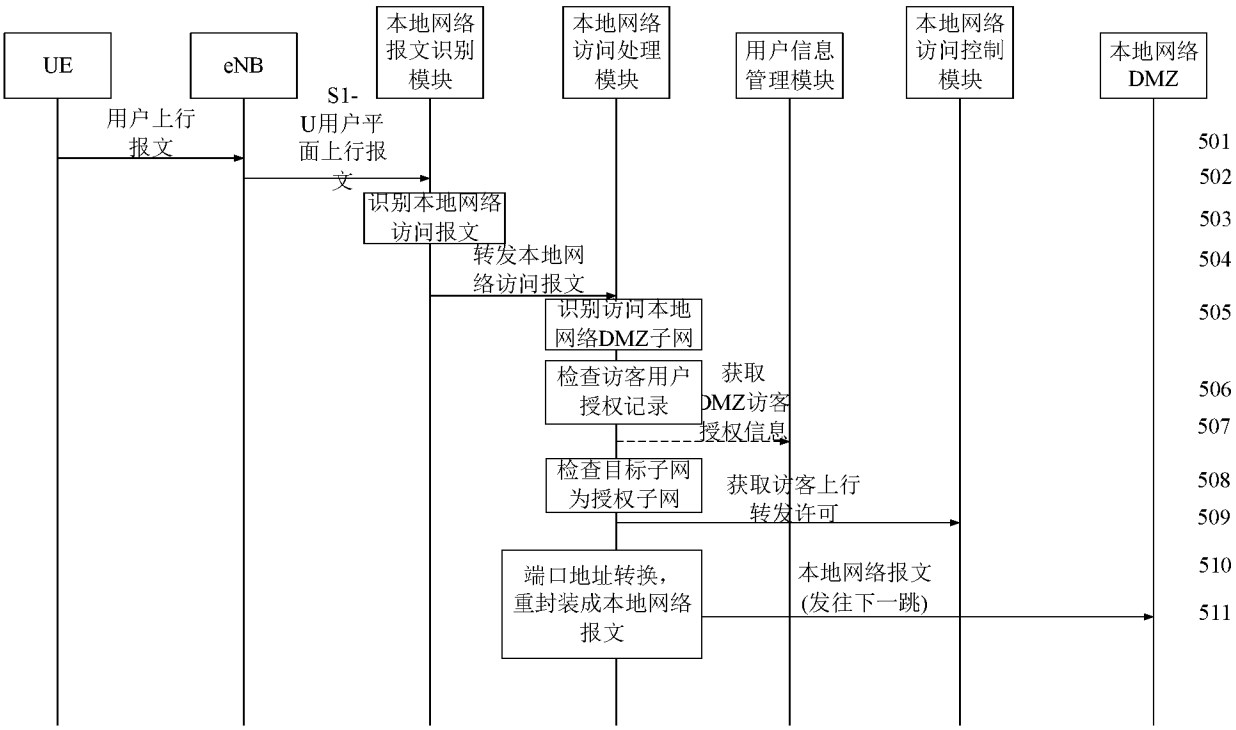
UE
eNB
本地网络报文识别模块
本地网络访问处理模块
用户信息管理模块
本地网络访问控制模块
本地网络DMZ
用户上行报文
S1-U用户平面上行报文
识别本地网络访问报文
转发本地网络访问报文
识别访问本地网络DMZ子网
检查访客用户授权记录
获取DMZ访客授权信息
检查目标子网为授权子网
获取访客上行转发许可
端口地址转换，重封装成本地网络报文
本地网络报文(发往下一跳)
501
502
503
504
505
506
507
508
509
510
511

图 10

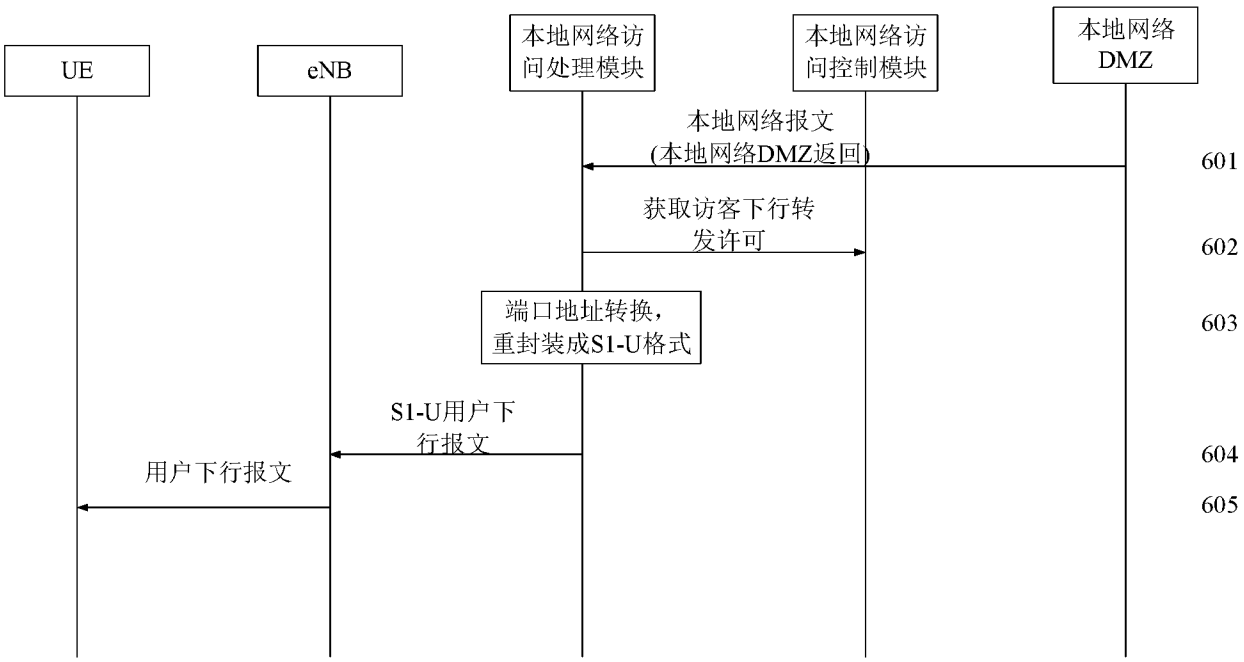
UE
eNB
本地网络访问处理模块
本地网络访问控制模块
本地网络DMZ
本地网络报文(本地网络DMZ返回)
601
获取访客下行转发许可
602
端口地址转换，重封装成S1-U格式
603
S1-U用户下行报文
604
用户下行报文
605

图 11

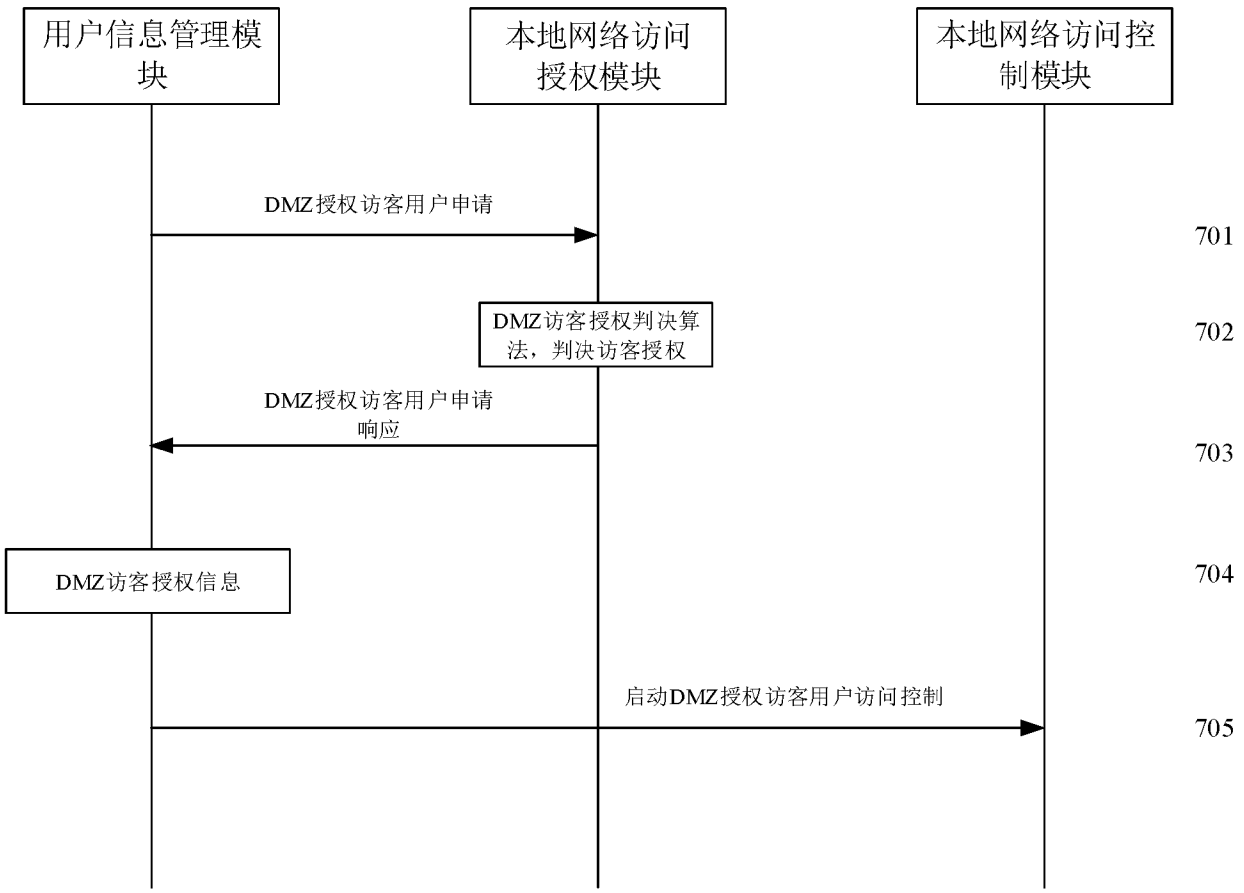
用户信息管理模块
本地网络访问授权模块
本地网络访问控制模块
DMZ授权访客用户申请
701
DMZ访客授权判决算法，判决访客授权
702
DMZ授权访客用户申请响应
703
DMZ访客授权信息
704
启动DMZ授权访客用户访问控制
705

图 12

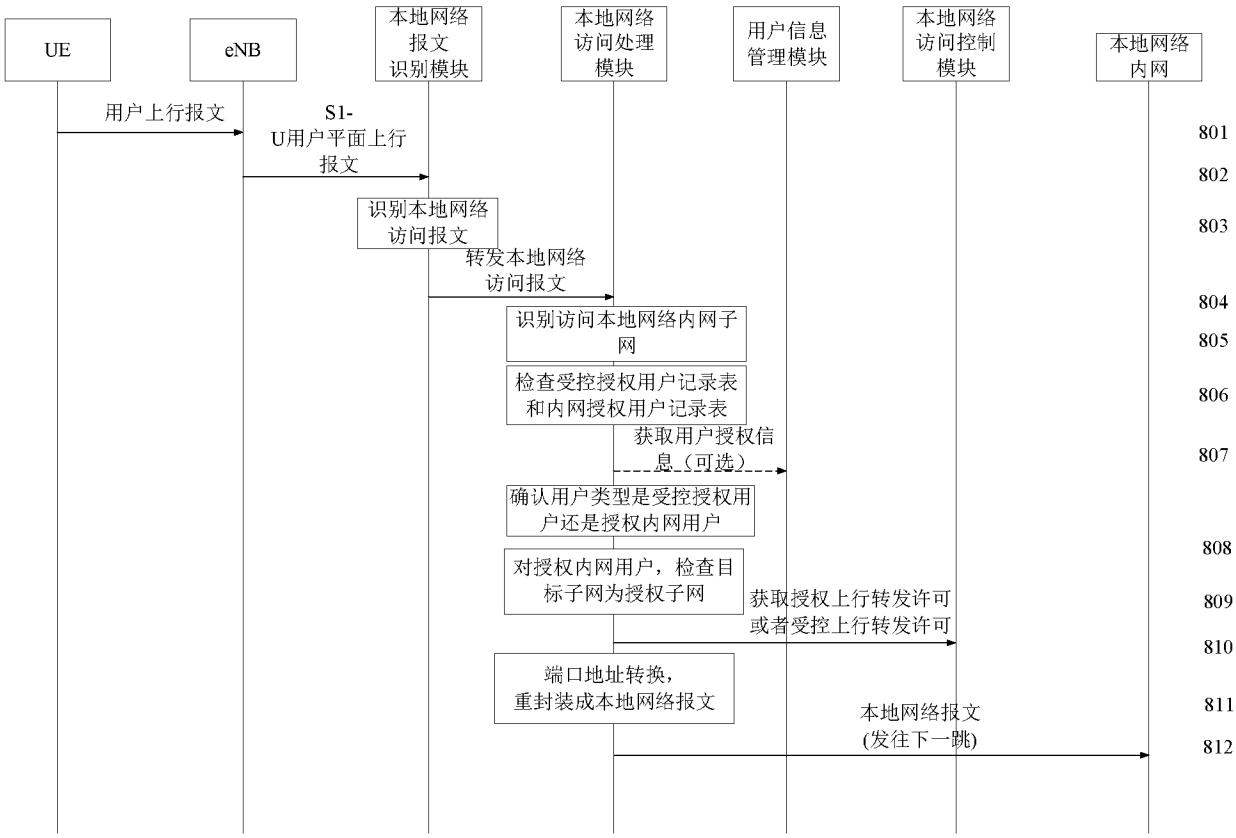
UE
eNB
本地网络报文识别模块
本地网络访问处理模块
用户信息管理模块
本地网络访问控制模块
本地网络内网
用户上行报文
S1-U用户平面上行报文
识别本地网络访问报文
转发本地网络访问报文
识别访问本地网络内网子网
检查受控授权用户记录表和内网授权用户记录表
获取用户授权信息（可选）
确认用户类型是受控授权用户还是授权内网用户
对授权内网用户，检查目标子网为授权子网
获取授权上行转发许可或者受控上行转发许可
端口地址转换，重封装成本地网络报文
本地网络报文(发往下一跳)
801
802
803
804
805
806
807
808
809
810
811
812

图 13

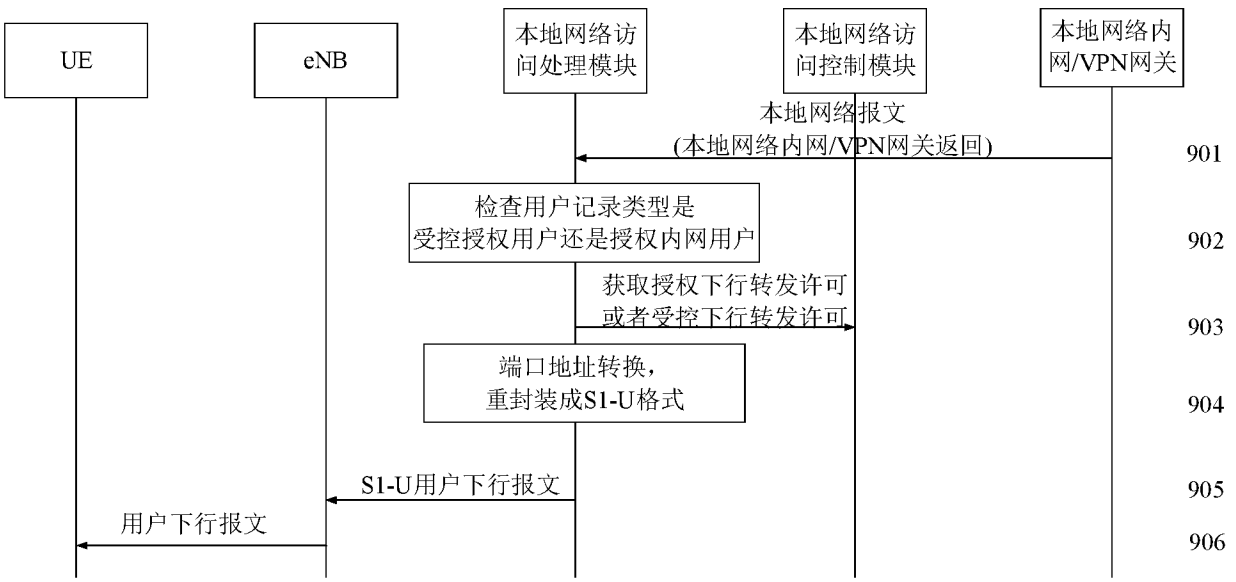
UE
eNB
本地网络访问处理模块
本地网络访问控制模块
本地网络内网/VPN网关
本地网络报文(本地网络内网/VPN网关返回)
检查用户记录类型是受控授权用户还是授权内网用户
获取授权下行转发许可或者受控下行转发许可
端口地址转换，重封装成S1-U格式
S1-U用户下行报文
用户下行报文
901
902
903
904
905
906

图 14

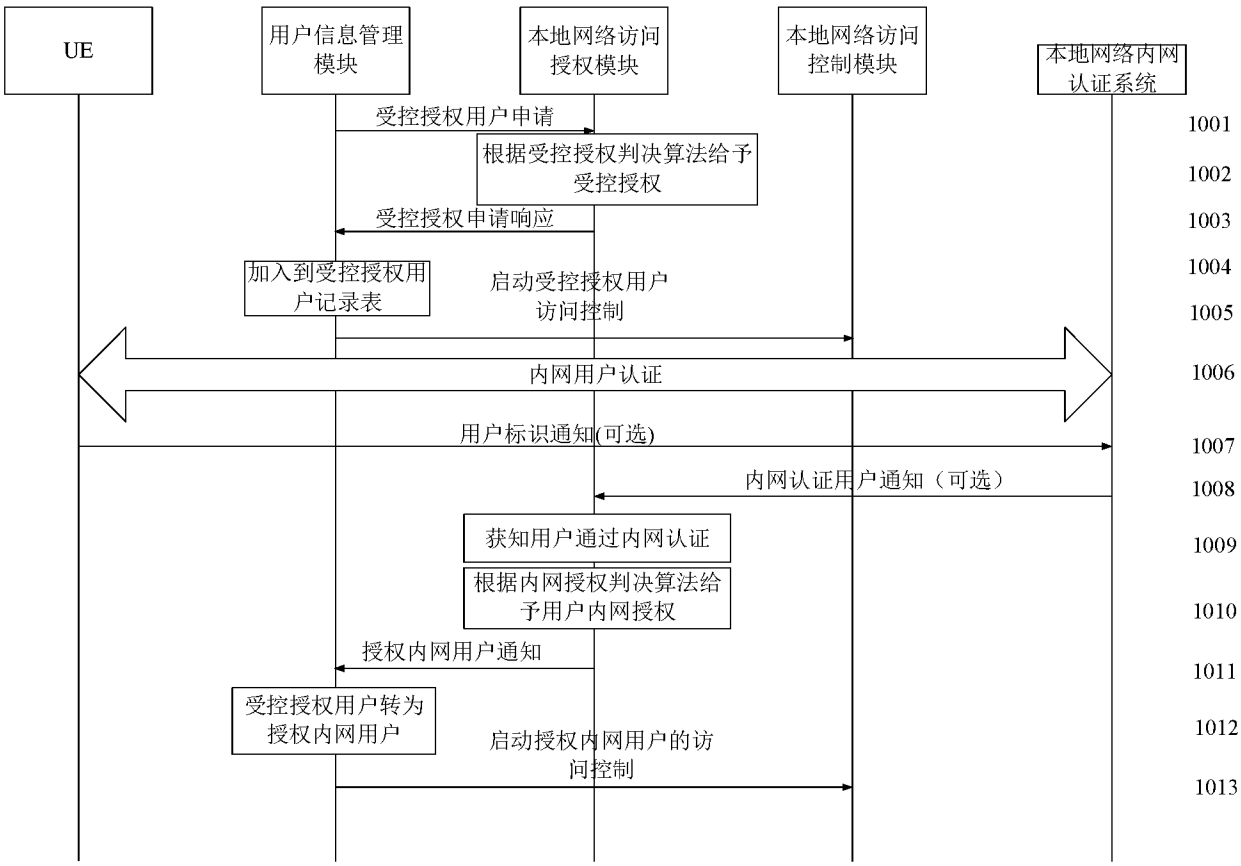
UE
用户信息管理模块
本地网络访问授权模块
本地网络访问控制模块
本地网络内网认证系统
受控授权用户申请
1001
根据受控授权判决算法给予受控授权
1002
受控授权申请响应
1003
加入到受控授权用户记录表
1004
启动受控授权用户访问控制
1005
内网用户认证
1006
用户标识通知(可选)
1007
内网认证用户通知（可选）
1008
获知用户通过内网认证
1009
根据内网授权判决算法给予用户内网授权
1010
授权内网用户通知
1011
受控授权用户转为授权内网用户
1012
启动授权内网用户的访问控制
1013

图 15

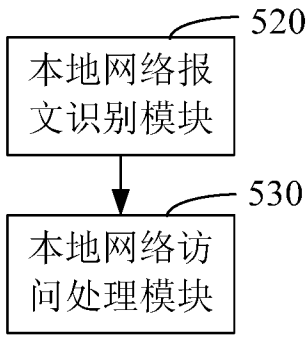
520
本地网络报文识别模块
530
本地网络访问处理模块

图 16

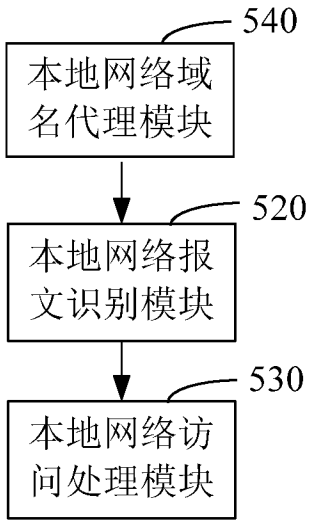
540
本地网络域名代理模块
520
本地网络报文识别模块
530
本地网络访问处理模块

图 17

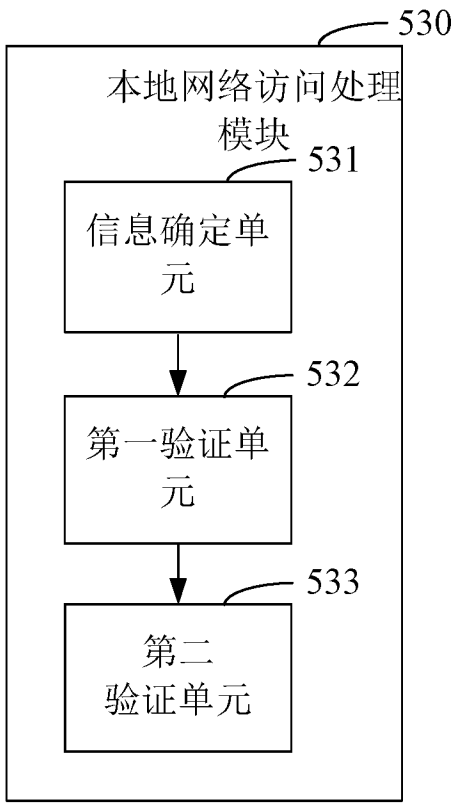
530
本地网络访问处理模块
531
信息确定单元
532
第一验证单元
533
第二验证单元

图 18

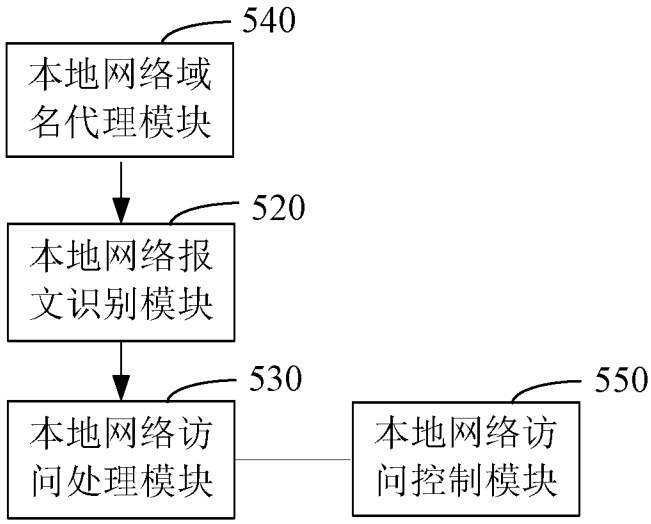
540
本地网络域名代理模块
520
本地网络报文识别模块
530
本地网络访问处理模块
550
本地网络访问控制模块

图 19

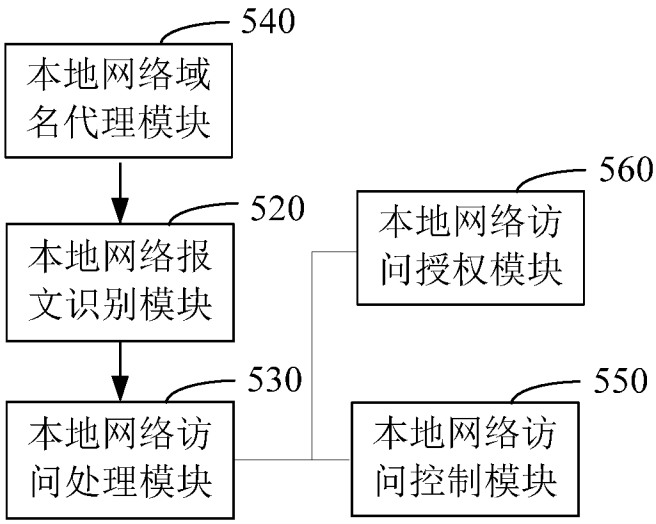
540
本地网络域名代理模块
560
本地网络访问授权模块
520
本地网络报文识别模块
530
本地网络访问处理模块
550
本地网络访问控制模块

图 20

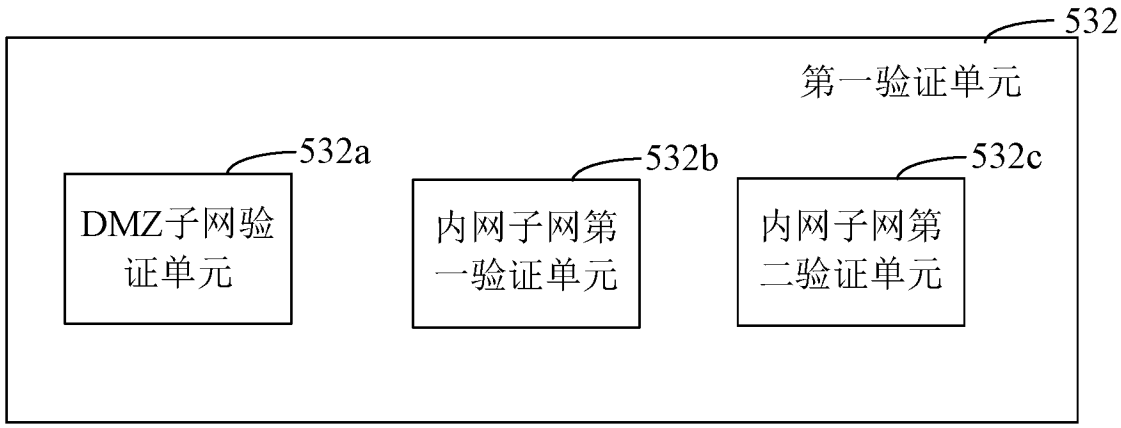
532
第一验证单元
532a
DMZ子网验证单元
532b
内网子网第一验证单元
532c
内网子网第二验证单元

图 21

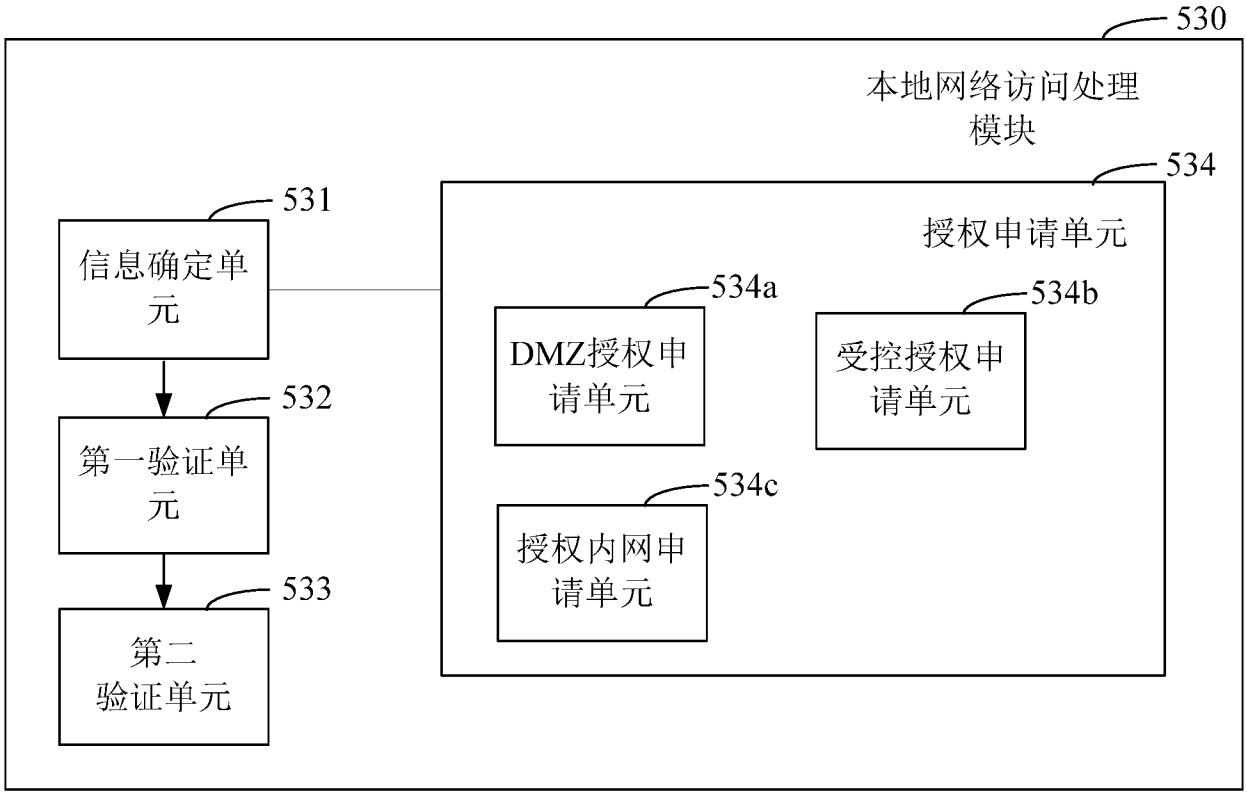
530
本地网络访问处理模块
531
信息确定单元
532
第一验证单元
533
第二验证单元
534
授权申请单元
534a
DMZ授权申请单元
534b
受控授权申请单元
534c
授权内网申请单元

图 22

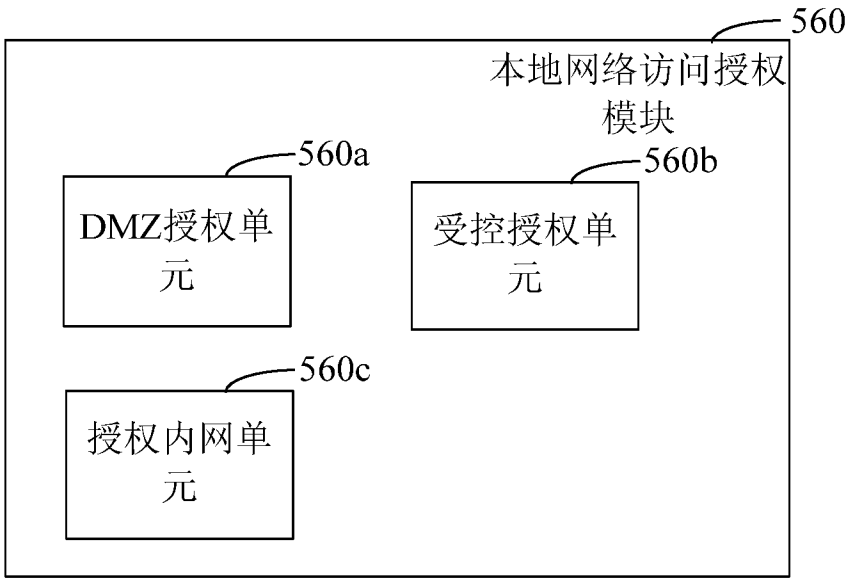
560
本地网络访问授权模块
560a
DMZ授权单元
560b
受控授权单元
560c
授权内网单元

图 23

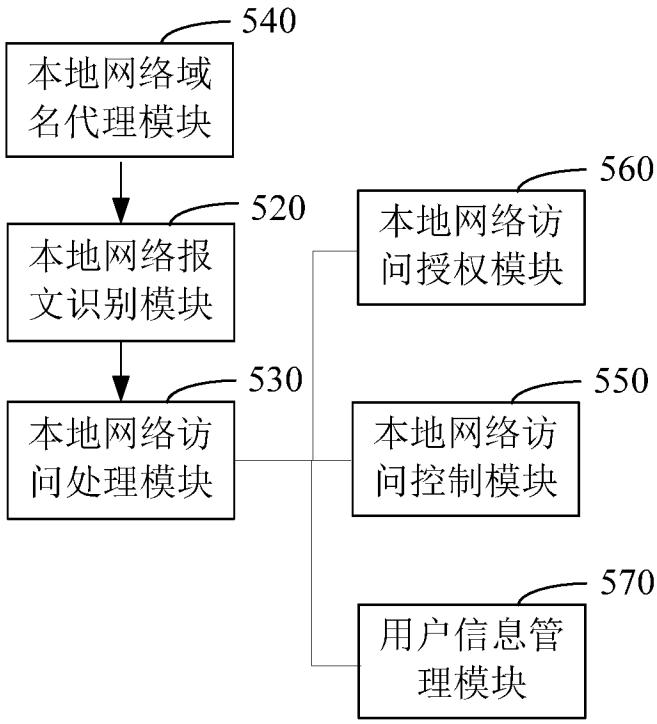
540
本地网络域名代理模块
520
本地网络报文识别模块
530
本地网络访问处理模块
560
本地网络访问授权模块
550
本地网络访问控制模块
570
用户信息管理模块

图 24


移动网基站
本地网络规则配置模块
本地网络域名代理模块
用户信息管理模块
本地网络访问处理模块
本地网络访问授权模块
本地网络访问控制模块
本地网络报文识别模块

图 25

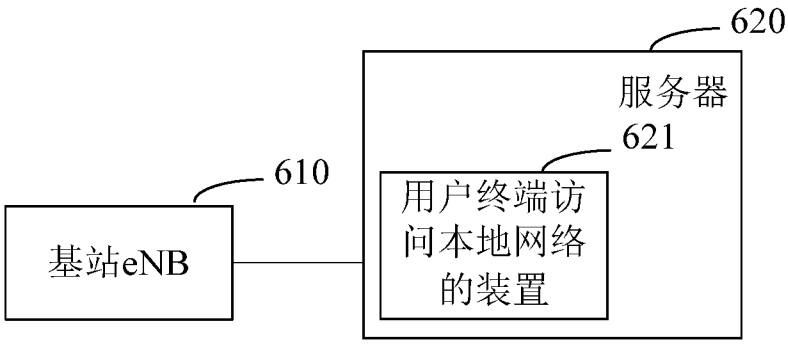
620
服务器
621
610
用户终端访问本地网络的装置
基站eNB

图 26

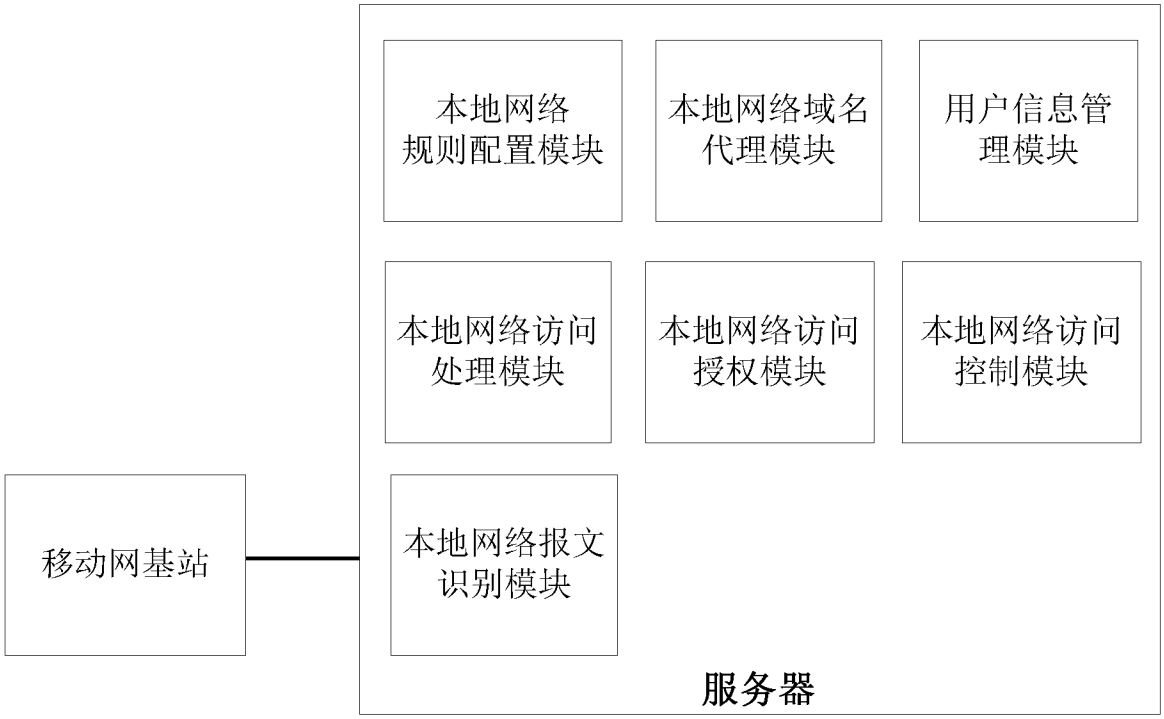
本地网络规则配置模块
本地网络域名代理模块
用户信息管理模块
本地网络访问处理模块
本地网络访问授权模块
本地网络访问控制模块
本地网络报文识别模块
移动网基站
服务器

图 27

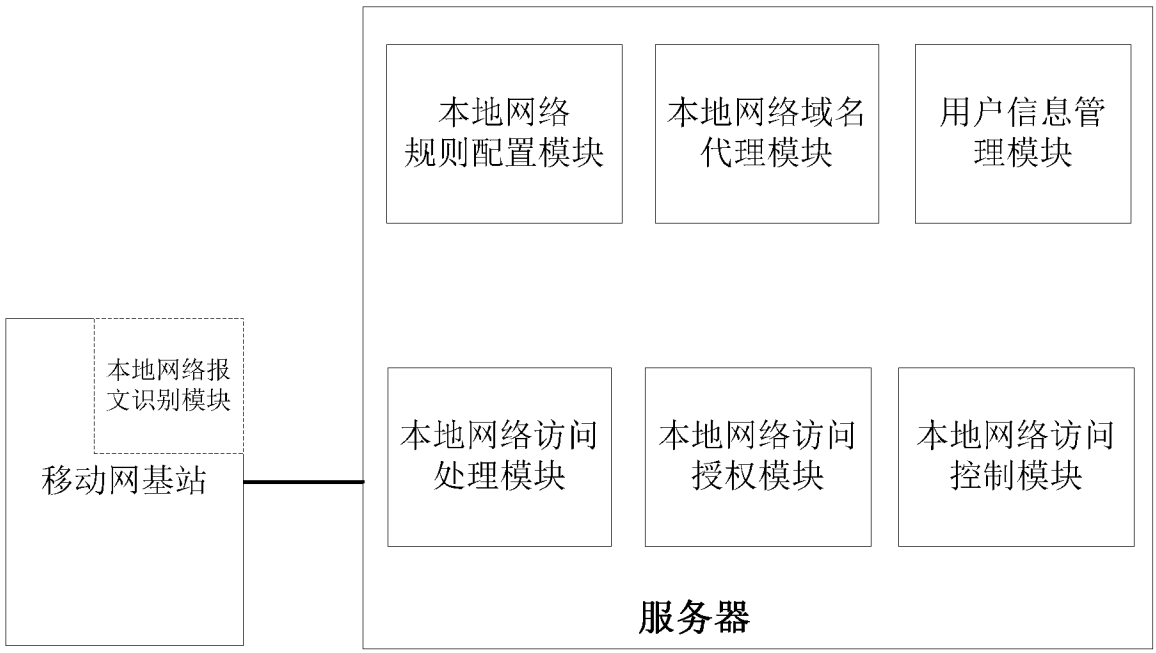
本地网络规则配置模块
本地网络域名代理模块
用户信息管理模块
本地网络报文识别模块
移动网基站
本地网络访问处理模块
本地网络访问授权模块
本地网络访问控制模块
服务器

图 28

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/100636

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L, 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)

CNPAT, CNKI, WPI, EPODOC: 无, 直接, 本地, 访问, 核心网, 不, 安全, 权限, 验证, 用户, 类, no, without, security, direct+, local, access+, core, network, epc, authority, privilege, permission, verif+, type, user

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102932953 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 13 February 2013 (13.02.2013), description, paragraphs [0003]-[0004] and [0024]-[0068], and figure 1	1-16
X	CN 101841886 A (ZTE CORP.), 22 September 2010 (22.09.2010), description, paragraphs [0007] and [0044]-[0109]	1-16
X	CN 101990313 A (ZTE CORP.), 23 March 2011 (23.03.2011), description, paragraphs [0076]-[0158], and figure 2	1-16
A	CN 102056142 A (ZTE CORP.), 11 May 2011 (11.05.2011), entire document	1-16
A	CN 102172078 A (TELEFON AB L.M. ERICSSON), 31 August 2011 (31.08.2011), entire document	1-16

☐ 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

"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	Date of mailing of the international search report
17 October 2017	01 November 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer YAN, Jie Telephone No. (86-10) 62413393

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/100636

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102932953 A	13 February 2013	CN 102932953 B	13 April 2016
CN 101841886 A	22 September 2010	WO 2011127684 A1	20 October 2011
CN 101990313 A	23 March 2011	WO 2011015092 A1	10 February 2011
		CN 101990313 B	01 January 2014
		WO 2011015124 A1	10 February 2011
CN 102056142 A	11 May 2011	WO 2011054264 A1	12 May 2011
		CN 102056142 B	02 July 2014
CN 102172078 A	31 August 2011	EP 2332370 A4	14 August 2013
		WO 2010039084 A1	08 April 2010
		EP 2332370 B1	16 November 2016
		US 2011182227 A1	28 July 2011
		EP 2332370 A1	15 June 2011
		US 8705553 B2	22 April 2014

国际检索报告

国际申请号
PCT/CN2017/100636

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L, 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））

CNPAT,CNKI,WPI,EPODOC:无，直接，本地，访问，核心网，不，安全，权限，验证，用户，类，no, without, security, direct+, local, access+, core, network, epc, authority, privilege, permission, verif+, type, user

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	CN 102932953 A (中国联合网络通信集团有限公司) 2013年 2月 13日 (2013-02-13) 说明书第[0003]-[0004]，[0024]-[0068]段、图1	1-16
X	CN 101841886 A (中兴通讯股份有限公司) 2010年 9月 22日 (2010-09-22) 说明书第[0007]，[0044]-[0109]段	1-16
X	CN 101990313 A (中兴通讯股份有限公司) 2011年 3月 23日 (2011-03-23) 说明书第[0076]-[0158]段、图2	1-16
A	CN 102056142 A (中兴通讯股份有限公司) 2011年 5月 11日 (2011-05-11) 全文	1-16
A	CN 102172078 A (爱立信电话股份有限公司) 2011年 8月 31日 (2011-08-31) 全文	1-16

☐ 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

“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	国际检索报告邮寄日期
2017年 10月 17日	2017年 11月 1日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 阎洁 电话号码 (86-10)62413393

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/100636

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）
CN	102932953	A	2013年 2月 13日	CN	102932953	B	2016年 4月 13日
CN	101841886	A	2010年 9月 22日	WO	2011127684	A1	2011年 10月 20日
CN	101990313	A	2011年 3月 23日	WO	2011015092	A1	2011年 2月 10日
				CN	101990313	B	2014年 1月 1日
				WO	2011015124	A1	2011年 2月 10日
CN	102056142	A	2011年 5月 11日	WO	2011054264	A1	2011年 5月 12日
				CN	102056142	B	2014年 7月 2日
CN	102172078	A	2011年 8月 31日	EP	2332370	A4	2013年 8月 14日
				WO	2010039084	A1	2010年 4月 8日
				EP	2332370	B1	2016年 11月 16日
				US	2011182227	A1	2011年 7月 28日
				EP	2332370	A1	2011年 6月 15日
				US	8705553	B2	2014年 4月 22日