



- (51) **International Patent Classification:**
H04W 8/26 (2009.01) *H04W 88/02* (2009.01)
- (21) **International Application Number:**
PCT/US2012/033840
- (22) **International Filing Date:**
16 April 2012 (16.04.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/475,647 14 April 2011 (14.04.2011) US
CN2011/073896 10 May 2011 (10.05.2011) CN
61/535,343 15 September 2011 (15.09.2011) US
- (71) **Applicant (for all designated States except US):** **ZTE (USA) INC.** [US/US]; 55 Madison Avenue, Suite 160, Morristown, NJ 07960 (US).
- (72) **Inventor; and**
- (75) **Inventor/Applicant (for US only):** **BHALLA, Rajesh** [IN/US]; 909 Aries Drive, Gahanna, OH 43230 (US).
- (74) **Agent:** **SATHE, Vinay**; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (US).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title:** METHODS AND APPARATUS FOR DETERMINING ADDRESS OF A MACHINE TYPE COMMUNICATION DEVICE IN A WIRELESS NETWORK

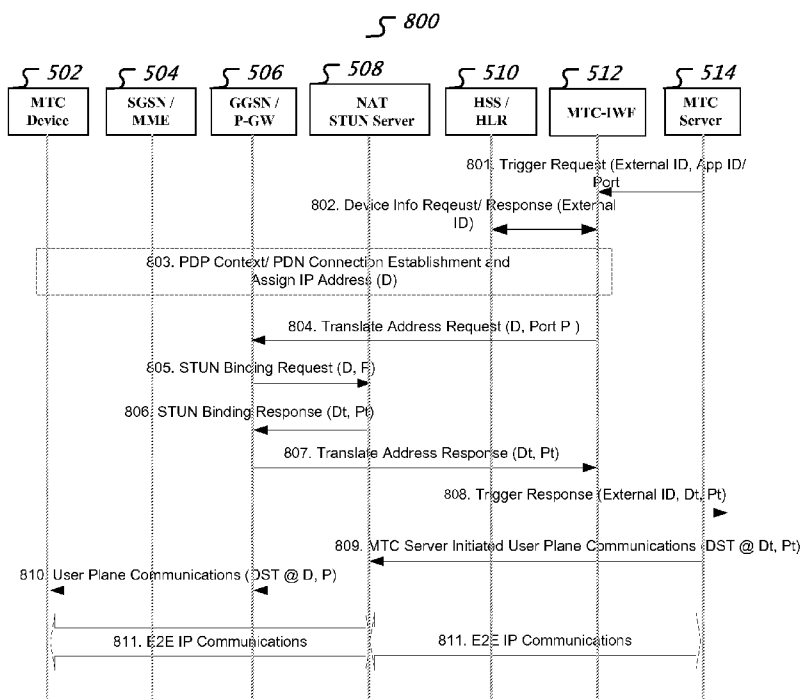


FIG. 8

(57) **Abstract:** Techniques, systems and apparatus are described for implementing a framework for an address determination technique for IPv4 addressing of MTC devices behind NATs in wireless networks. In one aspect, a method includes determining address for machine type communications (MTC) devices behind Network Address Translators (NATs) in a wireless communication network. The determining includes assigning a private address to an MTC device attached to the wireless communication network, and determining mapped public transport address.

**Declarations under Rule 4.17:**

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

METHODS AND APPARATUS FOR DETERMINING ADDRESS OF A MACHINE TYPE COMMUNICATION DEVICE IN A WIRELESS NETWORK

Cross-Reference to Related Applications

[0001] This patent document claims the benefit of priority of United States Provisional Application No. 61/475,647, filed on April 14, 2011, United States Provisional Patent Application No. 61/535,343, filed on September 15, 2011, and International Patent Application No. PCT/CN2011/073896, filed on May 10, 2011. The entirety of these patent applications are incorporated by reference in the present patent document.

Background

[0002] This patent document relates to communications, including machine type communications (MTC) and machine to machine (M2M) communications.

[0003] In many applications, wireless devices operating in a wireless network communicate with other devices and servers that are not operating in the wireless network but can be communicatively reachable. Various standards are available to provide such connectivity to wireless devices. For example, the Internet Protocol (IP) is one such framework by which a wireless device can be communicatively coupled with other devices, based on an IP address assigned to the wireless devices.

[0004] Certain operational cases, such as in systems that include machine type communications (MTC) and machine to machine (M2M) communications wireless devices, may lack the framework for IP connectivity.

Summary

[0005] Techniques, systems and apparatus are described for implementing a framework for address determination techniques for IP addressing of MTC devices. In some implementations, IPv4 addresses may be used such that an MTC device may operate in a different IPv4 address space behind a NAT than the IPv4 address space in which a server that may want to communicate with the MTC device.

[0006] In one aspect, a disclosed method, implementable at a gateway device in a wireless communications network, includes receiving a request to perform translation of a

first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system, obtaining a second IP address for the MTC device, the second IP address being in a second IP address space different from the first IP address space, transmitting a response to the request by including the second IP address and facilitating user data plane communication to and from the MTC device and another communication entity in the second IP address space.

[0007] In another aspect, a disclosed method, implementable at a network-side in a wireless communication network, comprises receiving a trigger request including an external identification (ID) of a machine type communication (MTC) device, transmitting a device information request including the external ID, receiving, in response to the device information request, a first internet protocol (IP) address for the MTC device, the first IP address being in a private address space of the wireless network, and obtaining a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received.

[0008] These, and other features, are described in greater detail below.

Brief Description of Drawings

[0009] FIG. 1 is a block diagram representation of a wireless communications network.

[0010] FIG. 2 is a block diagram of a wireless device operable in a wireless communications network.

[0011] FIG. 3 is a block diagram representation of a Network Address Translation system.

[0012] FIG. 4 depicts signals exchanged for facilitating private IPv4 address assignment.

[0013] FIG. 5 is a signal exchange diagram for a session establishment procedure.

[0014] FIG. 6 is a signal exchange diagram showing a UE initiated communications

[0015] FIG. 7 is a block diagram representation of messages exchanged during an IPv4 address translation for device triggering.

[0016] FIG. 8 depicts a signal exchange diagram of messages exchanged in an MTC server triggered communication.

[0017] FIG. 9 shows messages exchanged during the operation of maintaining STUN bindings.

[0018] FIG. 10 shows messages exchanged during the operation of releasing NAT bindings.

[0019] FIG. 11 is a block diagram representation of transport address translation for MTC device initiated communication (option 1).

[0020] FIG. 12 is a block diagram representation of transport address translation for MTC device initiated communication (option 2)

[0021] FIG. 13 shows example address mapping and data transport with a STUN server.

[0022] FIG. 14 shows example address mapping and data transport with a TURN relay.

[0023] FIG. 15 is a flow chart representation of a process implementable at a network-side in a wireless communication network.

[0024] FIG. 16 is a block diagram representation of an apparatus for facilitating wireless communications.

[0025] FIG. 17 is a flow chart representation of a process implementable at a gateway device in a wireless communication system.

[0026] FIG. 18 is a block diagram representation of a portion of a gateway device operable in a wireless communications network.

Detailed Description

[0027] This patent document discloses techniques, devices and systems that can be used, in some implementations, to determine address of a machine type communication (MTC) device in a wireless communications network. In some configurations, the disclosed techniques may be used to enhance the functionality of an existing inter-working function that is implemented at a hardware platform on the network-side in a wireless communications network. In some configurations, the disclosed techniques may be used to enhance the functionality of a gateway device (e.g., a packet gateway device P-GW) in a wireless communications network.

[0028] FIG. 1 shows an example of a wireless communication system. A wireless communication system can include one or more base stations (BSs) 105a, 105b, one or more wireless devices 110 and an access network 125. Base station 105a, 105b can provide wireless service to wireless devices 110 in one or more wireless sectors. In some implementations, a base station (e.g., 105a or 105b) includes directional antennas to produce two or more directional beams to provide wireless coverage in different sectors.

[0029] The access network 125 can communicate with one or more base stations 105a, 105b. In some implementations, the access network 125 includes one or more base stations 105a, 105b. In some implementations, the access network 125 is in communication with a core network (not shown in FIG. 1) that provides connectivity with other wireless communication systems and wired communication systems. The core network may include one or more service subscription databases to store information related to the subscribed wireless devices 110. A first base station 105a can provide wireless service based on a first radio access technology, whereas a second base station 105a can provide wireless service based on a second radio access technology. The base stations 105a may be co-located or may be separately installed in the field according to the deployment scenario. The access network 125 can support multiple different radio access technologies.

[0030] Various examples of wireless communication systems and access networks that can implement the present techniques and systems include, among others, wireless communication systems based Code Division Multiple Access (CDMA) such as CDMA2000 1x, High Rate Packet Data (HRPD), evolved HRPD (eHRPD), Universal Mobile Telecommunications System (UMTS), Universal Terrestrial Radio Access Network (UTRAN), Evolved UTRAN (E-UTRAN), Long-Term Evolution (LTE). In some implementations, a wireless communication system can include multiple networks using different wireless technologies. A dual-mode or multi-mode wireless device includes two or more wireless technologies that could be used to connect to different wireless networks. In some implementations, a wireless device can support Simultaneous Voice-Data Operation (SV-DO). For CDMA200 systems, the core network 125 can include, among others, mobile switching center (MSC), Packet Data Serving Node (PDSN) and others.

[0031] FIG. 2 is a block diagram representation of a portion of a radio station 205. A radio station 205 such as a base station or a wireless device can include processor electronics 210 such as a microprocessor that implements one or more of the wireless communications techniques presented in this document. The radio station 205 can include transceiver

electronics 215 to send and/or receive wireless signals over one or more communication interfaces such as antenna 220. The radio station 205 can include other communication interfaces for transmitting and receiving data. Radio station 205 can include one or more memories configured to store information such as data and/or instructions. In some implementations, the processor electronics 210 can include at least a portion of the transceiver electronics 215.

[0032] In some implementations, radio stations 205 can communicate with each other based on a CDMA air interface. In some implementations, radio stations 205 can communicate with each other based on an orthogonal frequency-division multiplexing (OFDM) air interface which can include Orthogonal Frequency-Division Multiple Access (OFDMA) air interface. In some implementations, radio stations 205 can communicate using one or more wireless technologies such as CDMA such as CDMA2000 1x, HRPD, WiMAX, LTE, and Universal Mobile Telecommunications System (UMTS).

[0033] Techniques, devices and system described in this document can be used to, among other application, provide an Unilateral Self Address Fixing (UNSAF) framework for IPv4 addressing of MTC devices behind NATs in wireless networks. In addition, the techniques, devices and systems described in this document can be used to, among other application, enable an MTC device and/or an MTC server to determine public routable address of an MTC device deployed behind one or more Network Address Translators (NATs).

[0034] In the description below, section headings are used only to facilitate the understanding of the disclosed subject matter and do not limit the scope of the claimed subject matter in any way.

UNSAF framework for IPv4 addressing of MTC devices behind NATs in Wireless Networks

[0035] Communicating endpoints that are separated by one or more NATs do not typically know how to refer to themselves using addresses that are valid in the addressing realms of their peers. For many purposes, the endpoints need to know the addresses (and/or ports) by which they are known to their peers.

[0036] This problem is sometimes known as *UNilateral Self-Address Fixing (UNSAF)*. As stated in RFC3424, UNSAF is the process whereby an entity behind the NAT attempts to determine or fix the address (and port) by which it is known in the ‘public’ domain (outside the NAT). This ‘public’ address can then be used in protocol exchanges for addressing the entity behind the NAT, or be advertised as a ‘public’ address from which the entity behind the NAT can receive communications.

[0037] For UNSAF, two cases need to be considered. In the first case, when the entity behind the NAT initiates communications, and in the second case, when an entity on the outside of the NAT needs to initiate communications.

2. UNSAF for Wireless Networks

[0038] Due to the limitation on the availability of public IPv4 addresses, MTC device(s) may be deployed behind NAT(s) and assigned private non-routable IPv4 address (and thus not reachable by the MTC Server(s)). Depending on the nature of the MTC applications, there could be a need either for the MTC device or for the MTC server to be the initiator of the communications. For some applications an MTC device behind the NAT needs to know its publicly routable transport address before initiating communications with a peer-entity. Initiation of communications from outside the wireless network (such as from the MTC server for device triggering) will require the outside entity to know the publicly routable transport address of the MTC device.

[0039] As used in this document, a transport address is the combination of an IP Address and Port Number (such as a UDP or TCP port number and therefore address resolution may imply resolving both the IP address and the associated port number.

[0040] With such requirements for MTC communications, address determination techniques for IPv4 addressing for MTC devices behind NATs for wireless networks are useful. Such address determination technique should be able to support the two scenarios below:

1. MTC device behind the NAT, where the MTC device or the client initiates communications, and
2. MTC server outside of the NAT and the server needs to initiate communications (e.g., for device triggering).

[0041] This document describes an exemplary framework for address determination techniques for IPv4 addressing of MTC devices behind NATs in 3GPP networks. Depending on the nature of the NATs, Endpoint-Independent-Mapping (EIM) and Endpoint-Dependent-Mapping (non-EIM) NAT, two solutions are disclosed. For NATs with EIM behaviour, address determination technique based on Session Traversal Utilities for NAT (STUN) protocol (IETF RFC5389) is proposed. For NATs with non-EIM behaviour, address determination technique based on Traversal Using Relays around NAT (TURN) protocol (IETF RFC5766) may be utilized.

Suitable Architecture:

[0042] Example reference architecture for NAT Traversal using Non-Managed NAT for MTC services for 3GPP networks is illustrated in FIG. 3. Similar reference model is applicable for other wireless networks by replacing the GGSN/P-GW entity with an appropriate network entity for the other wireless network. For example, for 3GPP2 networks the GGSN/P-GW entity is substituted with the PDSN in the illustrated reference model.

[0043] In the illustrated address translation system 300, IP address translations and address bindings in the NAT 310 are not controlled by the wireless network. Such IP address translations and address bindings are created by the use of session specific signaling when the MTC Server 314 wants to initiate communications with the MTC device (located at UE 302) used for Machine type communications. The Machine Type Communication InterWorking Function (MTC-IWF) 308 may be coupled between the MTC server 314 and the GGSN/P-GW 304.

[0044] In this example reference model illustration for 3GPP networks, the NAT device 306 is behind the GGSN/P-GW 304 in the operator domain and only user plane traffic traverses the NAT. GGSN stands for Gateway General Packet Radio Service Support Node. The NAT device 306 could be a standalone functional entity or integrated with the GGSN/P-GW 304. Address determination function in the NAT conforms to the protocol defined in RFC5389 (STUN) or RFC5766 (TURN) depending on the type of the NAT. For EIM type of NAT, user plane traffic 310 flows directly between the GGSN/P-GW 304 and the NAT. For non-EIM type of NAT, the user plane traffic flows between the GGSN/P-GW 304 and the TURN relay function 312. RFC5128 describes the EIM and non-EIM type NATs. The STUN function in the GGSN/P-GW 304 may be limited to the STUN/TURN client functions.

3. Address Determination Techniques for IPv4 Addressing of MTC Devices Behind NATs in Wireless Networks

3.1 Framework

[0045] The address determination technique described in this paper comprises of two steps:

- MTC device attaches to the wireless network and a private IPv4 address is assigned to the device
- Determination of the mapped public transport address

[0046] FIG. 4 is an exemplary illustration of an architecture 400 of private IPv4 address assignment and address registration procedures for 3GPP networks. An MTC device 412 behind a NAT 416 attaches (message 401) to the 3GPP network (domain) and requests establishment of a packet data protocol (PDP) context/ packet data network (PDN) connection and IP address assignment. For 3GPP2 networks, for illustrative purposes, the MTC devices 412 behind the NAT 416 attaches to the 3GPP2 network and requests establishment of the link layer (PPP) connection with the PDSN and the assignment of the IP address. Similar steps in other wireless networks are also possible.

[0047] The MTC device 412 is authenticated and authorized (message 402) with the AAA 426. A PDP context/PDN connection is established and a private-IPv4 Address is assigned (message 406) to the MTC device. Depending on the operator policy, the IP address may be assigned by the AAA 426 or by the GGSN/P-GW 414. Details of the AAA authentication and authorization procedures and IP address assignment procedures are as per the call setup procedures for the appropriate wireless technology. In this example illustration, the GGSN/P-GW 414 registers MTC device 412 specific information such as the GGSN/P-GW address, MTC device ID, assigned private IPv4 address information etc. with the HSS/AAA 418, 426. Alternatively the GGSN/P-GW may register all or part of such MTC device specific information with the MTC Gateway/Proxy (such alternate procedure is not shown in FIG. 4).

[0048] As regards the determination of the mapped public transport address, two scenarios need to be considered.

1. MTC device behind the NAT (client) initiates communications, and
2. MTC server outside of the NAT (server) needs to initiate communications (e.g., for device triggering).

[0049] Scenario-2 is considered first, and is illustrated in FIG. 7. When the MTC server 422 wants to initiate communications with an MTC device 412, if it already does not have the (public) transport address information for the MTC device 412, the MTC server 422 queries the transport address of the MTC device by sending a Query message 701 to the MTC Gateway/Proxy 420. The Query message 701 includes the MTC device ID. MTC Gateway/Proxy 420 queries the HSS/HLR 418 for the serving GGSN/P-GW 414 information and the private IPv4 address assigned to the MTC device, or obtains such information from its local cache if so available. On the receipt of the private IPv4 address assigned to the MTC device, the MTC Gateway/Proxy initiates Translate Address Request/Reply procedure (704, 705) by passing the assigned private IPv4 Address and pseudo Port information to the GGSN/P-GW 414, which in turn performs such procedure with the Address Determination Server 424. The 'port' chosen for the Translate Address Request 704 procedure could be a dynamic/private (ephemeral port) in the range of 48k to 64k or some other port. Alternatively, instead of the MTC Gateway/Proxy 420 choosing the pseudo Port, such port could be chosen by the GGSN/P-GW 414. The Address Determination Server 424 performs address translation and returns the mapped public transport address (public IP Address+ Port) information 705 to the GGSN/P-GW 414. Such information, in turn, is passed to the MTC Gateway/Proxy and the MTC server (706). MTC server 420 can now use such public transport address to initiate communications with the MTC device 412. The MTC device 412 (which may be assigned IP address in the private space of the wireless network 410) may be online or offline to receive such communications from the MTC server 420.

[0050] As regards scenario-1(MTC device behind NAT initiates communications), two procedures are illustrated in FIG. 11 and FIG. 12 respectively. For some applications an MTC device behind the NAT needs to know its routable transport address before initiating communications with a peer-entity. The MTC device 412 initiates Public Transport Address Request/Reply (1101, 1104) procedure by sending Device ID and the assigned private IPv4 address information to an entity (e.g., GGSN/P-GW 414, MTC Gateway/Proxy 420) in the

3GPP network. Such Public Transport Address determination procedure may be performed with the help of entities such as the GGSN/P-GW (Option 1) or the MTC Gateway/Proxy (Option 2).

[0051] For Option 1, the Public Transport Address Request/Reply procedure (1101, 1104) is performed with the help of entities such as the GGSN/PGW 414. When the MTC device 412 wants to initiate communications with a peer entity, and if it does not already have its (public) transport address information, depending on the application at the MTC device 412, the MTC device 412 selects the 'port' from which it wants to initiate communications with the peer entity. It then initiates Public Transport Address Request/Reply procedure (1101, 1104) by sending the Request message 1101 directed to the GGSN/P-GW 414. The Request message 1101 includes information such as the Device ID, the private IPv4 Address (assigned to the MTC device) and the 'port' information (chosen by the MTC device). Alternatively, if the IPv4 Address is not included in the Request message 1101, such information can be obtained by the GGSN/P-GW 414 by querying the HSS/HLR 418 based in the Device ID, or obtained from the local cache at the GGSN/P-GW 414 if so available. The GGSN/P-GW 414 then initiates Translate Address Request/Reply procedure (1102, 1103) by passing the assigned private transport address (IPv4 Address and the Port) information to the Address Determination Server 424. The Address Determination Server 424 performs address translation and returns (1103) the mapped public transport address (IP Address+ Port) information to the GGSN/P-GW 414, which in turn, is returned to the MTC device via Public Transport Address Reply procedure. MTC device can now use such public transport address information to initiate communications with the peer entity.

[0052] For Option 2, the Public Transport Address Request/Reply procedure (1201, 1206) is performed with the help of the MTC Gateway/Proxy 420. When the MTC device 412 wants to initiate communications with a peer entity, and if it does not already have its (public) transport address information, depending on the application at the MTC device 412, the MTC device 412 selects a 'port' from which it wants to initiate communications with the peer entity. It then initiates Public Transport Address Request/Reply procedure (1201, 1206) by sending the Request message directed to the MTC Gateway/Proxy. The Request message 1201 includes information such as the Device ID, the private IPv4 Address (assigned to the MTC device) and the 'port' information (chosen by the MTC device 412). It is assumed that the MTC Gateway/Proxy 420 has information about the serving GGSN/P-GW 414 and possibly the private IPv4 addressed to the MTC device 412. It is possible that the Request

message 1201 may not include the private IPv4 address assigned to the MTC device 412. Alternatively, such information (serving GGSN/P-GW and the IPv4 Address if not included in the Request message), can be obtained by the MTC Gateway/Proxy 420 by querying (1202) the HSS/HLR 418 based in the Device ID (and receiving a response 1203). The MTC Gateway/Proxy 420 then initiates Translate Address Request/Reply procedure (1204, 1205) by passing the assigned private transport address (IPv4 Address and the Port) information to the GGSN/P-GW 414 which in turn performs such procedure with the Address Determination Server 424. The Address Determination Server 424 performs address translation and returns the mapped public transport address (IP Address+ Port) information to the GGSN/P-GW 414 (1205). Such information, in turn, is passed to MTC Gateway/Proxy and returned to the MTC device via Public Transport Address Reply procedure (1206). MTC device can now use such public transport address information to initiate communications with the peer entity.

4. Exemplary Implementations in 3GPP Networks

[0053] In the description below, the MTC device 502, GGSN 506, NAT server 508, HSS/HLR 510, and MTC server 514 may be substantially similar to previously discussed MTC device 412, GGSN 414, NAT server 424, HSS/HLR 418, and MTC server 422 respectively. Furthermore, additional network elements – mobility management entity (504), MTC-IWF 512 are described below.

[0054] In general, when supporting MTC for UEs residing behind a NAT, there are no additional requirements on the UEs. Similarly, when supporting MTC for UEs residing behind a NAT, there are no additional requirements on the MTC Server.

[0055] When supporting MTC for UEs residing behind a NAT, the MTC InterWorking Function (MTC-IWF) may include one or more of the following functionalities:

[0056] The MTC-IWF may be able to recognize that the UE used for MTC is behind a NAT device.

[0057] The ability to recognize that the UE is being served by a GGSN/P-GW that is located behind a NAT based on the IPv4 address assigned to the UE used for MTC.

[0058] The ability to initiate procedures to obtain the public transport address (IP address + port) for the UE used for MTC by querying the GGSN/P-GW.

[0059] The ability to communicate the public transport address for the UE for MTC to the MTC Server.

[0060] When supporting MTC for UEs residing behind a NAT, the GGSN/P-GW may invoke STUN/TURN protocol mechanisms with the NATs for private to public transport address translations. The GGSN/P-GW may perform the following functions:

[0061] Support STUN/TURN functionality as specified in RFC5239 and RC5766.

[0062] Support STUN/TURN server discovery. In some implementations, a configuration mechanism can be used to provision STUN/TURN server addresses in the GGSN/P-GW.

[0063] When requested by the MTC-IWF, initiate procedures to obtain the public transport address for the UE used for MTC by performing STUN/TURN address determination procedure with the NAT.

[0064] Communicate the translated transport address assigned to the UE for MTC to the MTC-IWF.

[0065] Maintain NAT bindings by the use of STUN keep-alive mechanisms.

[0066] The STUN server and associated signaling requirements are documented in RFC5389. When supporting MTC for UEs that are residing behind a NAT, no additional requirements are placed on the STUN server. In some implementations, no STUN server may be deployed in the network. In some implementations, a STUN server may be deployed, thereby facilitating the discovery of the APN-facing transport address at the NAT for the UEs for the majority of NAT types. In one aspect, this may minimize the need for TURN resources by allowing UEs to directly communicate user plane traffic through the NAT.

[0067] The TURN relay and associated signaling requirements are documented in RFC 5766. When supporting MTC for the UEs that are residing behind a NAT, no additional requirements are placed on TURN relay server. In some implementations, no TURN may be deployed in the network. In some implementations, TURN may be deployed to facilitate the exchange of user plane traffic in the presence of all types of NATs.

[0068] The MTCyy reference point is between the GGSN/P-GW and the STUN/TURN Address Determination Function. This interface conveys the information necessary for the NAT device to activate the procedures in the GGSN/P-GW and in the STUN/TURN Address Determination Server.

5. Procedures for performing address determination

[0069] The procedures described in this clause are specific to the use of non-Managed NATs, and are applied in addition to other procedures for the support of Machine Type Communications.

5.1 NAT detection in MTC-IWF

[0070] When the PLMN supports non-managed NATs, based on the IPv4 address assigned to the UE used for MTC or based on local configurations, the MTC-IWF shall detect if a NAT is deployed between the GGSN/P-GW and the APN, and decide if address translation functions shall be invoked with the GGSN/P-GW.

5.2 Session establishment procedure

[0071] With reference to FIG. 5, the session establishment procedure 500 is applied when the UE used for MTC registers with the network and establishes PDP context/ PDN connection (501). Such procedures may be invoked by the UE initiating the procedures autonomously or as a result of being Paged by the network.

[0072] The MTC device performs Attach procedure with the network, either autonomously or as a result of being Paged by the network. As part of the Attach procedure the MTC device is assigned an IPv4 address, referred to here as 'D' (message 503). As the MTC device is deployed behind a NAT, the assigned IPv4 address is in the private address domain of the GGSN/P-GW. The Create Session Response message (not shown) is used to convey the address 'D' from the GGSN/P-GW to SGSN/MME. An MTC-IWF is also assigned for the MTC device.

[0073] As part of the previous step, or at the end of the Attach procedure, the SGSN/MME notifies the HSS/HLR of the address 'D' assigned to the MTC device. If an interface is defined between the GGSN/P-GW and the MTC-IWF, a Status Update Request/Response message 505 can be used to by the GGSN/P-GW to notify the MTC-IWF of the address 'D' assigned to the MTC device.

5.3 UE initiated communications

[0074] With reference to FIG. 6, the procedure 600 is applied when the UE used for MTC has registered with the network and has a PDN context/ PDP connection established and an IPv4 address assigned, as described above. Since the UE used for MTC is behind a NAT, a private IPv4 address 'D' is assigned to the UE.

[0075] The MTC device 502 sends a user plane packet addressed to the peer-entity over the established PDN context/ PDP connection (601). The source IP address of the packet is set to the private IPv4 address 'D' assigned to the MTC device.

[0076] On receiving the user plane packet for which there is no binding, the NAT device recognizes it as packet flow for a new session. The NAT device performs address and/or port translation on the private address/port (D, P) and replaces the source transport address of the user plane packet with the translated transport address (Dt, Pt), shown in message 603.

[0077] End-to-end IP communication 605 between the MTC device and the peer entity continues. The peer entity uses transport address (Dt, Pt) as the destination address in the user plane packets sent to the MTC device. NOTE: The NAT bindings are kept alive by virtue of the flow of user plane traffic. In case the NAT reboots and/or the old bindings are lost, new bindings are created on the receipt of user plane packet from the UE.

5.4 MTC Server triggered communications

[0078] The procedure 800 depicted in FIG. 8 is applied when the MTC Server wants to initiate communications with the UE used for MTC. The MTC Server determines the MTC-IWF that serves the UE used for MTC by performing DNS query with UE's External ID. As the MTC-IWF assigned for a particular UE used for MTC will change rarely, the MTC Server will need to perform DNS query to resolve the assigned MTC-IWF address rarely. This address is then used to request the MTC-IWF for the routable IP address to use for initiating user plane communications with the UE. DNS update and DNS query procedures for resolving MTC-IWF address are not shown in the following illustration.

[0079] In the following illustration the STUN Server element represents both a STUN server and TURN relay as a single logical element. It would be equally valid if these functions were represented as separate logical elements. The procedures are unaffected by the

grouping. Further, this call flow represents a simplified view to illustrate the NAT traversal procedures for STUN server only.

[0080] The MTC Server wants to initiate communications with an MTC device and if it does not have the IP address information for the MTC device or identifies a need to recover IP connectivity e.g., the MTC device is not responding anymore, the MTC Server queries the MTC-IWF for the IP address by sending a Trigger Request message 801. The Trigger Request message 801 includes the MTC device External Identifier, and Application Identifier for the application that the MTC Server wants to initiate with the MTC device.

[0081] The Application Identifier information can be in the form of an "Application ID" that is commonly understood by the service provider and the PLMN entities. Else, it could be in the form of a "port number" assigned to the application by the International Authority for Name Assignment (IANA) or some such other accredited organization.

[0082] In some implementations, the MTC server may determine the MTC-IWF that serves the UE used for MTC by performing a DNS query using the UE's external ID.

[0083] The MTC-IWF authorizes the trigger request, communicates (message 802) with the HSS/HLR to obtain the IP address assigned to the MTC device, if such information is not available in the local cache. If there is an active PDP context/ PDN connection for the MTC device, the HSS/HLR returns the private IPv4 address and the GGSN/P-GW assigned to the MTC device, and the procedures continue below. Else, if the PDP context/PDN connection is not established (as in 803) or the IP connectivity needs to be recovered, the HSS/HLR returns the internal Device ID (IMSI) and any additional information needed for triggering the MTC device as in Step 804.

[0084] The MTC-IWF selects the device trigger delivery mechanism and forwards trigger request to the next node involved in the delivery of the trigger to the MTC device. Resulting from triggering the MTC device, a PDP context/ PDN connection is established (803) and an IPv4 address assigned to the MTC device as per procedures in this document. At this stage, the IP address 'D' assigned to the MTC device is available at the HSS/HLR and/or at the MTC-IWF, which along with the assigned GGSN/P-GW information is made available to the MTC-IWF. As the MTC device is located behind the NAT, the MTC-IWF initiates address translation procedures by sending Translate Address Request message 804 that includes the (private) IPv4 address 'D' and Application ID/Port 'P' information to the assigned GGSN/P-GW.

[0085] The GGSN/P-GW implements STUN/TURN client function as specified in RFC5389 and RFC5766 respectively. The GGSN/P-GW sends STUN Binding Request message 805 to the STUN/TURN server to obtain the public transport address for the MTC device.

[0086] The STUN/TURN server performs address translation and returns the mapped public transport address information to the GGSN/P-GW in STUN Binding Response message 8-6. The STUN/TURN server maintains binding for the translated address for the duration of the binding 'lifetime' as per procedures in RFC5389.

[0087] The GGSN/P-GW intercepts STUN Binding Response message, and returns the translated transport address information to the MTC-IWF via Translate Address Response message 807.

[0088] The MTC-IWF returns the public transport address assigned to the MTC device to the MTC Server via Trigger Response message 808.

[0089] At this stage the MTC Server is ready to initiate communications with the MTC device. The MTC Server sends user plane packets 809 addressed to the MTC device with the target address set to the public transport address (Dt, Pt) assigned to the MTC device.

[0090] On receiving the user plane packets, the NAT recognizes the binding for the public transport address (Dt, Pt) and replaces the destination transport address information with the private address (D, P) assigned to the MTC device 810.

[0091] End-to-end IP communications 811 between the MTC Server and the MTC device continues. The MTC device uses the private address /port information (D, P) as the source address for the user plane packets, which is mapped to the public transport address (Dt, Pt) by the NAT device.

5.5 Maintaining STUN bindings

[0092] With reference to FIG. 9, the procedure 900 is applied for maintaining STUN bindings at the NAT device. NAT bindings are kept alive by virtue of the flow of user plane traffic. Additionally, the STUN client function at the GGSN/P-GW keeps the bindings alive by the use of STUN keep-alive signaling.

[0093] NAT bindings are kept alive by virtue of the flow of user plane traffic. Additionally, the STUN client function in the GGSN/P-GW keeps the bindings alive by sending periodic keep-alive STUN Binding Request message 901 to the STUN server.

[0094] The STUN server updates the lifetime of the binding and returns STUN Binding Response message 902 to the GGSN/P-GW. Binding Response message includes the mapped transport address (Dt, Pt) also. Inclusion of such information allows the GGSN/P-GW to determine if the NAT has rebooted and assigned new bindings (Dt', Pt') for the MTC device.

[0095] If NAT assigns new bindings, the GGSN/P-GW forwards such information to the MTC-IWF via Translate Address Response (Dt', Pt') message 903.

[0096] MTC-IWF forwards the new transport address information to the MTC Server. The MTC Server uses the new transport address (Dt', Pt') for further communications with the MTC device 904.

5.6 Releasing NAT bindings

[0097] With reference to FIG. 10, the procedure 1000 is applied for releasing STUN bindings at the NAT device. When the MTC-IWF learns about the release of the private IPv4 address 'D' assigned to the UE used for MTC, MTC-IWF initiates NAT binding release procedure by sending Translate Address Request (Release) message 1001 to the GGSN/P-GW. The MTC-IWF learns about the release of the IP address when the PDP context/ PDN connection for the UE used for MTC is released or by some other means.

[0098] The MTC-IWF learns about the release of the IP address 'D' assigned to the MTC device. MTC-IWF initiates NAT binding release procedure by sending Translate Address Request (Release) message 1101 to the GGSN/P-GW.

[0099] The GGSN/P-GW sends STUN Binding Request (D, P) message to the STUN server, with binding lifetime set to '0' 1002.

[00100] The STUN server releases the binding for the MTC device and responds with STUN Binding Response message with lifetime set to '0' 1003.

[00101] The GGSN/P-GW confirms the release of the NAT binding by returning Translate Address Response (Release Confirm) message to the MTC-IWF 1004.

[00102] FIG. 13 shows an exemplary process 1300 for Address Mapping and Data Transport with STUN Server 1302. Some NAT equipment behaves as ‘Endpoint-Independent mapping and filtering’ (EIM). They use the same public port mapping for all packets sent from the same (source) IP address and port of the MTC device (behind the NAT) irrespective of the destination IP transport address of the MTC server. Additionally, such NATs do not filter incoming packets with source transport address different from that of the destination in the previous outgoing packets. In this case, an Address Server (STUN Server 1302) can be deployed for address determination procedures and to obtain the mapped public transport address for the MTC device.

[00103] When the MTC server 422 wants to initiate communications with an MTC device 414, if it already does not have the (public) transport address information for the MTC device, the MTC server queries the transport address of the MTC device by sending a Query message 1310 to the MTC Gateway/Proxy 420. The Query message 1310 includes the MTC Device ID. MTC Gateway/Proxy queries the HSS/HLR for the serving GGSN/P-GW location information and the private IPv4 address assigned to the MTC device, or obtains such information from its local cache if so available. On the receipt of the private IPv4 address assigned to the MTC device, the MTC Gateway/Proxy initiates Translate Address Request/Reply procedure with the GGSN/PGW by passing the assigned private IPv4 Address and pseudo Port information to the GGSN/PGW. The ‘port’ chosen for the Translate Address Request procedure can be a dynamic/private (ephemeral port) in the range of 48k to 64k or some other port that is FFS. Alternatively, instead of the MTC Gateway/Proxy choosing the pseudo Port, such port could be chosen by the GGSN/P-GW. The GGSN/P-GW performs STUN Binding Request/Response (1308) procedure (RFC5389 – Session Traversal Utilities for NAT) with the STUN Server (Address Determination Server), which performs address translation and returns the mapped public transport address (public IP Address+ Port) information to the GGSN/P-GW in XOR-Mapped-Address attribute. Such information, in turn, is passed (1312) to the MTC Gateway/Proxy and to the MTC server. MTC server can now use such public transport address of the MTC device to initiate communications. The MTC device may be online or offline to receive such communications from the MTC server.

[00104] The GGSN/P-GW may use DNS Discovery procedures to determine the STUN Server, or STUN Server address information could be configured at the GGSN/P-GW. STUN message exchange between the GGSN/P-GW (STUN client) and the STUN Server can be protected by the Authentication and Message Integrity Mechanisms specified for STUN

protocol (RFC5389). STUN Binding Indications can be used for keep-alive procedures to maintain address translations at the NAT entities. Default settings of the lifetime information for address translations at the NAT, and keep-alive procedures are FFS. The MTC server 422 may then perform data packet communication 1304 via the NAT (translated addresses as data packets 1306).

Secnario-2:

[00105] FIG. 10 shows an exemplary process for Address Mapping and Data Transport with TURN Relay 1402. If NAT behaviour is 'Endpoint-Dependent' NAT ('non-EIM'), then it may behave as Address-Dependent or Address-and-Port-Dependent NAT. For such NATs, performing address resolution with a STUN Server whose address could be different from the address of the MTC server will not be a workable solution. Such NATs (non-EIM) may filter downlink packets that are not sent from the same transport address as that of the transport address of the STUN Server used for address mapping purpose. In this case, a Relay Server (TURN Relay) can be deployed to obtain the relay transport address for the MTC device.

[00106] When the MTC server wants to initiate communications with an MTC device, if it already does not have the (public) transport address information for the MTC device, the MTC server queries the transport address of the MTC device by sending a Query message 1410 to the MTC Gateway/Proxy. The Query message includes the MTC device ID. MTC Gateway/Proxy queries the HSS/HLR for the serving GGSN/P-GW location information and the private IPv4 address assigned to the MTC device, or obtains such information from its local cache if so available. On the receipt of the private IPv4 address assigned to the MTC device, the MTC Gateway/Proxy initiates Translate Address Request/Reply procedure with the GGSN/PGW by passing the assigned private IPv4 Address and pseudo Port information to the GGSN/PGW. The 'port' chosen for the Translate Address Request procedure can be a dynamic/private (ephemeral port) in the range of 48k to 64k or some other port that is FFS. Alternatively, instead of the MTC Gateway/Proxy choosing the pseudo Port, such port could be chosen by the GGSN/P-GW. Knowing that the NAT behaves as a non-EIM NAT, the GGSN/P-GW performs TURN Allocate Request/Response procedure 1408 (RFC5766 – Traversal Using Relays Around NAT) with the TURN Relay (Address Determination Server), which returns the relay transport address (public IP Address+ Port) to the GGSN/P-

GW in XOR-Relayed-Address Attribute. Such information, in turn, is passed to the MTC Gateway/Proxy and to the MTC server (1412). The GGSN/P-GW (TURN client) performs CreatePermission and/or ChannelBind procedure(s) with the TURN Relay to enable communications with the MTC server. MTC server can now use such TURN relay transport address to initiate communications with the MTC device. The MTC device may be online or offline to receive such communications from the MTC server.

[00107] The GGSN/P-GW may use DNS Discovery procedures to determine the serving TURN Relay or TURN Relay address information can be configured at the GGSN/P-GW. TURN message exchanges between the GGSN/P-GW (TURN client) and the TURN Relay can be protected by the Authentication and Message Integrity Mechanisms specified for TURN protocol (RFC5766). Binding Indications can be used for keep-alive procedures to maintain address translations at the NAT entities. Default settings of the lifetime information for address translations at the NAT, TURN relay address mappings lifetime and keep-alive procedures are FFS. Details of the CreatePermission and ChannelBind methods are also FFS.

[00108] The MTC server 422 may then perform data packet communication 1404 via the NAT (translated addresses as data packets 1406).

[00109] FIG. 15 is a flow chart representation of a process 1500 implementable at a network-side in a wireless communication network. The process 1500 may be implemented, e.g., on the platform on which the previously discussed MTC-IWF is implemented. At 1502, a trigger request including an external identification (ID) of a machine type communication (MTC) device is received. At 1504, a device information request that includes the external ID is transmitted. At 1506, in response to the device information request, a first IP address is received for the MTC device. The first IP address may be in a private address space of the wireless network. At 1508, a second IP address is obtained based on the first IP address. The second IP address corresponds to a translation of the first IP address in a second network from which the trigger request was received. In some implementations, the second IP address may be obtained by transmitting an address translation request including the first IP address and receiving the second IP address in response. In some implementations, the trigger request is responded to by providing a response message that includes the second IP address. In some implementations, the second IP address may correspond to the public space. The process 1500 may be applicable to IPv4 addresses.

[00110] FIG. 16 is a block diagram representation of an apparatus 1600 for facilitating wireless communications. The module 1602 (e.g., a trigger request receiver) is for receiving a trigger request including an external identification (ID) of a machine type communication (MTC) device. The module 1604 (e.g., a request transmitter) is for transmitting a device information request including the external ID. The module 1606 (e.g., an IP address receiver) is for receiving, in response to the device information request, a first IP address for the MTC device, the first IP address being in a private address space of the wireless network. The module 1608 (e.g., an IP address obtainer) is for obtaining a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received. The apparatus 1600 and modules 1602, 1604, 1606, 1608 may be configured to further perform one or more techniques disclosed in this document.

[00111] FIG. 17 is a flow chart representation of a process 1700 implementable at a gateway device in a wireless communication system. At 1702, a request is received to perform translation of a first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system. At 1704, a second IP address is obtained for the MTC device, the second IP address being in a second IP address space different from the first IP address space. At 1706, a response is transmitted to the request by including the second IP address. At 1708, user data plane communication to and from the MTC device and another communication entity in the second IP address space is facilitated.

[00112] FIG. 18 is a block diagram representation of a portion of a gateway device 1800 operable in a wireless communications network. The module 1802 (e.g., a request receiver) is for receiving a request to perform translation of a first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system. The module 1804 (e.g., an IP address obtainer) is for obtaining a second IP address for the MTC device, the second IP address being in a second IP address space different from the first IP address space. The module 1806 (e.g., a response transmitter) is for transmitting a response to the request by including the second IP address. The module 1808 (e.g., a gateway server) is for facilitating user data plane communication to and from the MTC device and another communication entity in the second IP address space. The apparatus 1800 and modules 1802, 1804, 1806, 1808 may further be configured to implement one or more techniques disclosed in this document.

[00113] It will be appreciated that techniques for identifying IP address of a machine type communication (MTC) device located behind an NAT are disclosed. MTC devices often are located in a wireless network in which a private IPv4 address is often allocated to the MTC device. Because of limitations in the range of address available using IPv4 protocol, the private address may be in an address range different from a range in which an MTC server's IP address may be. Therefore, the MTC server may not be directly able to communicate with the MTC device and may need address translation services. However, because the MTC device typically operates by entering long sleep modes, the private IPv4 address of the MTC device may not be available to the MTC server when the MTC server wants to communicate with the MTC device.

[00114] It will be appreciated that the disclosed signal exchange technique, in one aspect, allow an MTC device to discover its own public IP address (i.e., the IP address by which the MTC device is known to an MTC server). In one aspect, this knowledge may be useful for the MTC device to be able to establish secure communication or request and receive digital certificates that include information about the public IP address of the MTC device.

[00115] It will further be appreciated that the disclosed processes, apparatus and system, in one aspect, facilitate rapid communication between an external device (e.g., an MTC server) and the MTC device, regardless of whether the MTC device is in an active state with an already assigned IP address, in a mode in which the MTC device has its RF turned off but still has an IP address assigned or in a mode in which the MTC device has its RF turned off and no IP address is currently assigned to the MTC device (Active, Dormant and Inactive states). Using the signal exchanges disclosed in the present document, a practical system may be able to establish communication with the MTC device within a short period of time of the order of a few (e.g., 2 to 10) milliseconds, regardless of the operational mode of the MTC device when a trigger request is received for establishing communication with the MTC device.

[00116] The disclosed and other embodiments and the functional operations described in this document can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this document and their structural equivalents, or in combinations of one or more of them. The disclosed and other embodiments can be implemented as one or more computer program products, i.e., one or more modules of computer program instructions encoded on a computer readable medium for

execution by, or to control the operation of, data processing apparatus. The computer readable medium can be a machine-readable storage device, a machine-readable storage substrate, a memory device, a composition of matter effecting a machine-readable propagated signal, or a combination of one or more them. The term “data processing apparatus” encompasses all apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, or multiple processors or computers. The apparatus can include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them. A propagated signal is an artificially generated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal, that is generated to encode information for transmission to suitable receiver apparatus.

[00117] A computer program (also known as a program, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program does not necessarily correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[00118] The processes and logic flows described in this document can be performed by one or more programmable processors executing one or more computer programs to perform functions by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus can also be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application specific integrated circuit).

[00119] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read only memory or a random access memory or both. The essential elements of a

computer are a processor for performing instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto optical disks, or optical disks. However, a computer need not have such devices. Computer readable media suitable for storing computer program instructions and data include all forms of non volatile memory, media and memory devices, including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto optical disks; and CD ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[00120] While this document contains many specifics, these should not be construed as limitations on the scope of an invention that is claimed or of what may be claimed, but rather as descriptions of features specific to particular embodiments. Certain features that are described in this document in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a sub-combination or a variation of a sub-combination. Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results.

[00121] Only a few examples and implementations are disclosed. Variations, modifications, and enhancements to the described examples and implementations and other implementations can be made based on what is disclosed.

CLAIMS

What is claimed is:

1. A method, implementable at a network-side in a wireless communication network, comprising:
 - receiving a trigger request including an external identification (ID) of a machine type communication (MTC) device;
 - transmitting a device information request including the external ID;
 - receiving, in response to the device information request, a first internet protocol (IP) address for the MTC device, the first IP address being in a private address space of the wireless network; and
 - obtaining a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received.
2. The method of claim 1, wherein the obtaining the second IP address includes:
 - transmitting an address translation request including the first IP address; and
 - receiving the second IP address in an address translation response message.
3. The method of claim 1, further comprising:
 - responding to the trigger request by providing a trigger response message including the second IP address.
4. The method of claim 1, wherein the first IP address and the second IP address comprise IP version 4 (IPv4) addresses.
5. The method of claim 1, wherein the trigger request is received when the MTC device does not have any IP address assigned.
6. An apparatus, operable at a network-side in a wireless communication network, comprising:
 - a trigger request receiver that receives a trigger request including an external identification (ID) of a machine type communication (MTC) device;

a request transmitter that transmits a device information request including the external ID;

an internet protocol (IP) address receiver that receives, in response to the device information request, a first IP address for the MTC device, the first IP address being in a private address space of the wireless network; and

an IP address obtainer that obtains a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received.

7. The apparatus of claim 6, wherein the IP address obtainer includes:

a translation request transmitter that transmits an address translation request including the first IP address; and

another IP address receiver that receives the second IP address in an address translation response message.

8. The apparatus of claim 6, further comprising:

a trigger request responder that responds to the trigger request by providing a trigger response message including the second IP address.

9. The apparatus of claim 6, wherein the first IP address and the second IP address comprise IP version 4 (IPv4) addresses.

10. The apparatus of claim 6, wherein the trigger request is received when the MTC device does not have any IP address assigned.

11. A computer program product comprising a non-volatile, computer-readable medium having code stored thereupon, the code, when executed on a processor, causing the processor to implement a method, comprising:

receiving a trigger request including an external identification (ID) of a machine type communication (MTC) device;

transmitting a device information request including the external ID;

receiving, in response to the device information request, a first internet protocol (IP) address for the MTC device, the first IP address being in a private address space of the wireless network; and

obtaining a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received.

12. The computer program product of claim 11, wherein the obtaining the second IP address includes:

transmitting an address translation request including the first IP address; and
receiving the second IP address in an address translation response message.

13. The computer program product of claim 11, wherein the method further comprises:

responding to the trigger request by providing a trigger response message including the second IP address.

14. The computer program product of claim 11, wherein the first IP address and the second IP address comprise IP version 4 (IPv4) addresses.

15. The computer program product of claim 11, wherein the trigger request is received when the MTC device does not have any IP address assigned.

16. An apparatus, operable at a network side in a wireless communications network, comprising:

means for receiving a trigger request including an external identification (ID) of a machine type communication (MTC) device;

means for transmitting a device information request including the external ID;

means for receiving, in response to the device information request, a first internet protocol (IP) address for the MTC device, the first IP address being in a private address space of the wireless network; and

means for obtaining a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received.

17. The apparatus of claim 16, wherein the means for obtaining the second IP address includes:

means for transmitting an address translation request including the first IP address;

and

means for receiving the second IP address in an address translation response message.

18. The apparatus of claim 16, further comprising:

means for responding to the trigger request by providing a trigger response message including the second IP address.

19. The apparatus of claim 16, wherein the first IP address and the second IP address comprise IP version 4 (IPv4) addresses.

20. The apparatus of claim 16, wherein the trigger request is received when the MTC device does not have any IP address assigned.

21. A method, implementable at a gateway device in a wireless communications network, comprising:

receiving a request to perform translation of a first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system;

obtaining a second IP address for the MTC device, the second IP address being in a second IP address space different from the first IP address space;

transmitting a response to the request by including the second IP address; and

facilitating user data plane communication to and from the MTC device and another communication entity in the second IP address space.

22. The method of claim 21, wherein the operation of obtaining a second IP address comprises:

exchanging messages with a session traversal utilities for network address translation (STUN) server.

23. The method of claim 22, wherein the exchanging the messages includes: transmitting an address binding request including the first IP address; and receiving the second IP address in a binding response message.

24. The method of claim 21, wherein the operation of obtaining a second IP address comprises:
exchanging messages with a traversal using relay network address translation (TURN) server.

25. The method of claim 24, wherein the exchanging the messages includes: transmitting an address binding request including the first IP address; and receiving the second IP address in a binding response message.

26. An apparatus, operable at a gateway device in a wireless communications network, comprising:
a request receiver that receives a request to perform translation of a first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system;
an IP address obtainer that obtains a second IP address for the MTC device, the second IP address being in a second IP address space different from the first IP address space;
a response transmitter that transmits a response to the request by including the second IP address; and
a gateway that facilitates user data plane communication to and from the MTC device and another communication entity in the second IP address space.

27. The apparatus of claim 26, wherein the IP address obtainer includes:
a message exchanger that exchanges messages with a session traversal utilities for network address translation (STUN) server.

28. The apparatus of claim 27, wherein the message exchanger includes:

a binding request transmitter that transmits an address binding request including the first IP address; and

a binding response receiver that receives the second IP address in a binding response message.

29. The apparatus of claim 26, wherein the IP address obtainer includes:

a message exchanger that exchanges messages with a traversal using relay network address translation (TURN) server.

30. The apparatus of claim 29, wherein the exchanging the messages includes:

a binding request transmitter that transmits an address binding request including the first IP address; and

a binding response receiver that receives the second IP address in a binding response message.

31. A computer program product comprising a non-volatile, computer-readable medium having code stored thereupon, the code, when executed on a processor, causing the processor to implement a method, comprising:

receiving a request to perform translation of a first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system;

obtaining a second IP address for the MTC device, the second IP address being in a second IP address space different from the first IP address space;

transmitting a response to the request by including the second IP address; and

facilitating user data plane communication to and from the MTC device and another communication entity in the second IP address space.

32. The computer program product of claim 31, wherein the operation of obtaining a second IP address comprises:

exchanging messages with a session traversal utilities for network address translation (STUN) server.

33. The computer program product of claim 32, wherein the exchanging the messages includes:

transmitting an address binding request including the first IP address; and
receiving the second IP address in a binding response message.

34. The computer program product of claim 31, wherein the operation of obtaining a second IP address comprises:

exchanging messages with a traversal using relay network address translation (TURN) server.

35. The computer program product of claim 34, wherein the exchanging the messages includes:

transmitting an address binding request including the first IP address; and
receiving the second IP address in a binding response message.

36. An apparatus operable at a gateway in a wireless communications network, comprising:

means for receiving a request to perform translation of a first Internet Protocol (IP) address of a machine type communication (MTC) device that is in a first IP address space private to the wireless communication system;

means for obtaining a second IP address for the MTC device, the second IP address being in a second IP address space different from the first IP address space;

means for transmitting a response to the request by including the second IP address;
and

means for facilitating user data plane communication to and from the MTC device and another communication entity in the second IP address space.

37. The apparatus of claim 36, wherein the means for obtaining a second IP address comprises:

means for exchanging messages with a session traversal utilities for network address translation (STUN) server.

38. A wireless communications system, comprising:

a machine type communication interworking function (MTC-IWF) that:

- receives a trigger request including an external identification (ID) of a machine type communication (MTC) device;

- transmits a device information request including the external ID;

- receives, in response to the device information request, a first internet protocol (IP) address for the MTC device, the first IP address being in a private address space of the wireless network; and

- obtains a second IP address based on the first IP address, the second IP address corresponding to a translation of the first IP address in a second network from which the trigger request was received; and

- a packet data gateway (P-GW) that:

- receives a request to perform translation of the first IP address;

- exchanges messages to generate the second IP address for the MTC device;

- provides the second IP address to the MTC-IWF; and

- facilitates user data plane communication to and from the MTC device and another communication entity in the second IP address space.

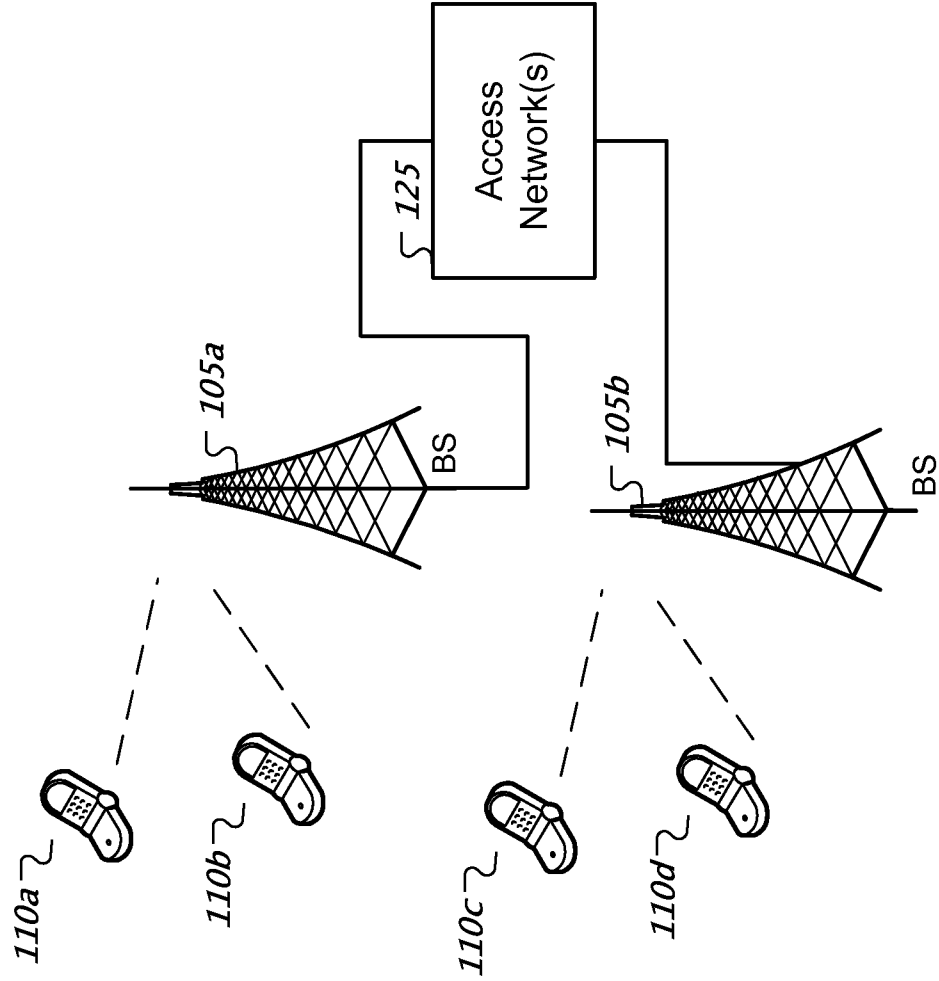


FIG. 1

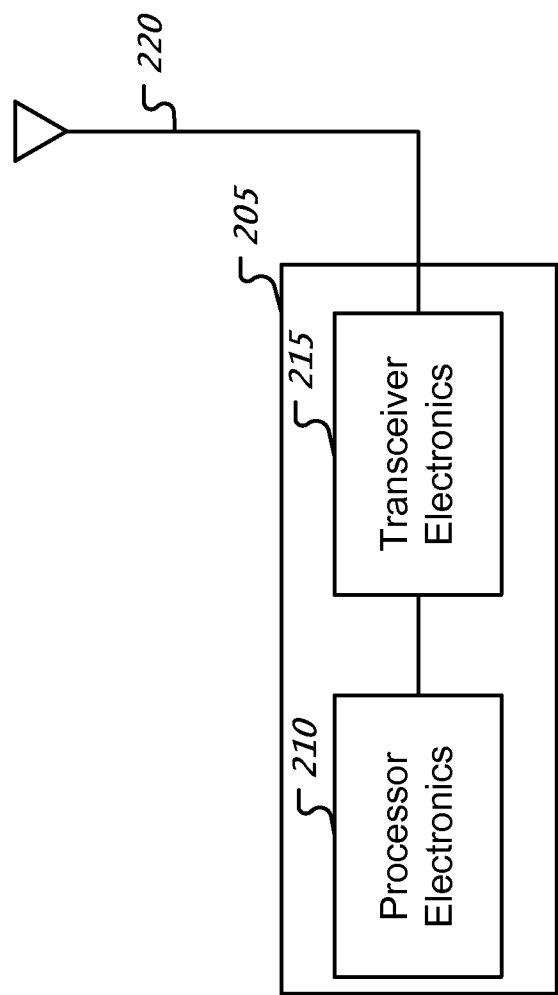


FIG. 2

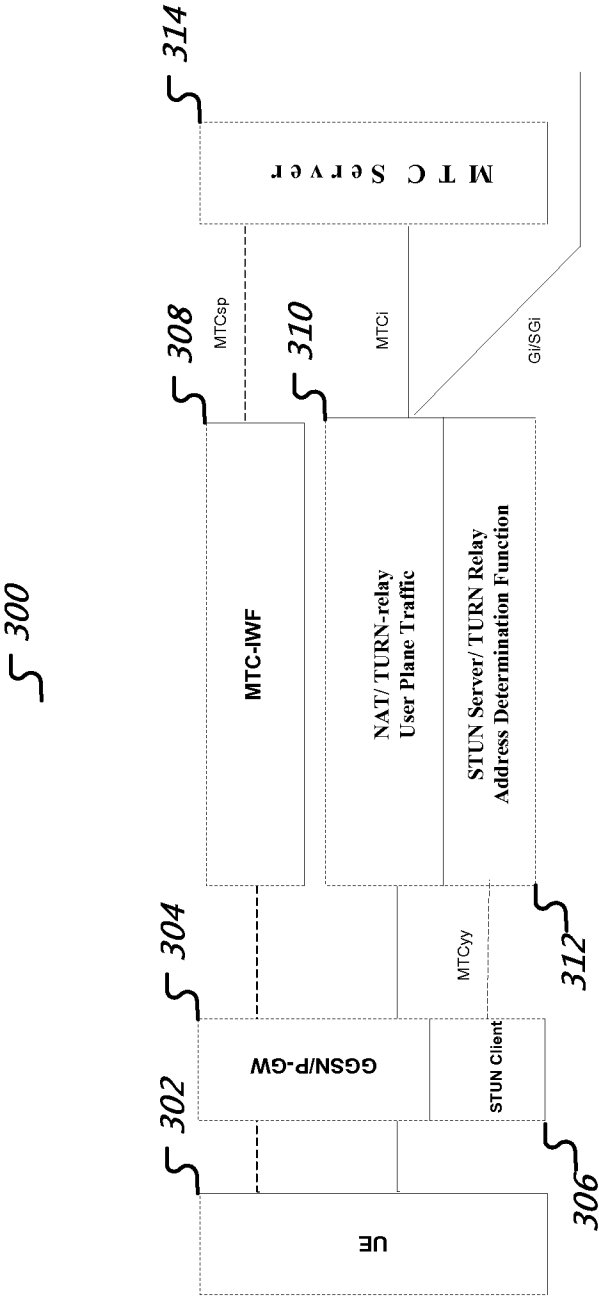


FIG. 3

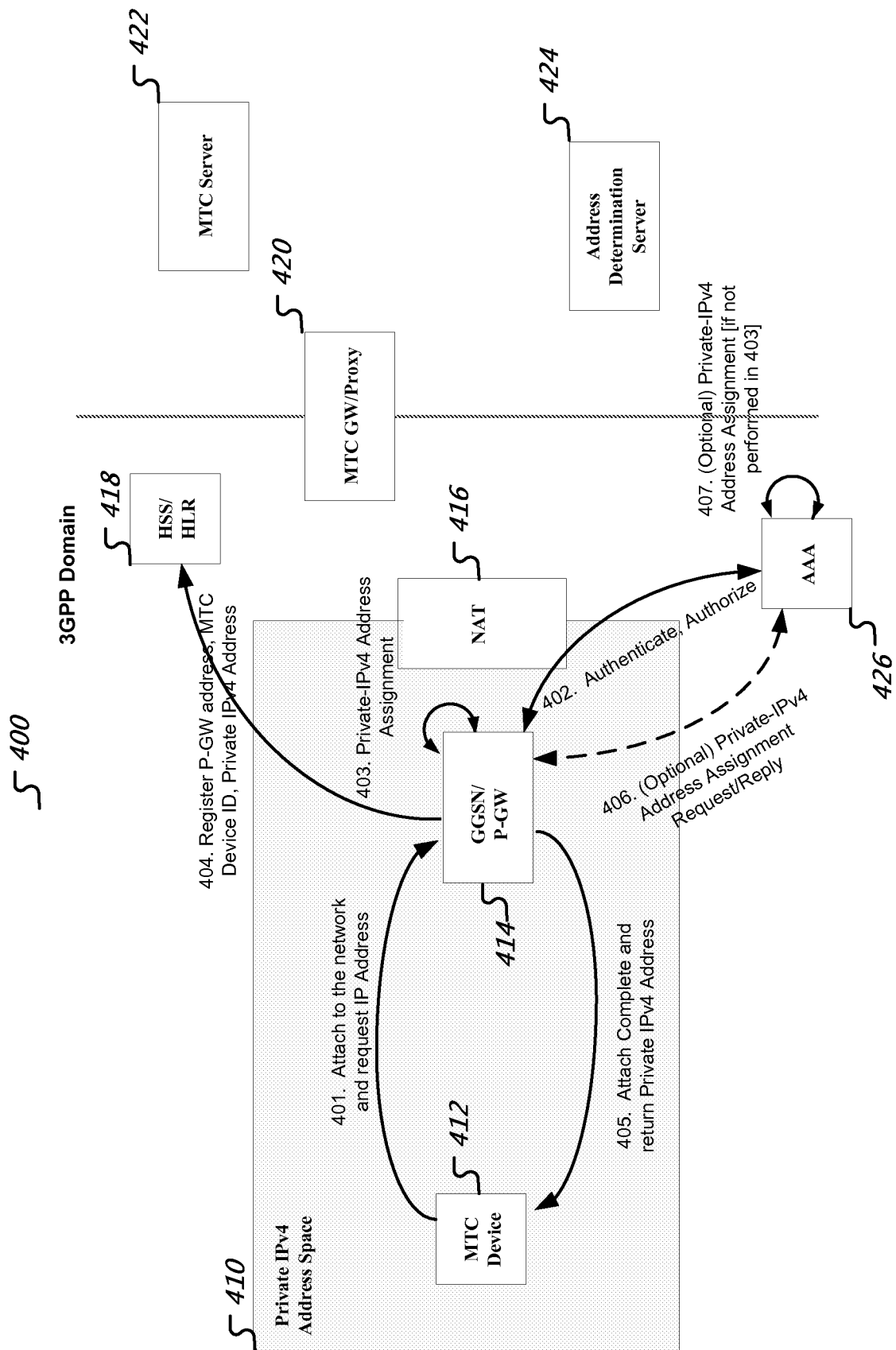


FIG. 4

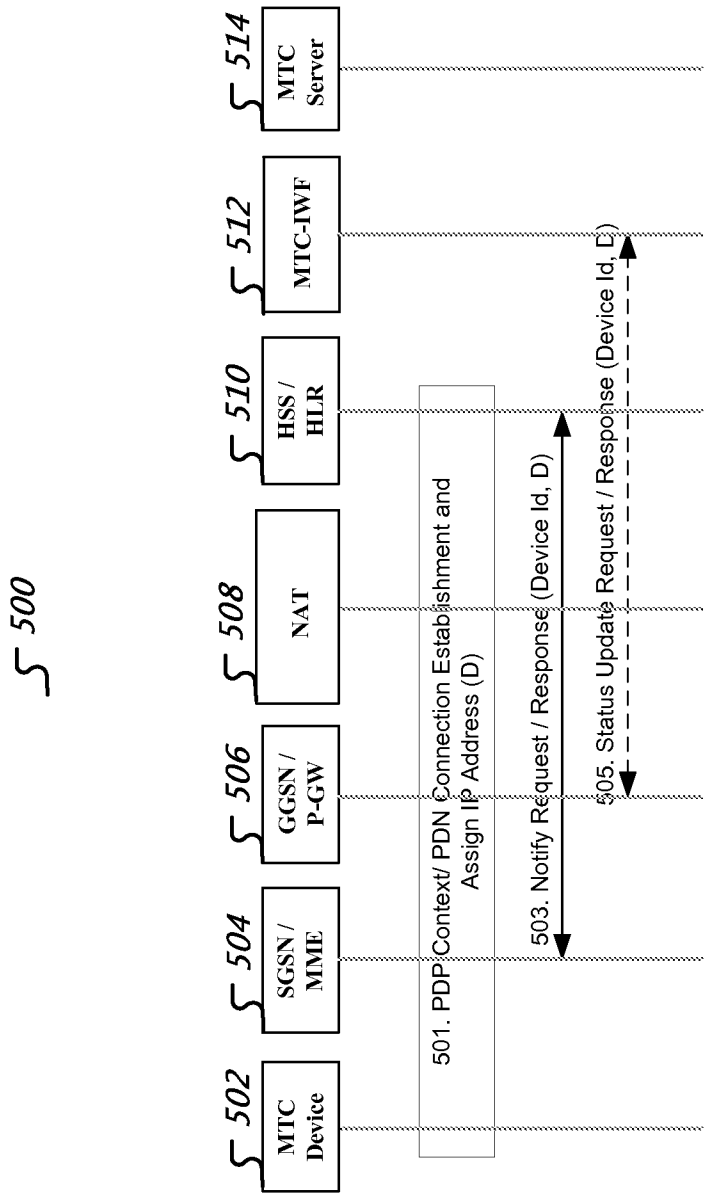


FIG. 5

5 600

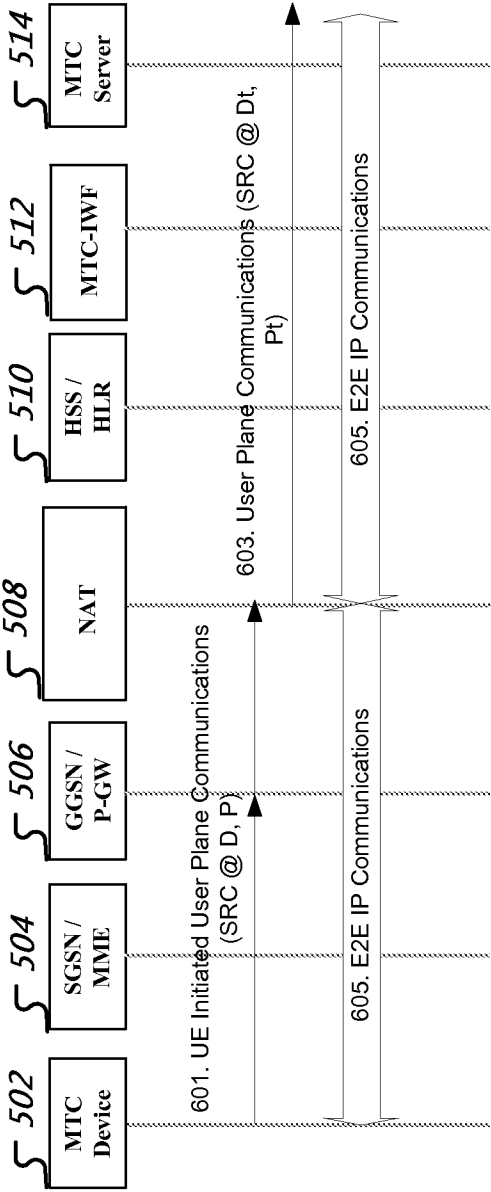


FIG. 6

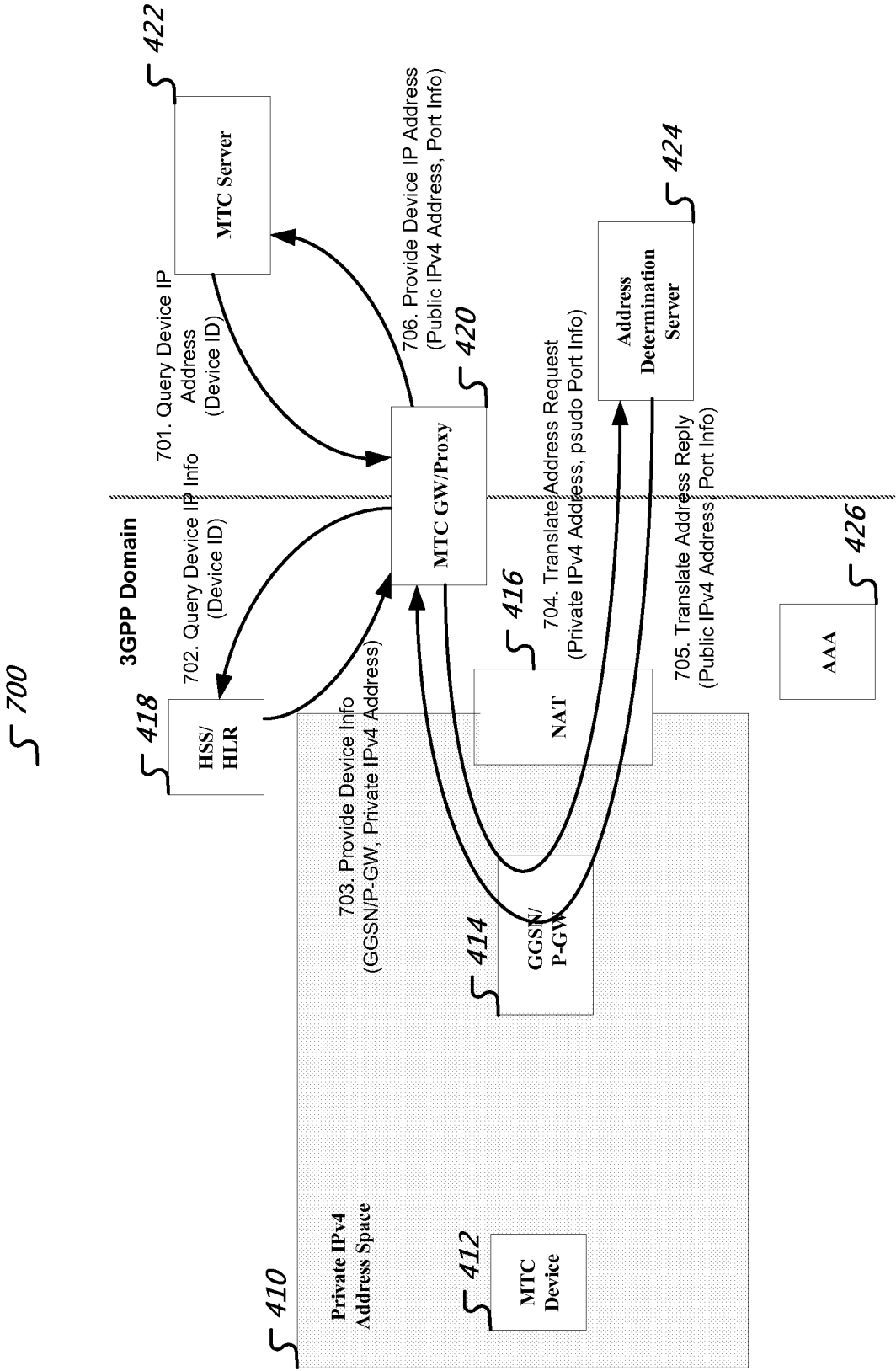


FIG. 7

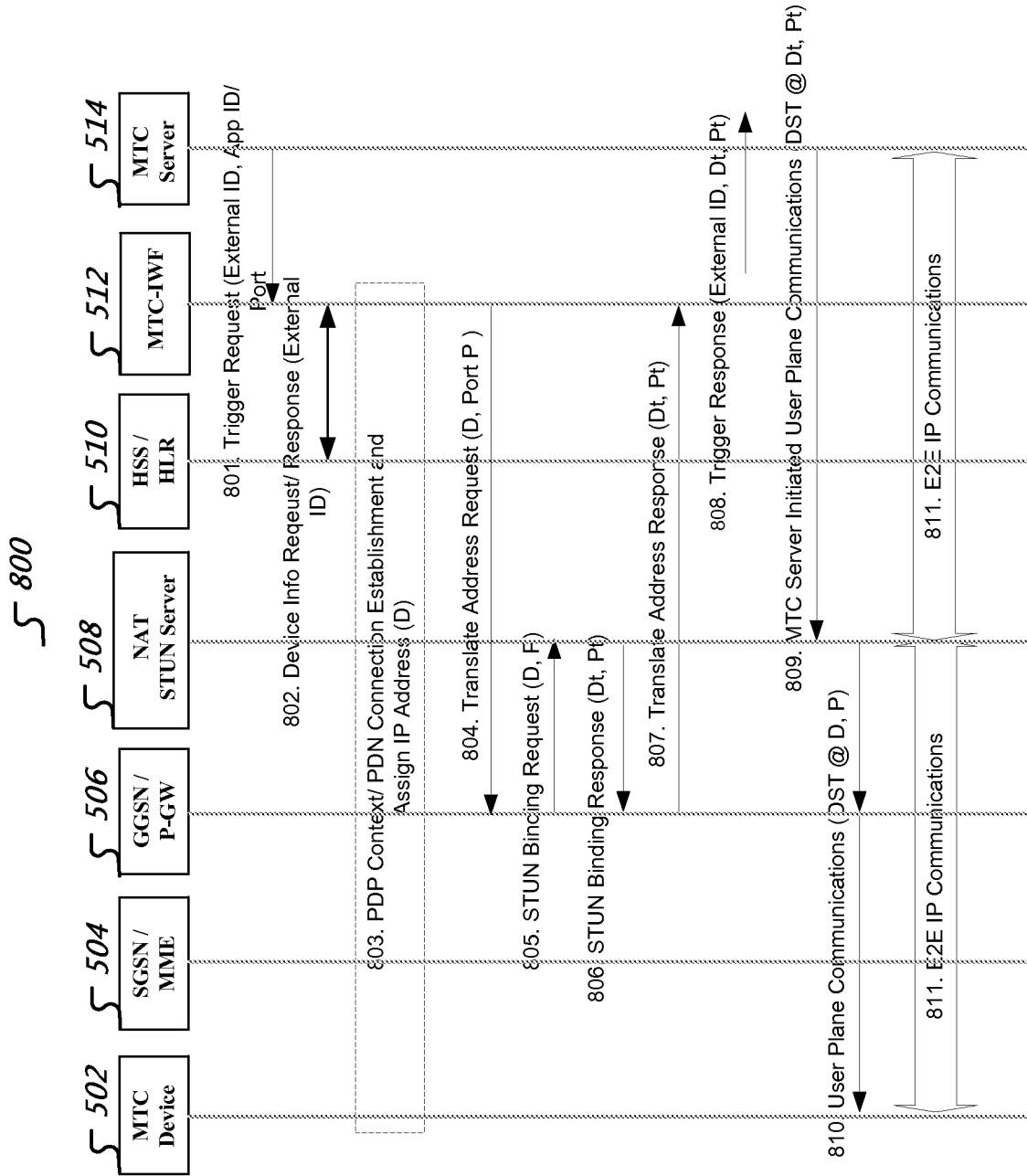


FIG. 8

900

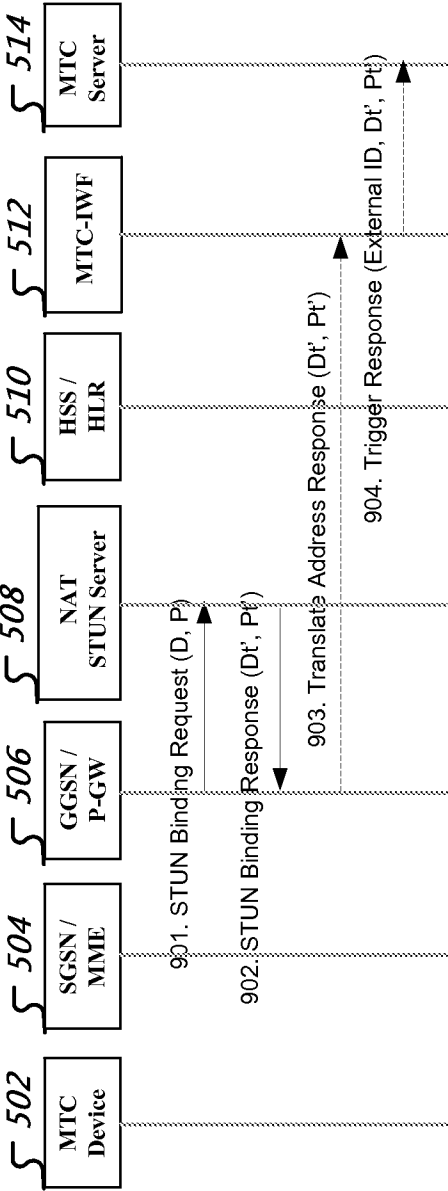


FIG. 9

Σ 1000

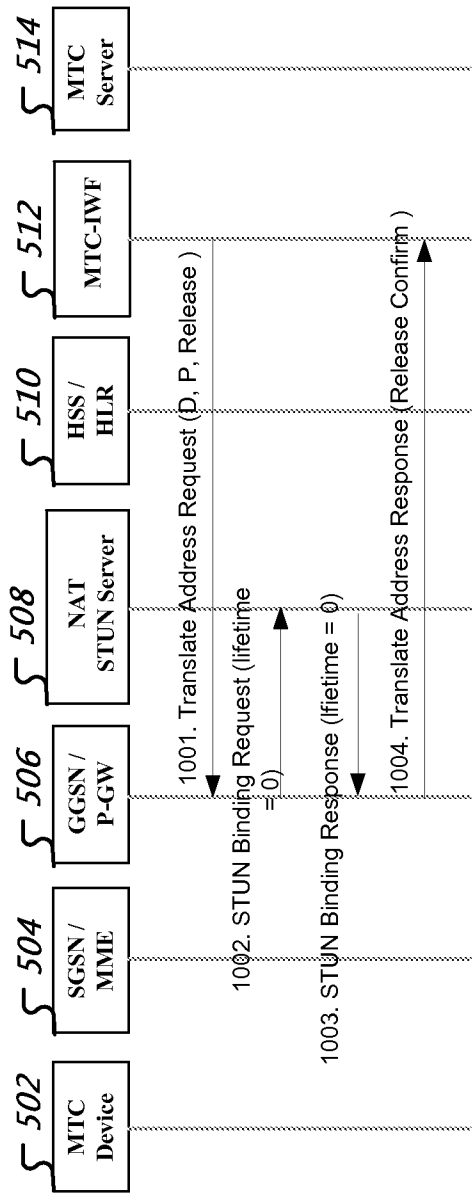


FIG.10

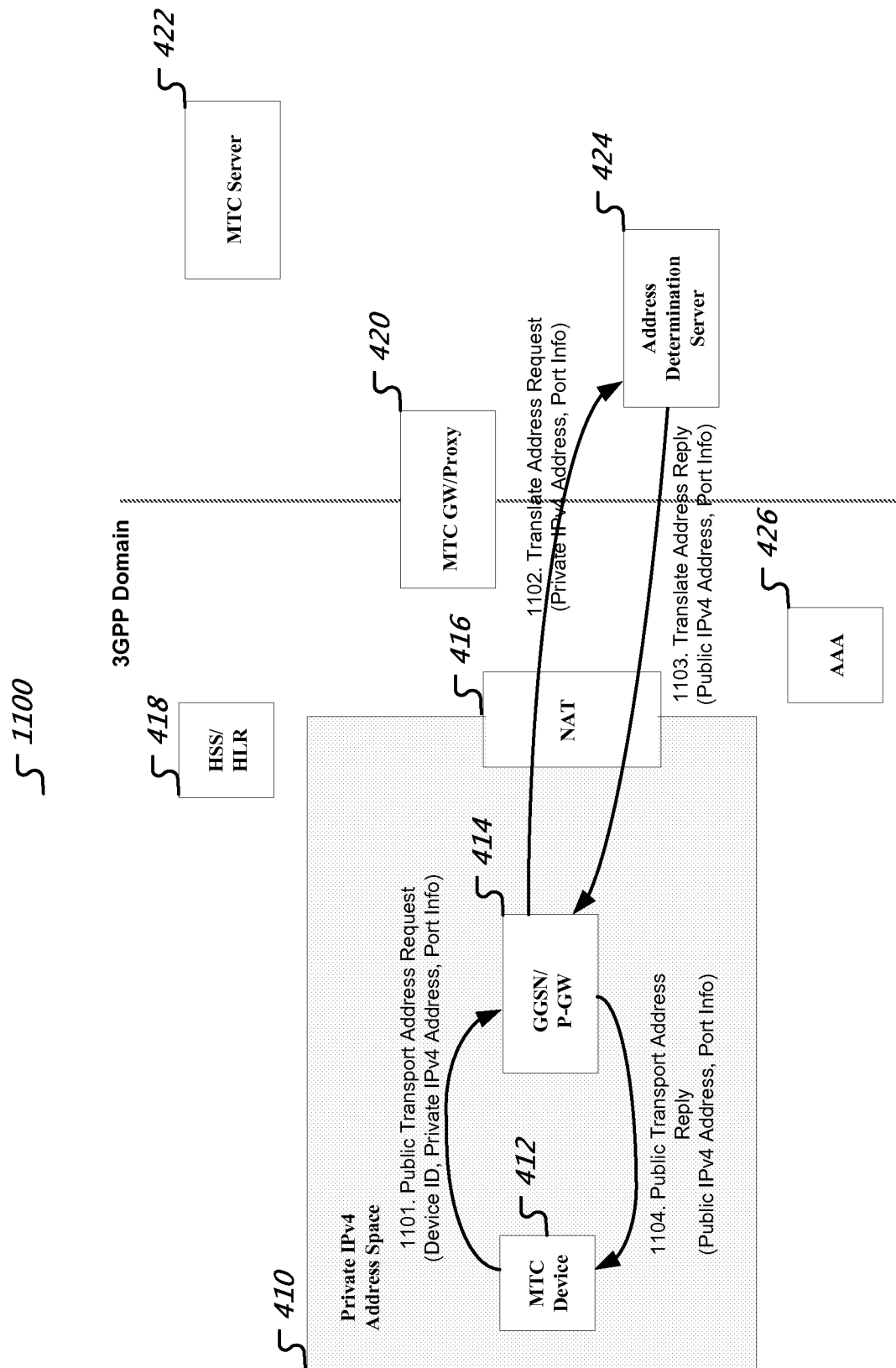


FIG. 11

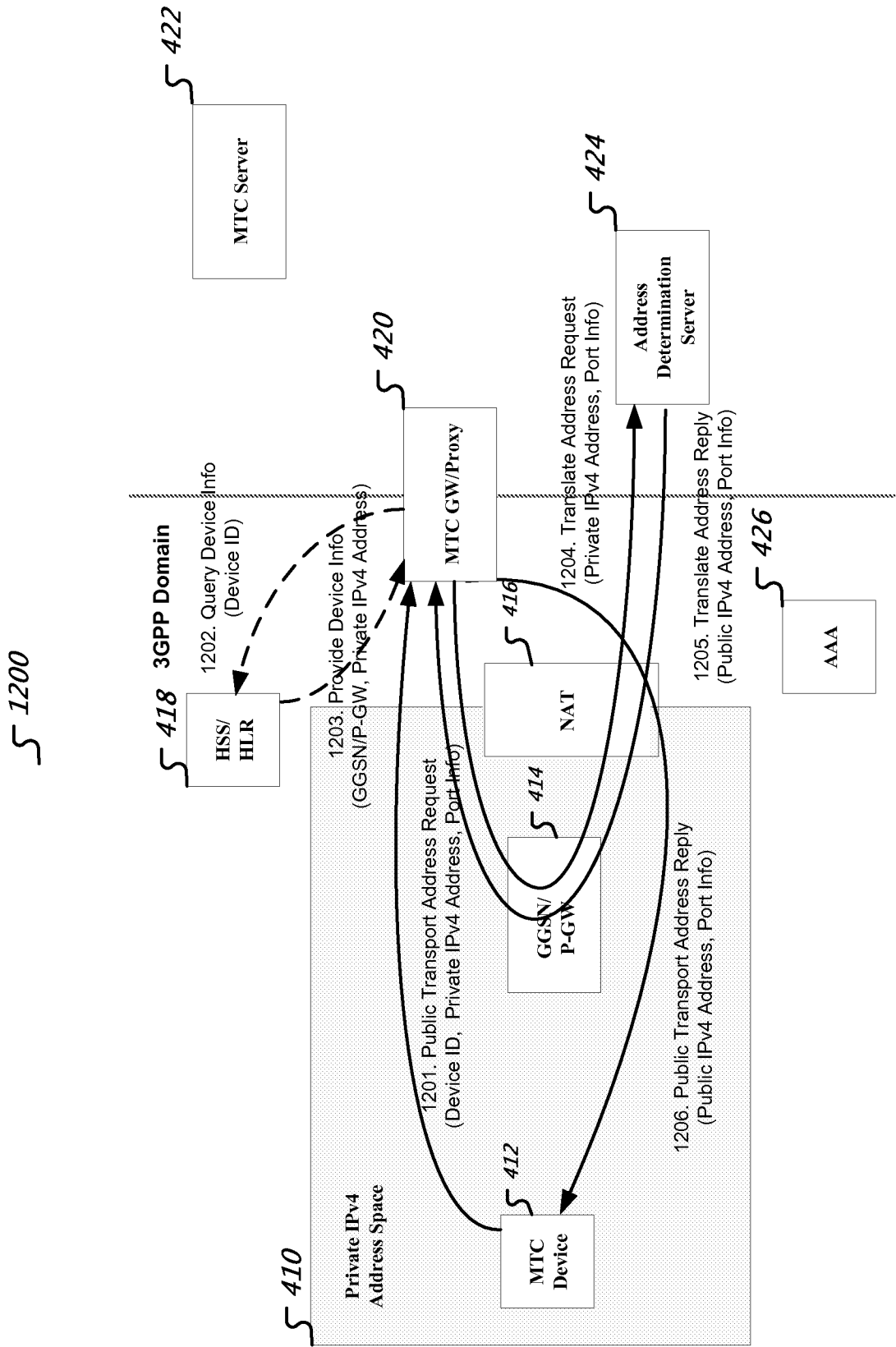


FIG. 12

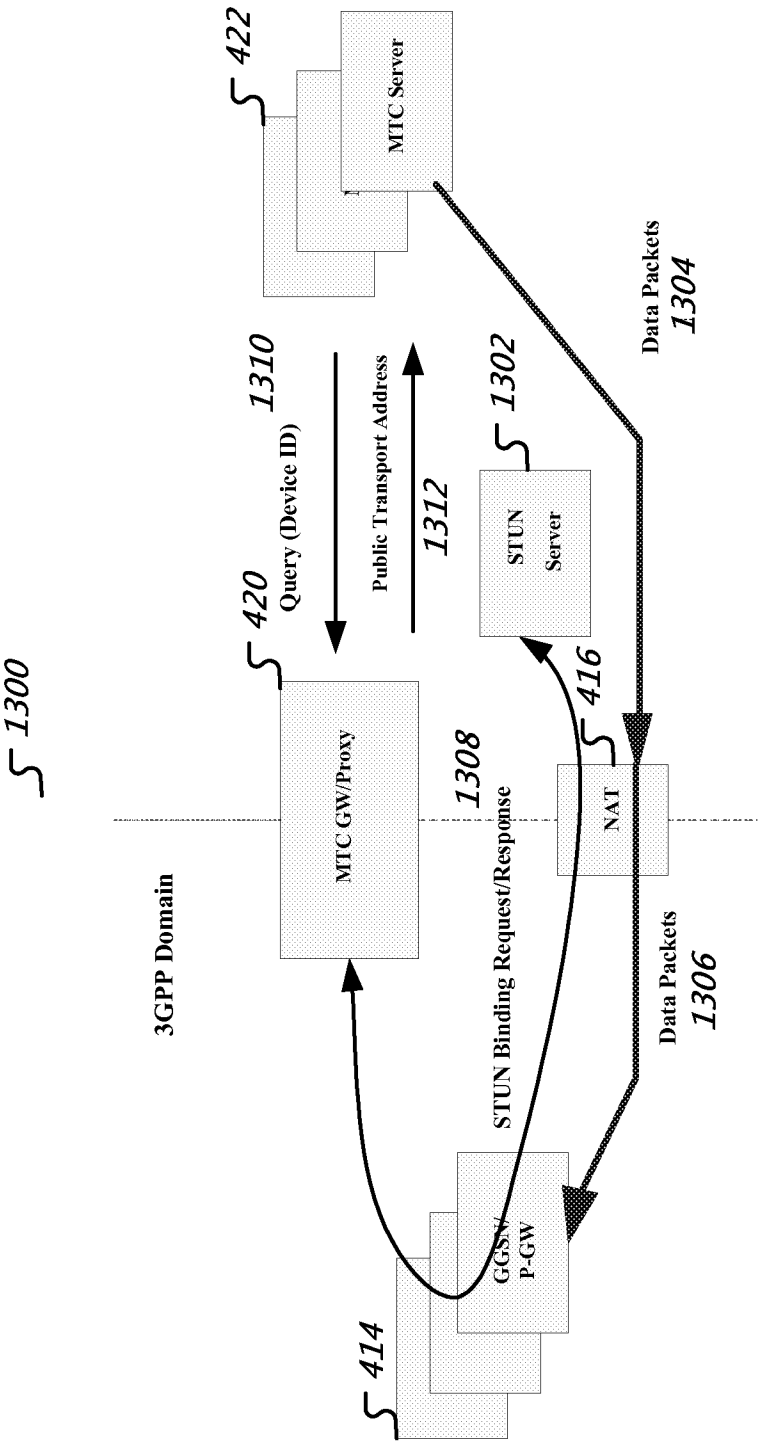


FIG. 13

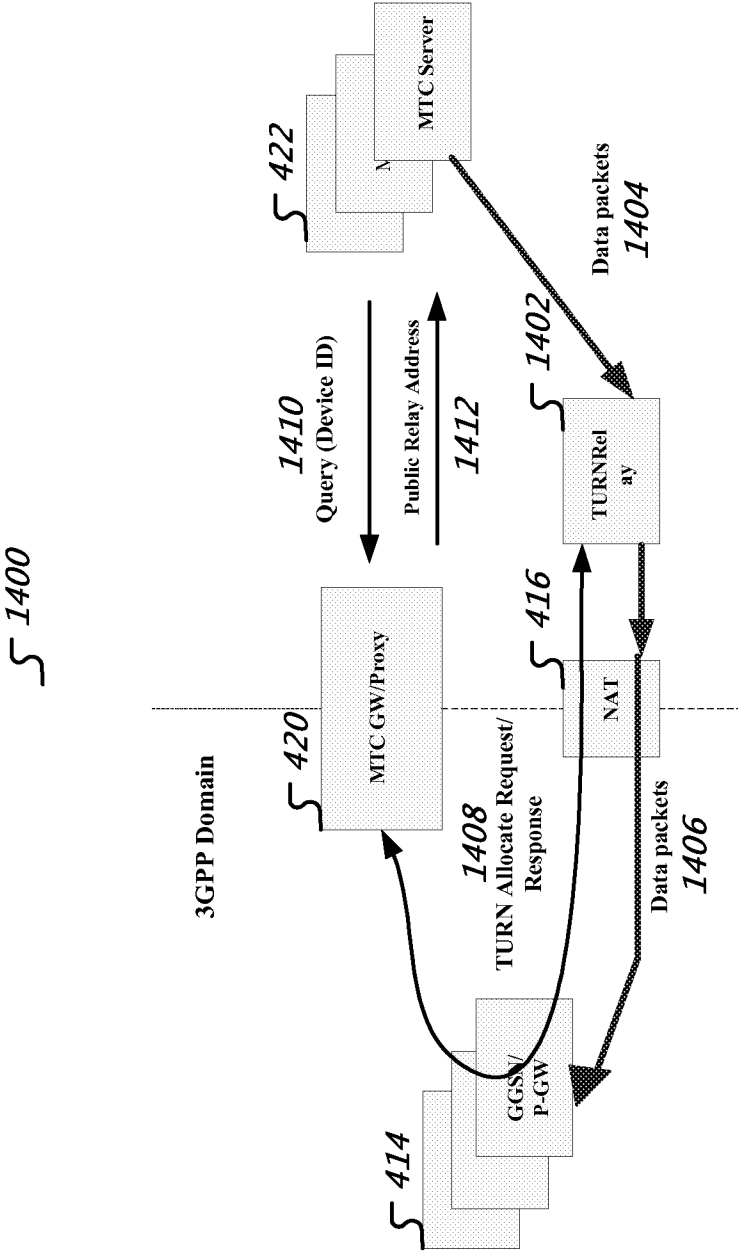


FIG. 14

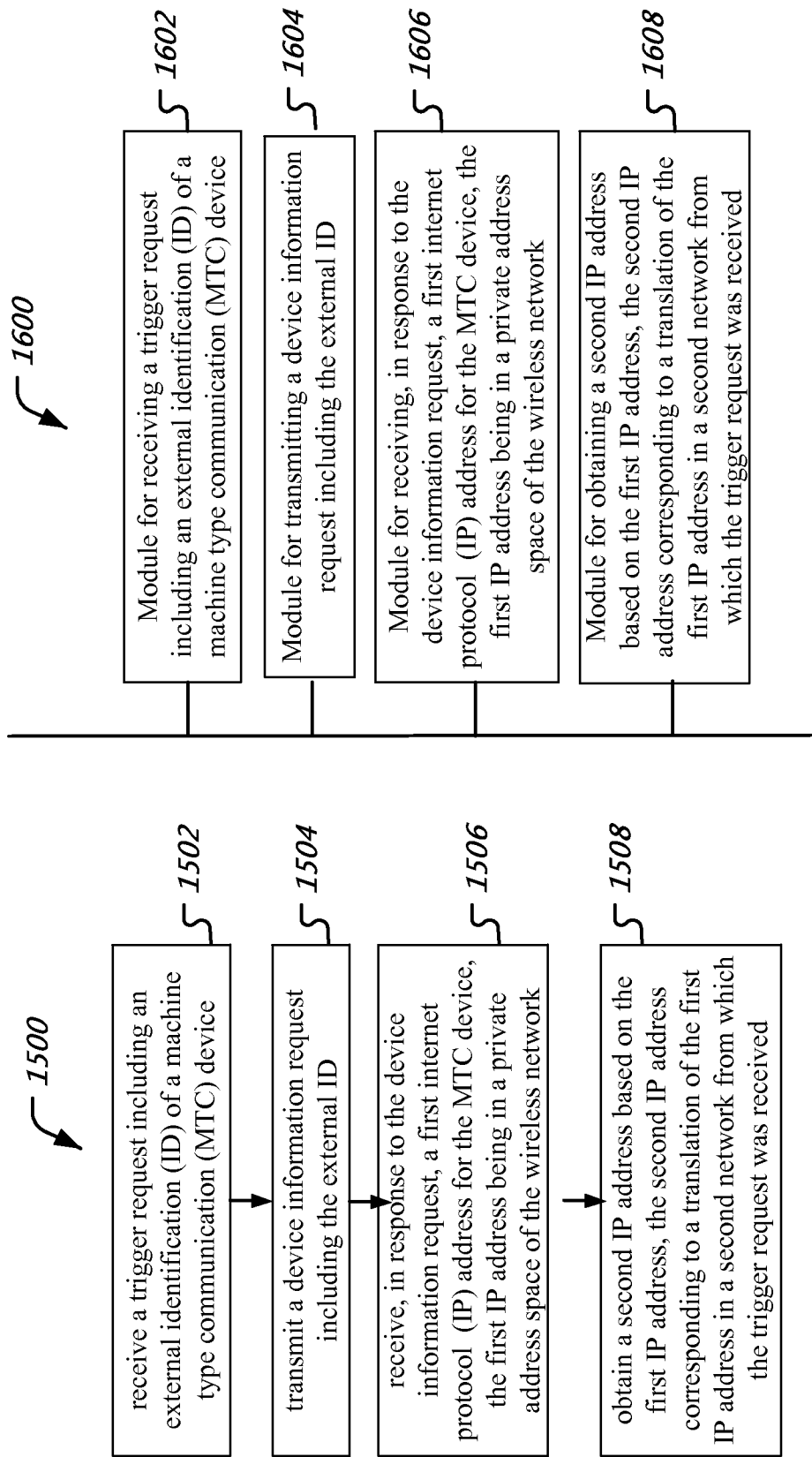
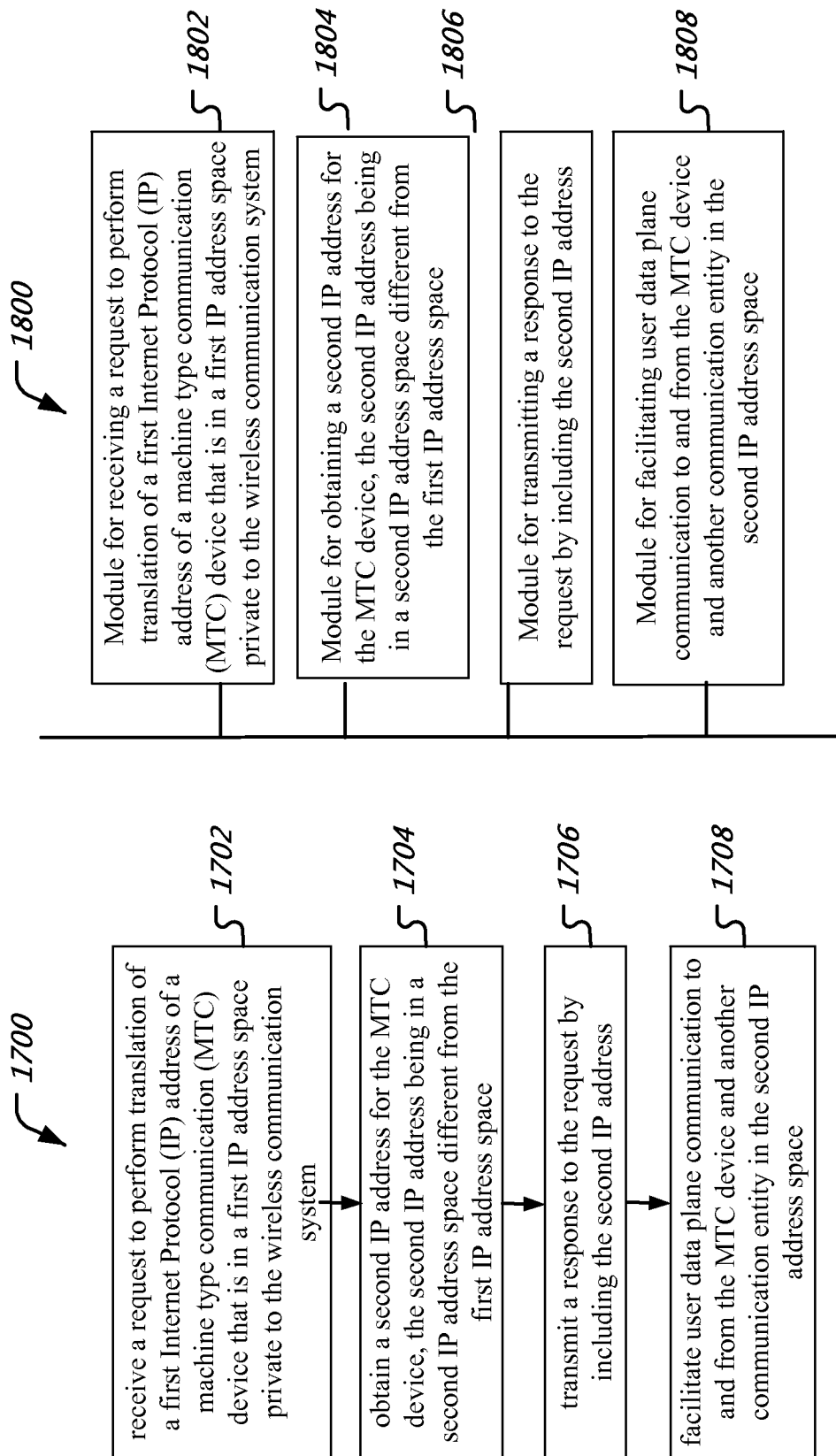


FIG. 15

FIG. 16

**FIG. 18****FIG. 17**