(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 November 2003 (20.11.2003)

PCT

(10) International Publication Number
WO 03/096588 A2

(51) International Patent Classification⁷: H04L

(21) International Application Number: PCT/US03/11619

(22) International Filing Date: 14 April 2003 (14.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/372,655 15 April 2002 (15.04.2002) US

(71) Applicant *(for all designated States except US)*: **FLARION TECHNOLOGIES, INC.** [US/US]; Bedminster One, 135 Route 202/206 South, Bedminster, NJ 07921 (US).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only)*: **O'NEILL , Alan** [GB/AU]; 184 Military Road, Henley Beach, South Australia 5022 (AU).

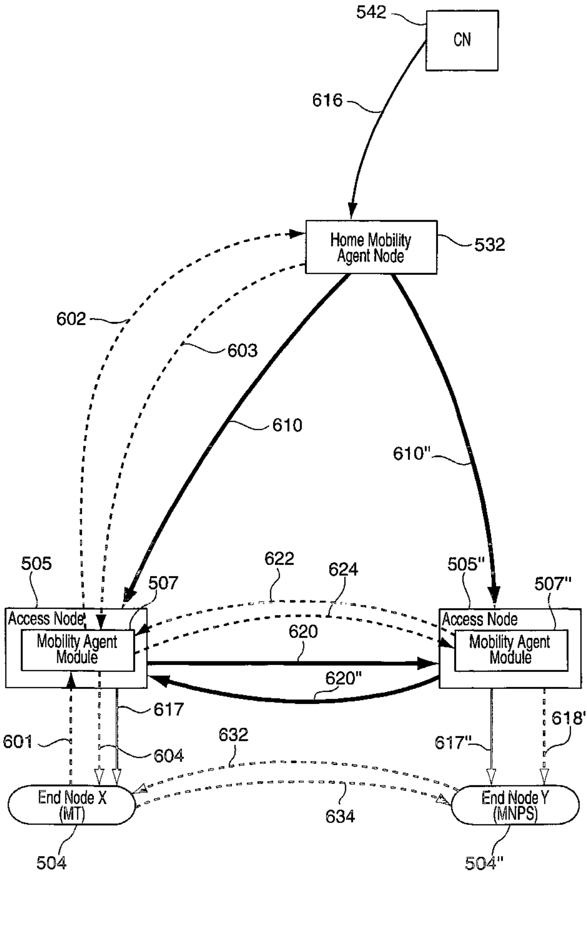
(74) **Agent: STRAUB, Michael, P.**; Straub & Pokotylo, 1 Bethany Road, Suite 83, Bldg. 6, Hazlet, NJ 07730 (US).

(81) **Designated States** *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (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 EXTENDING MOBILE IP



**(57) Abstract:** Methods and apparatus for extending Mobile IP to enable a Mobile IP Home Agent to forward to a default proxy MN server when it does not have a current binding for a MN home address. This can be used to route traffic when the MN is absent and to add processes onto the Proxy MN server that enables application intelligence at the Proxy MN server to act on behalf of the MN when the MN so wishes, e.g. substituting for the MN while the MN is in sleep mode or otherwise unavailable.

WO 03/096588 A2

**Published:**

— *without international search report and to be republished upon receipt of that report*

# METHODS AND APPARATUS FOR EXTENDING MOBILE IP

## RELATED APPLICATIONS

The present application claims the benefit of the filing date of U.S. Provisional Patent Application 60/372,655 filed April 15, 2002 titled "Communications Methods and Apparatus".

## FIELD OF THE INVENTION

The present application relates to communications methods and, more particularly, to methods and apparatus for extending mobile IP to support proxy mobile node servers and to using such servers to act as mobile node proxies with regard to one or more existing applications.

## BACKGROUND

Mobile IP (v4/v6), also indicated as MIPv4 and MIPv6 enables a mobile node (MN) to register its temporary location indicated by a care-of-address (CoA) to its Home Agent (HA). MIPv4 is described at http://www.ietf.org/rfc/rfc3220.txt MIPv6 is described in http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-21.txt. In MIP the HA then keeps a mapping (also called a binding) between the MN's permanent address, otherwise called Home Address (HoA), and the registered CoA so that packets for that MN can be redirected to its current location using IP encapsulation techniques (tunneling).

The CoA used by a MN can be an address that belongs to a Foreign Agent (FA) when MIPv4 is used or, in MIPv4 and MIPv6, it can be a temporarily allocated address to the MN itself in which case is called a collocated care-of-address (CCoA).

The concepts and solutions described here are applicable to both MIPv4 and MIP unless otherwise mentioned.

MIPv4/v6 also has a feature called reverse tunneling. This ensures that all uplink traffic from the MN goes via the HA before its final destination. The traffic is essentially tunnelled back to the HA either by the MN itself or by the FA the MN is connected to. Similarly as before, the HA will not accept reverse tunnelled packets from a given CoA or CCoA unless the MN registers that CoA/CCoA with it.

In Mobile IP the home subnet is the location of the HA and is also where the MN is typically located. When a MN is on its home subnet, the MN responds to Address Resolution Protocol (ARP) requests for the HoA. When it is away from home, the HA instead uses proxy ARP to respond to ARP requests for the HoA of the MN so that packets for the MN are routed towards and by the HA towards the current CoA. When a MN returns home, the HA and the MN send gratuitous ARP signals to update all the ARP caches to inform them that the MN is now home and that the link-layer address for the HoA is now that of the MN and not the HA. If the MN is not at home, and the HA does not have a current CoA binding for the MN, then both the HA and the absent MN will ignore incoming packets which will blindly be dropped on the subnet. The AR processing is described in section 4.6 of IETF RFC 3220. In mobility systems, such as in 3G cellular or 802.11, especially when dynamic addressing is employed, the MN typically does not have a home subnet and there is never a MN available to respond to ARP requests in the absence of a current CoA binding in the HoA, maintained by the MN.

Additionally, in mobility systems, the MN may be absent from the system for a number of reasons. The MN could be switched off, unreachable in a disconnected part of the Internet fabric (a private domain), it could be in various forms of power-saving sleep states, or could simply not wish to be reachable on a specific HoA (privacy, on-leave etc). Therefore, when the MN is absent and not maintaining its CoA binding, incoming packets for that HoA will simply be dropped on the local subnet.

## SUMMARY OF INVENTION(S)

The methods and apparatus of the present invention allow a server, referred to as a proxy MN server, to act as a proxy for an MN with regard to one or more active applications when the MN is unavailable, e.g., in sleep mode, otherwise absent, or unreachable. Thus, applications which might time out due to a lack of signals from an MN may be maintained even while the MN is absent. This allows the MN to continue interacting with an application when it returns, e.g., awakens from a sleep mode of operation.

One feature of the invention is to provide an additional layer of processing in an HA to enable the HA and a proxy MN server of the invention to process incoming packets for HoAs that do not have a currently maintained binding by the MN. In known processing the HA stops issuing proxy ARPs for the HoA when the CoA binding from the MN ceases, and signals this by issuing a gratuitous ARP on the home subnet for the HoA. If the MN is absent from the subnet then any incoming packets towards the HoA will be lost in the known systems. To avoid this unfortunate result we define a proxy MN server that reacts to hearing the HA gratuitous ARP (that cancels the ARP binding between the HA and the HoA), by itself issuing gratuitous ARPs to redirect HoA addressed packets to itself. In some embodiments, the proxy MN server of the present invention does this in cases where the MN can not itself be on the home subnet and not in other cases thereby avoiding the situation of both the MN and the proxy MN server issuing competing gratuitous ARPs, and subsequent ARPs for the HoA. If they can both be on the home subnet at the same time, then various techniques can be used to resolve who is the receiver of the packets. These techniques can also be used to give the MN explicit control over when packets are forwarded to the proxy MN server.

1) Both the MN and the proxy MN server could, and in some embodiments does, issue gratuitous ARPs but with different priorities such that the MN will win if present on the subnet, causing the proxy server to cease proxy ARP whilst it sees ARPs from the MN.

2) Before the MN binding is lost in the HA, the MN could, and in some embodiments does, issue a signal to the proxy MN server explicitly requesting it to act on the MNs behalf wrt ARPs.

3) A HA could, and in some embodiments does, have a default CoA installed for the MN such that whilst the MN has no active binding, packets are instead forwarded to the default CoA which points to the location of the proxy MN server. This has the additional benefit of explicitly removing the ARP context between the MN and the proxy MN server, and enables the proxy MN server to be located off the home subnet, on any foreign subnet, and specifically behind a firewall in the operator web-farm and/or operations centre.

4) The MIP could, and in some embodiments does, also use a MIP hand-off to specifically inform the HA to install a long lifetime binding that points to the default CoA which is either a CCoA of the proxy MN server, or a FA CoA of a router in front of the proxy MN server, whilst the MN is away. The MIP signalling looks like a forward (proactive) hand-off towards the

proxy MN server CoA and has the advantage of giving the MN specific feedback from the HA (MIP Reply) and the proxy MN server (via BU/Buack) about the progress of the hand-off. Alternatively, the MN can request that the MNPS issues a reactive hand-off to transfer forwarding towards the MNPS CoA in the HA, a binding which is maintained by the MNPS. In addition, the MN can transfer layer 2 and IP layer state to the proxy MN server using Context transfer mechanisms to assist that server in processing the incoming traffic, and to act as a storage point for MN state. Application state can also be sent between the MN and the MNPS.

Reviewing the forwarding rules, for the above, the HA first forwards to the current MN managed binding and next to any binding managed by the MNPS. Failing that, it forwards to any default CoA for the MN. Failing that, the HA issues a gratuitous ARP to release the ARP binding and the proxy MN server issues a gratuitous ARP to claim the packets for that MN. If the MN is also on the home subnet then the ARP from the MN over-rules the ARP from the proxy MN server and also suppresses the proxy MN server using a suppression timer (similar concept to that in IGMP).

When the MN wishes to reclaim forwarding from the proxy MN server, it can either issue a gratuitous ARP on the home subnet, or install a binding into the HA to cancel the default CoA, or request the MNPS to release its binding and redirect forwarding the MN. Note that it should also be possible for the MN to be able to issue a 'cancel all bindings message' to the HA to cause the HA to stop forwarding to the proxy MN server, when the MN is able to also install forwarding to the default CoA (i.e., when it is not a true default, but a signalled optional CoA). For all CoAs, a filter can be installed into the HA so that only a subset of packets are redirected to the MNPS rather than all packets, such that remaining packets are then delivered to the MN.

Packets for the MN are forwarded to the proxy MN server in the absence of the MN where various applications can be deployed of benefit to the operator and the MN. These applications include, for example:

1) Fault management. Packets arriving at a HA with no current CoA binding from the MN indicates a potential error in the system. Rather than simply dropping and losing the packet, forwarding them to the proxy MN server enables a record of the packet headers to be taken so that they can be correlated with other records to identify what went wrong in the system.

2) Paging. Whilst the MN is sleeping, incoming packets are forwarded to the proxy MN server where a paging classifier is interrogated and a decision is made as to whether or not to page the MN given the packet details, e.g., data contents. The paging system can then be used to locate the MN. Once located and contacted by the paging system the proxy MN server hands-off to the MN which appears to the system in terms of MIP signalling as if the MN actually moved from the proxy to the present FA. During this hand-off, the BU from the MN can be used to cause forwarding of packets at the proxy MN server through to the MN, and Context transfer can be used to transfer locally stored MN state, e.g., current application and MN related communication information, from the proxy MN server back to the FA and the MN so that the MNs state accurately reflects the status at the point the proxy MN server transferred application responsibility back to the MN.

3) Application proxies. The proxy MN server can be statically configured, or dynamically programmed by the MN, with information about application processing that the proxy can undertake for the MN whilst it is away. This is useful for a number of reasons. Firstly, a number of Internet applications issue keep-alives and need responses from the MN to remain active. The MN would therefore have the choice of either being prevented from moving into power efficient sleep state for longer than the keep-alive timers, or it would have to lose application liveness. The proxy MN server eliminates this problem because it can instead act on the MNs behalf in a controlled manner, to respond to selected keep-alives whilst the MN is sleeping (for IPSEC, VPN apps, mail servers, the MIP default CoA registration, SIP servers, streaming servers, multicast group memberships etc). Secondly, the MN can order processes to complete e.g., via interaction with the proxy MN server, whilst it is sleeping/missing. Such processes include content distribution (web-pages, files, video streams, software etc), mail uploads and downloads and in fact any application flow that could be more quickly routed through the proxy than directed to or from the MN, or that enables the MN to sleep and hence download content using bursty airlink opportunities. The proxy MN server could then optionally page the MN to inform it that the process has completed. The MN can then wake-up and rapidly download the content from the proxy or receive the delivery notification confirmation. For such application control, the proxy MN server may utilize an application proxy for each such application (web caches and content distribution mechanisms already exist) and signalling systems to control what processes those proxies keep-alive and/or complete in its absence, and the action to undertake when the

process terminates (or keep-alive fails). Exemplary actions include paging the MN, store and forward, store until the MN wakes up and triggers the queries the application proxy cache. A range of other triggers and applications activities can be imagined within this general framework.

The MNPS will generally need to have a security association with the MN, and with the peer systems of the MN to be able to secure the MIP signalling and the signalling packet flows with peers of the MN as described in this invention.

Numerous additional features, benefits and exemplary embodiments are described in the detailed description which follows.

## DESCRIPTION OF THE FIGURES

Fig. 1 illustrates an exemplary access node implemented in accordance with the present invention.

Fig. 2 illustrates an exemplary end node implemented in accordance with the present invention.

Fig. 3 illustrates an exemplary home mobility agent node implemented in accordance with the present invention.

Fig. 4 illustrates the exemplary contents of visitor list state which is exemplary of state that may be included in the visitor list state shown in any one of figs 1, 2 and 3.

Fig. 5 illustrates a network diagram of an exemplary communications system in which the invention is applicable.

Fig. 6 illustrates exemplary signalling and packet flows for the network of figure 5.

Fig. 7 illustrates a second exemplary signalling and packet flows for the network of figure 5.

Fig. 8 illustrates another exemplary signalling and packet flows for the network of figure 5.

Fig. 9 illustrates a network diagram for an alternative exemplary communications system in which the invention is applicable, along with exemplary signalling and packets flows associated with said network.

## DETAILED DESCRIPTION

Fig. 1 illustrates an exemplary access node 12, e.g., access router or base station, implemented in accordance with the invention. The access node 12 includes antennas 203, 205 and corresponding receiver, transmitter circuitry 202, 204, respectively. The receiver circuitry 202 includes a decoder 233 while the transmitter circuitry 204 includes an encoder 235. The circuitry 202, 204 is coupled by a bus 230 to an I/O interface 208, a processor (e.g., CPU) 206 and memory 210. The I/O interface 208 couples the access mode 12, e.g., base station, to the Internet. The memory 210 includes routines, which when executed by the processor 206, cause the access node 12 to operate in accordance with the invention. Memory includes communications routines 223 used for controlling the access node 12 to perform various communications operations and implement various communications protocols. The memory 210 also includes an access node control routine 225 used to control the access node's 12, e.g. base station's, operation and signaling to implement the steps of the method of the present invention. The access node control routine 225 includes a scheduler module 222 used to control transmission scheduling and/or communication resource allocation. Thus, module 222 may serve as a scheduler. The memory 210 also includes a mobility agent module 226 used to process and send mobility related signaling implementing the steps of the method of the present invention. Thus, module 226 may serve as a Mobile IPv4 Foreign Agent or a Mobile IPv6 Attendant. Memory 210 also includes information 212 used by communications routines 223, control routine 225 and mobility agent module 226. The information 212 includes an entry 213, 213' for each active end node (EN1, ENn, respectively), which includes the context state 243, 243' at the access node associated with each end node (EN1, ENn), said context state being passed between access nodes during hand-off of the end node, and including such information as the end node profile, security associations, and end node multicast membership. Entry 213,213' also includes MIP visitor list state 214, 214' associated with said end node (EN1, ENn), respectively, at that access node. In particular, information for end node 1 213 includes context state 243 for end node 1 213, and includes MIP visitor list state 214, shown in detail in Fig. 4.

Figure 2 illustrates an exemplary end node 14 implemented in accordance with the present invention. The end node 14 may be used by a user as a mobile terminal (MT) or the end node can act as the Mobile Node proxy Server (MNPS) for a mobile terminal (MT). The end node 14 includes receiver and transmitter antennas 303, 305 which are coupled to receiver and transmitter circuitry 302, 304 respectively, when the end node is connected to the access node 12 via a wireless link. The receiver circuitry 302 includes a decoder 333 while the transmitter circuitry 304 includes an encoder 335. The receiver transmitter circuits 302, 304 are coupled by a bus 330 to a memory 310, a processor 306, and an I/O interface 308. When the end node 14 is connected to the access node via a fixed link then the I/O interface 308 is employed. Processor 306, under control of one or more routines stored in memory 310, causes the end node 14 to operate in accordance with the methods of the present invention. In order to control operation of the end node 14, memory 310 includes communications routine 323 and end node control routine 325. The end node communications routine 323 is used for controlling the end node 14 to perform various communications operations and implement various communications protocols. The end node control routine 325 is responsible for insuring that the end node operates in accordance with the methods of the present invention and performs the steps described in regard to end node operations and signaling. Memory 310 also includes a MNPS control routine 326. The MNPS control routine 326 is responsible for insuring that the end node operates in accordance with the methods of the present invention and performs the steps described in regard to MNPS operations and signaling. The memory 310 also includes user/device/application/session /resource information 312 which may be accessed and used to implement the methods of the present invention and/or data structures used to implement the invention. In particular, User/Device/Application/Session/Resource information 312 includes MIP visitor state information 313 described in detail in Fig. 4. Information 312 also includes MNPS state 314 that includes addresses of the MNPS when the end node is a MT, or a home address of the MT when the end node 14 is a MNPS, associated security association for securing signaling between the MT and its MNPS, and state indicating whether the MT or the MNPS is presently receiving/sending packets from/to the home address of the end node 14. Information 312 also includes application state 315 that describes the intended behavior of the application software on the MT 14 and the MNPS 14, the application state that is sent from the MT 14 to the

MNPS 14, and the classifier information that is sent to a home agent that describes which packet flows are directed to the MT 14 and which flows are sent to the MNPS 14 for the MT 14.

Fig. 3 illustrates an exemplary home mobility agent node 15 implemented in accordance with the invention. The home mobility agent node 15 includes a bus 430 that couples together an I/O interface 408, a processor (e.g., CPU) 406 and memory 410. The I/O interface 408 couples the home mobility agent node 15 to the Internet. The memory 410 includes routines, which when executed by the processor 406, cause the home mobility agent node 15 to operate in accordance with the invention. Memory 410 includes communications routines 423 used for controlling the mobility agent node 15 to perform various communications operations and implement various communications protocols. The memory 410 also includes a mobility agent control routine 425 used to control the mobility agent node's 15 operation and signaling to implement the steps of the method of the present invention. The mobility agent node control routine 425 includes a scheduler module 422 used to control transmission scheduling and/or communication resource allocation. Thus, module 422 may serve as a scheduler. The memory 410 also includes a mobility agent module 426 used to process and send mobility related signaling implementing the steps of the method of the present invention. Thus, module 426 may serve as a Mobile IP Home Agent. Memory 410 also includes information 412 used by communications routines 423, control routine 425 and mobility agent module 426. The information 412 includes an entry 413, 413' for each active end node (EN1, ENn), respectively. In particular, information for end node 1 413 includes visitor list state 414, shown in detail in Fig. 4. Information about end node N 413' includes visitor list state 414' also shown in detail in Fig. 4

Fig. 4 illustrates example visitor list state 100, associated with a given mobility agent such as an end node 14, access node (foreign agent) 12, or a home mobility agent node (home agent) 15, implementing list state 313 in Fig. 2, the visitor list state 214, 214' in Fig. 1, and visitor list state 414,414' in Fig. 3, respectively. From the perspective of the access node 12 and the end node 14 of Figs. 1 and 2 respectively visitor list state 100 may include a number of state entries 110, 120.

According to this invention Visitor state 100 includes entries for at least one MN 14, each entry including state for a MN home address (HoA) 112, a Home Agent (HA) address 115, a Care of Address (CoA) 116, a binding lifetime 113, MIP signaling flags 117 and MIP security state associations 114 applicable to that mobility agent. When the mobility agent is a home mobility agent then the visitor list state information 100 further includes default CoA state information 110 including the default CoA 118 for an end node 1, e.g., mobile node (MN) or mobile terminal (MT), to be employed by the home agent 15 when the visitor list does not have a valid CoA 116 for the home address 112. Default CoA state information 110 also includes MIP Control State 119 used in the operation of MIP signaling and forwarding between the end node 14 and the home agent node 15. Additionally, when the mobility agent is a home mobility agent then the visitor list state information 100 includes MNPS CoA State information 120 for a home address 112 to be employed by the home agent node 15 when the visitor list is maintained by the corresponding MNPS of a end node 1, rather than the end node 1, e.g. MT, itself. MNPS CoA state 120 includes the MNPS CoA 127 that is employed instead of the default CoA 118 or the end node 1 CoA 116 when the MNPS is issuing MIP registrations to the home agent node 15. State 120 further includes MIP security state 128 to secure such registrations at the home agent, and MIP control state 129 used for the operation of MIP signaling and forwarding between the MNPS 14 and the home agent 15.

Fig. 5 illustrates an exemplary system 500 comprising a plurality of access nodes 505, 505', 505'' implemented in accordance with the present invention. Fig. 5 also depicts communication cells 501, 501', surrounding each access node 505, 505', respectively, which represents the coverage area of the radio technology employed by corresponding access node 505, 505', respectively with end nodes. Access node 505'' in contrast employs fixed links to end nodes and hence does not employ a communications cell but is otherwise part of the network. The same physical and functional elements are otherwise depicted in each of the communication cells 501, 501', and the network thus the following description of the elements in the cell 501 surrounding access node 505 is directly applicable to each of the cells 501, 501', and the network portion containing the access node 505''. The depiction of the access node 505 is a simplified representation of the access node 12 depicted in Fig. 1. For simplicity access node 505 is shown to include a mobility agent module 507 responsible for the signaling implementing this present invention. Fig. 5 illustrates the access node 505 providing connectivity to a plurality of N end nodes 502, 504 (End Node (MT) 1, End Node (MT) N (X)), via corresponding access link 506, 508, respectively. End nodes 502, 504 are simplified versions of the end node 14 depicted in Fig2.

Interconnectivity between the access nodes 505, 505', 505'' is provided through network links 510, 511, 512 and an intermediate network node 520. Home network 530 in Fig. 5 is connected to the rest of the system via link 522 and node 520. Home Network 530 further includes network node 536 also connected to link 522 and mobility agent node 532, connected to node 536 via link 538 and operating as mobility agent of at least end node N 504. Network 540 in Fig. 5 is connected to the rest of the system via link 523 and node 520. Network 540 further includes network node 546 also connected to link 523 and a correspondence node (CN) 542, connected to node 546 via link 548 and operating as corresponding node in a data session with at least end node N 504 for illustration of the methods of this present invention. Access Node 505 is considered to support mobile terminals (MTs) in the communications network 500 providing wireless communications, e.g., via links (506, 508) with end nodes (end node (MT) 1 502, end node (MT) N (X) 504). Similarly, access node 505' is considered to support MTs in the communications network 500 providing wireless communications, e.g., via links (506', 508') with end nodes (end node (MT) 1 502', end node (MT) N 504'). In contrast, the access node 505'' is considered to support fixed links to end nodes that are MNPSs which further support the end nodes that are MTs in the communications system 500. Access node 505'' is shown to be coupled via fixed links (506'', 508'') to end nodes (end node (MNPS) 1 502'', end node (MNPS) N (Y) 504''), respectively.

Figures 6-8 illustrate example embodiments of the various methods of this present invention. Figs. 6-8 are simplified versions of the system Fig. 5 including elements as required to further explain this present invention. Fig. 6 shows access nodes 505, 505'', including mobility agent modules 507, 507'', respectively, providing access to MT end node X 504, and MNPS end node Y 504'' that provides functionality to the MT end node X 504. Fig. 6 also shows home mobility agent node 532 serving end node (MT) X 504 and a CN node 542 being in a communication session with said end node (MT) X 504. In Fig. 6 solid thin arrows depict inner data traffic and the direction of the arrow points to the destination of said data traffic; thick solid lines depict encapsulated inner data traffic and the direction of the arrow points to the destination of said tunnel; dashed lines depict signaling messages used for the registration of an end node to the foreign mobility agent 507 and the home mobility agent 532, and the direction of the arrow points to the destination of said signaling. Dashed lines are also used for other types of signaling associated with MIP hand-off and with controlling the MNPS functionality.

Fig. 6 shows the packet forwarding and signaling for an exemplary example of the invention in operation in network 500. The dashed arrows indicate signaling messages and the solid arrows are packet flows. The thin solid arrows are inner packets whilst the thick arrows are encapsulated inner packets using an outer header. In fig 6, end node (MT) X 504 is initially receiving packets from the CN 542 as packet flow 616 to the home mobility agent node 532, which tunnels these packets to the access node 505 as packet flow 610, and then the foreign agent 507 in the access node 505 then decapsulates the packets 610 and forwards them as packets 617 to the end node (MT) X 504. When the end node (MT) X 504 wishes to invoke the MNPS functionality of the invention, then the end node (MT) X 504 sends registration request signals 601, 602 towards the home mobility agent 532, via the foreign agent 507 and receives the registration reply via messages 603 and 604. The registration message 601 includes the home address of the end node (MT) X 504, the address of the mobility agent node 532, the address of the access node 505, the end node X CoA field for the home address of the end node (MT) X 504, and the requested lifetime of the registration. The registration message is intended to cancel the binding between the home address and the CoA of the end node (MT) X 504 in the foreign and home agents 507,532. To achieve this, without loss of generality, the CoA may be set equal to the home address and/or the lifetime is set to zero or a very short time value. When the dynamic binding between the home address and dynamic CoA is cancelled or replaced by the end node (MT) X 504 in the home agent 532, then the home agent replaces the dynamic CoA entry with the default CoA entry in the binding. The default CoA is either preconfigured into the home agent via a management process, can be delivered in the MN profile from a policy server, or can be dynamically configured by the end node (MT) X 504 by including a default CoA in this or a previous registration message. The default CoA is permanent and is only removed from the home agent mobility node 532 when the default CoA functionality is no longer applicable such as when the home address is no longer allocated to end node (MT) X 504. The home agent 532 then tunnels packets that arrive for the home address of end node (MT) X 504 to the default CoA of end node (MNPS) Y 504'' rather than to the dynamic CoA of the end node (MT) X 504. The default CoA in figure 6 is the address of the agent node 505'' to which the end node (MNPS) Y 504''is connected. End node (MNPS) Y 504'' is the MNPS of the end node (MT) X 504 such that packets addressed to the home address of the end node (MT) X 504 are now delivered to end node (MNPS) Y 504'' where the application proxy for that end node (MT) X 504 is located. The forwarding at the access node 505'' is preconfigured with a binding between the home address of the end node (MT) X 504 and the end node (MNPS) Y 504'' so that the access node 505'' can decapsulate the packets from the home agent 532 and forward them as packets 617'' to the end node (MNPS) Y 504''. The end node (MNPS) Y 504'' becomes the network end point for packets 617 addressed to the home address of the end node (MT) X 504 whilst the default CoA is active at the home agent 532.

In a further embodiment, the home mobility agent node 532, foreign mobility agent 507'', end node (MNPS) Y 504'' or any intermediate node that is on the path of the packet flow between the home agent 532 and the end node (MNPS) Y 504'', can act as a Network translator and convert the destination address of the packets in the packet flow from the home address of the end node (MT) X 504 to the interface address of the end node (MNPS) Y 504'' so that the end node (MNPS) Y 504'' application proxy can avoid re-using the home address of the end node (MT) X 504 as a network address.

These features of the invention enable an end node (MT) X 504 to redirect its packets to an end node (MNPS) Y 504'' under the control of the end node (MT) X 504 and its home agent 532.

The end node (MNPS) Y 504'' receives the packets 617'' and undertakes the processing of the packets and the application data within the packets, as if it was the end node (MT) X 504. The end node (MNPS) Y 504'' has an interface that matches the destination address of packets 617'' and passes the application data contained in the packets to the application software in the application proxy that is configured to process said packet data. The processing of the packet data is controlled by application proxy configuration state which enables the MNPS at end node Y (MNPS) 504'' to provide services on behalf of the MN in the end node (MT) X 504 to CN 542. These services include the ability to generate application data, create packets and send said packets to the CN 542 as part of the ongoing communications session, or to any other end node including the end node (MT) X 504. In addition, the application proxy is able to send and receive signaling data in signaling packets that can be used to create, maintain and terminate communications sessions with CNs.

Signaling or application data packets generated by the end node (MNPS) Y 504'', on behalf of the end node (MT) X 504, as part of the session with the CN 542, are typically returned to the CN 542 using the reverse path and associated processing through the foreign agent 507'' and Home agent 532. Where alternative nodes other than the home agent 532 have the dynamic CoA state, such as is the case with the CN 542 when employing Mobile IP Route optimization (http://www.ietf.org/proceedings/99nov/I-D/draft-ietf-mobileip-optim-08.txt), then the CN 542 may additionally have the default CoA state described in this invention.

In a further embodiment of the invention, the home agent 532 can have a filter associated with the default CoA for a home address of an end node (MT) X 504 that identifies a specific subset of packets addressed to that home address that are to be forwarded to the default CoA when a dynamic CoA is not active. The application proxy at the end node (MNPS) Y 504'' therefore only needs to be able to provide applications services for said subset of packets rather than for all possible applications employed by the end node (MT) X 504. The filter can be configured or delivered using any of the methods employed for the default CoA. Similarly, the application proxy configuration can include filters that limit the type of applications packets can be emitted by the application proxy from the source address of the end node (MT) X 504, or any associated source address that is translated into the home address of the end node (MT) X 504. Further, a filter can alternatively be installed into the foreign agent 507'' to police packet flows in either direction between the CN 542 and the end node (MNPS) Y 504''.

In a further embodiment of the invention, the message 601 can include the address of the access node 505'' and an instruction to trigger message 624 and acknowledgment 622 which causes the context state associated with the end node (MT) X 504 at the access node 505 to be transferred to the access node 505'' so that the access node 505'' can police and provide services to the packet flow 617'' and the end node Y (MNPS) 504'', as is provided by the access node 505 to the end node (MT) X 504 and packets 617. Specific context state examples are the policy profile, the paging classifier, Multicast group membership and security associations needed by the access nodes 505, 505'' for the end node (MT) X 504. Alternatively, this context state can be preconfigured in the access node 505'' via a similar policy process such as AAA signaling that is used to deliver the context state to the access node 505, and the message 624 only used to carry incremental and/or temporary changes to that preconfigured state. Messages 624 and 622 can also be used to configure a tunnel 620 between access nodes 505 and 505'' so that in-flight packets towards the end node (MT) X 504 can also be directed to the end node (MNPS) Y 504''. The message 618'' is sent from the access node 505'' to the end node (MNPS) Y 504'', following message 622/624, to inform end node (MNPS) Y 504'' that it is now responsible for the packets to and from the home address of the end node (MT) X 504.

In advance of issuing messages 601 towards the foreign agent 505, the end node (MT) X 504 can issue message 634 to end node (MNPS) Y 504'' using the home address of the end node (MT) X 504 as a source address and the interface address of end node (MNPS) Y 504'' as the destination address. Message 634 generates a reply message 632. Message 634 is used to request that the end node (MNPS) Y 504'' become the end point for packets to and from the home address of the end node (MT) X 504, to which the end node (MNPS) Y 504'' responds with an acknowledgement message 632. Message 634 can include modifications to the application configuration at the application proxy in the end node (MNPS) 504'', such as application control or data state, as well the filter state which is used by the end node (MNPS) Y 504'' to select a subset of packet flows 617 for which the application proxy will process on behalf of the end node (MT) X 504. The reply message 632 can include the address of the access node 505'' to which the end node (MNPS) Y 504'' is connected so that the end node (MT) X 504 can include that address in message 601 to the access node 505 so that access node 505 knows the address of the access node 505'' for the context transfer as part of message 624. Alternatively, both the interface address of the end node (MNPS) Y 504'' and its access node 505'' can be known in advance at the end node (MT) X 504. Messages 632 and 634 need to be at least authenticated and integrity protected to avoid the hijacking of packet flows. The end nodes (MT) X 504 and (MNPS) Y 504'' therefore share a security association to secure messages between them, tied to the home address of end node (MT) X 504 and the interface address of end node (MNPS) Y 504''. T his security association can be pre-configured, provided by a policy server or dynamically generated. The end node (MT) X 504 must know its MNPS end node Y 504'' interface address in advance of sending message 634 but the end node (MNPS) Y 504'' can be dynamically informed of the home address for which it is to provide application proxy services via the contents of message 634.

When end node (MT) X 504 wishes to reclaim the packet flow from the end node (MNPS) Y 504'', then the end node (MT) X 504 sends and receives messages 601, 602, 603 and 604 to install into the home agent 532 and foreign agent 507 the dynamic CoA at its current access node 505, 505', which therefore overrules the default CoA at the home agent 532. In advance of this, the end node (MT) X 504 can send message 634 to end node (MNPS) Y 504'' to request back the packet flow and to terminate the application proxy in the end node (MNPS) Y 504''. The end node (MNPS) Y 504'' can then inform the end node (MT) X 504 in message 632 when it is ready (i.e., when application data is at an appropriate stage to transfer control), and can return any associated application control state or data back to the end node (MT) X 504 so that the end node (MT) X 504 can continue with the application processing. Messages 624 and 622 can also be triggered by message 601 at the access node 505 to this time install a tunnel 620'' back to the access node 505, for in-flight packets towards the access node 505'' for the end node (MNPS) Y 504'', creating the reverse of packet flow 620. Messages 624 and 622 can also recover the context state from access node 505'' including any changes that have occurred at access node 505'', back to access node 505. This enables the access node 505'' to act as a temporary storage point for the context state if the end node (MT) X 504 should leave access node 505 causing that access node to eliminate said context state associated with that end node (MT) X 504. Message 618'' is used to inform the end node (MNPS) Y 504'' that it is no longer responsible for the set of packets to and from the home address of the end node (MT) X 504.

Figure 7 shows an alternative embodiment of the invention that uses a MNPS CoA in the home agent 532 instead of the default CoA. This time it is the end node (MNPS) Y 504'' that sends the registration signals to the home agent 532 via the foreign agent 507'' as messages 601'' and 602'' which include the home address of end node (MT) X 504 and the CoA of the end node (MNPS) Y 504''. This results in reply messages 603'' and 604'' along with the update of the binding in the home agent 532 to redirect packets from tunnel 610 to tunnel 610''. The end node (MNPS) Y 504'' is then able to redirect packets addressed to the home address away from the end node (MT) X 504. The end node (MNPS) Y 504'' and foreign agent 507'' should share a security association with the home agent 532 to secure these messages to avoid redirection attacks from unauthorized nodes. Note that the registrations from end node (MNPS) Y 504'' do not eliminate the registration state issued by the end node (MT) X 504 itself, both of which are treated independently, but the registration state and specifically the CoA from the end node (MNPS) Y 504'' is prioritized above that of the end node (MT) X 504. This is so that the end node (MNPS) Y 504'' can safely redirect the packet flows of an end node (MT) X 504 when it is disconnected from the network or suffering a malfunction.

This time message 601'' triggers message 622 which has a reply message 624. These are once again used to install temporary packet forwarding 620 between the access node 505 and the access node 505'' and to fetch the context state from the access node 505. Similarly, messages 601'', 602'', 603'', 604'', 622 and 624 are used to redirect packet flow back to the end node (MT) X 504, and its access node 505, by canceling the MNPS CoA in the home agent 532, when the end node (MNPS) Y 504'' no longer wishes to receive packets for the home address of end node (MT) X 504. Message 618 is used to inform the end node (MT) X 504, as a result of messages 622, 624 whether or not it is presently responsible for packets to its home address. The end node (MT) X 504 can trigger the end node (MNPS) Y 504'' to send message 601'', to either take or release the redirection of the packets, by first sending message 634 to the end node (MNPS) Y 504'' which again responds with message 632. Other nodes such as the access node 505, CN 542 or home agent 532 can alternatively trigger the end node (MNPS) Y 504'' to issue message 601'' using messages similar to message 634.

Figure 8 is the same as figure 6 apart from the fact that the MNPS CoA of end node (MNPS) Y 504'' is this time a Co-located CoA which is equal to the interface address of end node (MNPS) Y 504''. Redirected packet flow 611' is therefore now a tunnel directly between the home agent 532 and the end node (MNPS) Y 504'', which avoids the need for the access node 505'' needing a foreign agent function 507''. In addition, in-flight packets 620 can be sent directly to the CCoA of the end node (MNPS) Y 504'' rather than via the access node 505''. However, if it is the end node (MNPS) Y 504'' that issues the message 601'' as in Figure 7, rather than the end node (MT) X 504 as in Figure 6, and that registration should be sent via the access node 505'' or in-flight packets 620 are still sent to the access node 505, then the foreign agent 507'' is still required.

Figure 9 shows an alternative embodiment of the default CoA functionality in the special case that the end node (MNPS) Y 504'' is on the same mac_layer network as the home agent 532, which is therefore also the home network 530' of the end node (MT) X 504. The Figure 9 shows the networking between the CN 542 and the network 530 components of figure 5. Figure 9 introduces links 508''' and 506''' which are used to connect end node (MT) X 504 and end node (MNPS) Y 504'' to the home agent 532. The nodes run a protocol which distributes the mapping between the mac_layer address of each interface and its associated IP address, such as in the case of Address Resolution Protocol (ARP) or Neighbour Discovery in IPv6 (ND). When the end node (MT) X 504 is not on the home network 530' but is connected to a foreign access node such as 505, and the end node (MT) X 504 has a dynamic CoA in the home agent 532, then the home agent will send a proxy ARP signal 902''' with a mapping between its mac_layer address and the home address of the end node X 504, to indicate that packets addressed to that home address should be forwarded to it by all nodes on the mac_layer network. The home agent 532 then tunnels these packets to the current registered dynamic CoA as shown by the large solid arrow. When however the end node X (MT) 504 is on the home network 530' then it will issue the ARP message 915''' onto the mac_layer network, containing its mac_layer address on link 508''', so that such packets 920''' are instead forwarded to it. This ARP message 915''' cancels the proxy ARP message 902''' from the home agent 532 to all other nodes on the mac_layer network. Note that the home agent will typically not send message 902'''.

In an exemplary embodiment of the invention, the end node (MNPS) Y 504'' can issue for example, without loss of generality, a proxy ARP message 905''' to redirect packets to the home address of the end node (MT) X 504, towards the end node (MNPS) Y 504'' creating packet flow 910'''. This reproduces the redirection functionality of the MNPS CoA in the limited case of the end node (MNPS) Y 504'' being on the home network. The proxy ARP messages: 902'''sent by the home agent 532, 915''' sent by end node(MT) X 504, and 905''' sent by end node (MNPS) Y 504'' can be strictly ordered using a priority flag in the ARP messages, or the last message can instead be considered the latest configuration and a system of message suppression using internal priorities used by the nodes to identify who is the present receiver of packets addressed to the home address of end node (MT) X 504. The default CoA capability can be reproduced in this special case by instead storing a default ARP binding in the home agent 532 which is activated when the end node (MT) X 504 is neither on the home network nor has a valid dynamic CoA registered in the home agent 532. The default ARP binding is then advertised by the home agent and identifies the mac_layer address of the end node (MNPS) Y 504'' rather than the mac layer address of the home agent 532.

Various alternative embodiments exist in the implementation of the invention. Firstly, the access node 505'' can contain the home agent 532 whilst still using default and MNPS CoA features. In addition, it is possible for there to be multiple MNPSs for each home address, with filters used to route packets to the correct MNPS functionality for each subset of the packet flows. One of said MNPSs can also be located in the same node as the home agent 532. In addition, the MNPS software can be located in the access node 505''. The invention can use Mobile IP v4 and/or v6 signaling and forwarding, including the various forwarding options including route optimisation. The various messages detailed in the invention can be used in various subsets and combinations as appropriate to the requirements of the application proxy in relation to the subset of packets being redirected from the end node (MT) X 504.

Some example application proxy features will now be described.

Firstly, the default CoA can be used to redirect all packets to an allocated home address, that does not have a registered dynamic CoA in the home agent 532, towards an application proxy that acts as an error-logger by simply capturing the packet headers.

Secondly, an extended IP paging system can be supported whereby the end node (MT) X 504 can go into sleep at the access node 505 and packets can be redirected to the access node 505'' where a paging classifier is contained in the context state of the end node (MT) X 504. The paging classifier can decide whether packets are dropped, forwarded to the MNPS or trigger a paging message to the present location of the end node (MT) X 504, said location being accessible by the access node 505''. Packets that are forwarded to the end node (MNPS) Y 504'' are processed in the MNPS and application events can then trigger message 601'' to return packet forwarding to the end node (MT) X 504 at its present location which is installed as the CoA in the home agent 532 using message 602''. Alternatively, the MNPS can simply send message 632 towards the end node X 504 which will be passed to the access node 505'' and will then trigger the paging function at that access node towards the present location of the end node (MT) X 504. The potential result of the paging function is the end node (MT) X 504 will wake up and wish to recover its packet reception and forwarding. It will therefore use message 601 to update the home agent with its present CoA, trigger 622/624 to recover its context state from the access node 505'' and use message 634 and 622 to recover its application state from the MNPS.

Whilst the end node (MT) X 504 is asleep, the MNPS can issue keep-alive packets for any applications and protocols at the CN that require such keep-alives to maintain a session. The message 634/632 exchange is used by the end node (MT) X 504, along with preconfigured application proxy state, to inform the MNPS of the sessions to be refreshed, the refresh interval, any security state used to secure the keep-alive signalling, the keep-alive peer and the response behaviour if the session terminates or if incoming data packets arrive on that session. This enables the end node X (MT) 504 to go into power efficient extended sleep but not loose connectivity to application servers and networking gateways.

In a third application of the invention, a content distribution system can be developed whereby the end-node (MT) X 504 can order delivery of a piece of content but direct its delivery to the MNPS in the end node (MNPS) Y 504'' using a filter in the home agent 532. The application proxy state in the MNPS can then direct a message to the end node (MT) X 504 when the content has been delivered in its entirety, or simply wait for the end node (MT) X 504 to query its delivery status. The end node (MT) X 504 or end node (MNPS) Y 504'' can then use the methods of the invention to direct packets back to the end node (MT) X 504 and then the end node (MNPS) Y 504'' can deliver the content to the end node (MT) X 504. This enables the end node X (MT) 504 to either go to sleep or use its bandwidth for other purposes whilst the content is delivered to end node (MNPS) Y 504'', and then request delivery when it best suits that end node (MT) X 504.

In an alternative, content distribution system, the end node (MNPS) Y 504'' can act as a content server for content from the end node (MT) X 504. The end node (MT) X 504 can then wake-up and efficiently deliver a content update to end node (MNPS) Y 504'' whilst using filters to direct content requests to the content server at the end node (MNPS) Y 504''. This avoids the end node (MT) X 504 from having to publish its content from either itself, or a fixed node, ensuring that the content is served locally. It also means that the server address is the same whether or not the end node (MT) X 504 or end node (MNPS) Y 504'' is actually serving the content, so enabling the end node (MT) X 504 to serve a subset of flows, some or all of the time as it so wishes. Messages 634/632 keep the end node applications in synch whilst messages 601, 602, 603, 604, 622, 624 and 618 manage the packet forwarding.

The present application hereby expressly incorporates the U.S. Provisional Patent Application listed in the Related Application section of this patent application. However, it is to be understood that any mandatory language such as, e.g., must, is required, and necessary, found the provisional application is to be interpreted as applying to the examples and embodiments described in the particular provisional application and in no way limits the scope of the claims or invention described in the text of this application which is not incorporated by reference.

In various embodiments nodes described herein are implemented using one or more modules to perform the steps corresponding to one or more methods of the present invention, for example, signal processing, message generation and/or transmission steps. Thus, in some embodiments various features of the present invention are implemented using modules. Such modules may be implemented using software, hardware or a combination of software and hardware. Many of the above described methods or method steps can be implemented using machine executable instructions, such as software, included in a machine readable medium such as a memory device, e.g., RAM, floppy disk, etc. to control a machine, e.g., general purpose computer with or without additional hardware, to implement all or portions of the above described methods, e.g., in one or more nodes. Accordingly, among other things, the present invention is directed to a machine-readable medium including machine executable instructions for causing a machine, e.g., processor and associated hardware, to perform one or more of the steps of the above-described method(s). The methods and apparatus of the present invention are applicable to a wide range of communications systems including many OFDM, CDMA and other non-OFDM systems.

The methods and apparatus of the present invention may be, and in various embodiments are, used with CDMA, orthogonal frequency division multiplexing (OFDM), and/or various other types of communications techniques which may be used to provide wireless communications links between access nodes and mobile nodes. In some embodiments the access nodes are implemented as base stations which establish communications links with mobile nodes using OFDM and/or CDMA. In various embodiments the mobile nodes are implemented as notebook computers, personal data assistants (PDAs), or other portable devices including receiver/transmitter circuits and logic and/or routines, for implementing the methods of the present invention.

Numerous additional variations on the methods and apparatus of the present invention described above will be apparent to those skilled in the art in view of the above description of the invention. Such variations are to be considered within the scope of the invention.

**WHAT IS CLAIMED IS:**

1. A communications method for use with a communications system including a first node having a first address, said first address being a home address of the first node, and including a prefix with a third node and a third address, said third address being assigned to that third node, and a second node that shares a prefix with a second address said second address being a Care of Address, the method comprising:

operating the third node to receive inner packets with the first address as a destination address and a fourth address, assigned to a fourth node, as a source address; the third node encapsulating said inner packets with an outer header having the third address as a source address and the second address as a destination address, a mapping between the first and second address being stored in a binding table in the third node;

operating the node that has been assigned the second address, this being one of the first or second nodes, to decapsulate the inner packet from the outer header and to forward the inner packet to the first node;

the system additionally comprising a fifth node that is connected to a sixth node, and a fifth address that shares a prefix with the sixth node; and

operating the third node to encapsulate and forward inner packets in an outer header containing the fifth address instead of the second address, and operating the node that is assigned the fifth address, this being either the fifth or sixth nodes, to decapsulate the inner packet from the outer header and forward the inner packet to the fifth node.

2. The communications method of claim 1 wherein the first node is a Mobile IP Mobile Node, the second node is an access node, the third node is an MIP Home Agent or a Regional Mobility Agent, the fourth node is a MIP Correspondent Node, the fifth node being a Mobile Node Poxy Server and the sixth node being another access node, said access nodes containing a Mobile IP mobility Agent when the access node is performing the decapsulation of the inner packet from the outer header.

3. The communications method of claim 1 wherein the third node uses the fifth address instead of the second address when the second address is not known.

4. The communications method of claim 2 wherein the third node uses the fifth address instead of the second address when the lifetime of the state containing the second address expires, said

fifth address being a default Care of Address.

5. The communications method of claim 2 wherein the third node uses the fifth address instead of the second address when an explicit signal is received from the first node or the fifth node.

6. The communications method of claim 1 wherein the third node, the fifth node, and the sixth node are on the same network such that they have direct mac-layer connectivity and wherein the fifth address is assigned to the fifth node and is equal to the first address, the method further comprising:

operating the fifth node to issue a first message that is received at the third node indicating a mapping between the mac-layer address of the fifth node and the fifth address at that fifth node;

operating the third node to stop encapsulating and forwarding the packets addressed to the first address to the second address; and

said packets addressed to the first address then being directed to the mac_address of the fifth node by all other nodes on the network.

7. The communications method of claim 6, wherein the first node is additionally on the same network;

operating said first node to issue a second message that is received at the third node and the fifth node indicating a mapping between the mac-layer address of the first node and the first address at that first node;

operating the fifth node to stop issuing the first message when it receives the second message; and

said packets addressed to the first address then being directed to the mac_address of the first node by all other nodes on the network.

8. The communications method of claim 1, further comprising;

operating the first node to send a third message to the third node to install the fifth address into the binding table in the third node as an alternative address to the second address.

9. The communications method of claim 1, further comprising;

operating the first node to send a fourth message to the third node to select as a tunnel address at the third node between the fifth address and the second address.

10. The communications method of claim 1, further comprising; operating the first node to send a fifth message to the fifth node to trigger it to activate the application proxy for the first node at the fifth node.

11. The communications method of claim 10, further comprising; operating the fifth node to send a sixth message to the third node to select the fifth address rather than the second address as the tunnel destination address so that packets originally intended for the first node will be received at the fifth node.

12. The communications method of claim 10, further comprising: operating the second node to send a seventh message to the first node to inform the first node that it is not the end point for the tunnelled packets from the third node.

13. The communications method of claim 10, further comprising: operating the sixth node to send a seventh message to the fifth node to inform the fifth node that it is the end point for the tunnelled packets from the third node.

14. The communications method of claim 10, further comprising: operating the first node to send application state to the fifth node to direct application software processing at the fifth node.

15. The communications method of claim 10, further comprising: operating the first node to send context state to the fifth or sixth nodes to provide the fifth or sixth nodes with network configuration state to support packet forwarding and secure policy controlled network signaling at the fifth and sixth nodes in support of the forwarding and processing of the inner packets that would otherwise be sent and received by the first node.

16. The communications method of claim 15, wherein context state includes at least one of the first address of the MN, the NAI of the MN, the security association between the first node and the third node, and the second address.

17. The communications method of claim 2, where said third node includes a classifier associated with the fifth and second addresses, said method further comprising:

operating the classifier to direct a subset of inner packets to be encapsulated with the fifth address and the remaining packets to be encapsulated with the second address.

18. The communications method of claim 2 further comprising;
maintaining a security association between the first node and the fifth node that secures signalling between the first and fifth nodes.

19. The communications method of claim 2 further comprising;
maintaining a security association between the second node and the sixth node that secures signaling between the second and sixth nodes.

20. The communications method of claim 2 further comprising;
maintaining a security association between the sixth node and the third node that secures signaling between the third and the sixth nodes.

21. The communications method of claim 9 further comprising;
operating the second node to send an eighth message to the sixth node triggered by the fourth message to install packet forwarding of in-flight packets at the second node, addressed to the first address towards the fifth or sixth nodes.

22. The communications method of claim 11 further comprising;
operating the sixth node to send an ninth message to the second node, triggered by the sixth message, to install packet forwarding of in-flight packets at the sixth node addressed to the first address, towards the first or second nodes.

23. A communications system comprising a fifth node, said fifth node comprising a network interface connected to a sixth node, said node receiving packets sent by a fourth node to a first node, said fifth node including an application proxy for at least one first node, said application proxy including a plurality of software applications, each software application having application state that directs the software applications to receive, process and send application data that is intended for the equivalent software applications on the first node;
operating said fifth node to receive inner packets from a peer node, originally addressed to the first address of the first node, to then pass the contents of the inner packets to an IP stack of the fifth node where the contents of the inner packet will be passed to the appropriate

software application in the application proxy associated with the destination address of the inner packet;

operating said software application in the fifth node to process the contents of the inner packet according to the application state; and

operating said software application to generate output application data within IP packets with a source and destination address that is equal to the destination address and source address received by the IP stack of the application proxy in the incoming inner packets from the peer, and sending said IP packet to the said peer node, said receiving processing and sending of IP packets creating a peer to peer communications session.

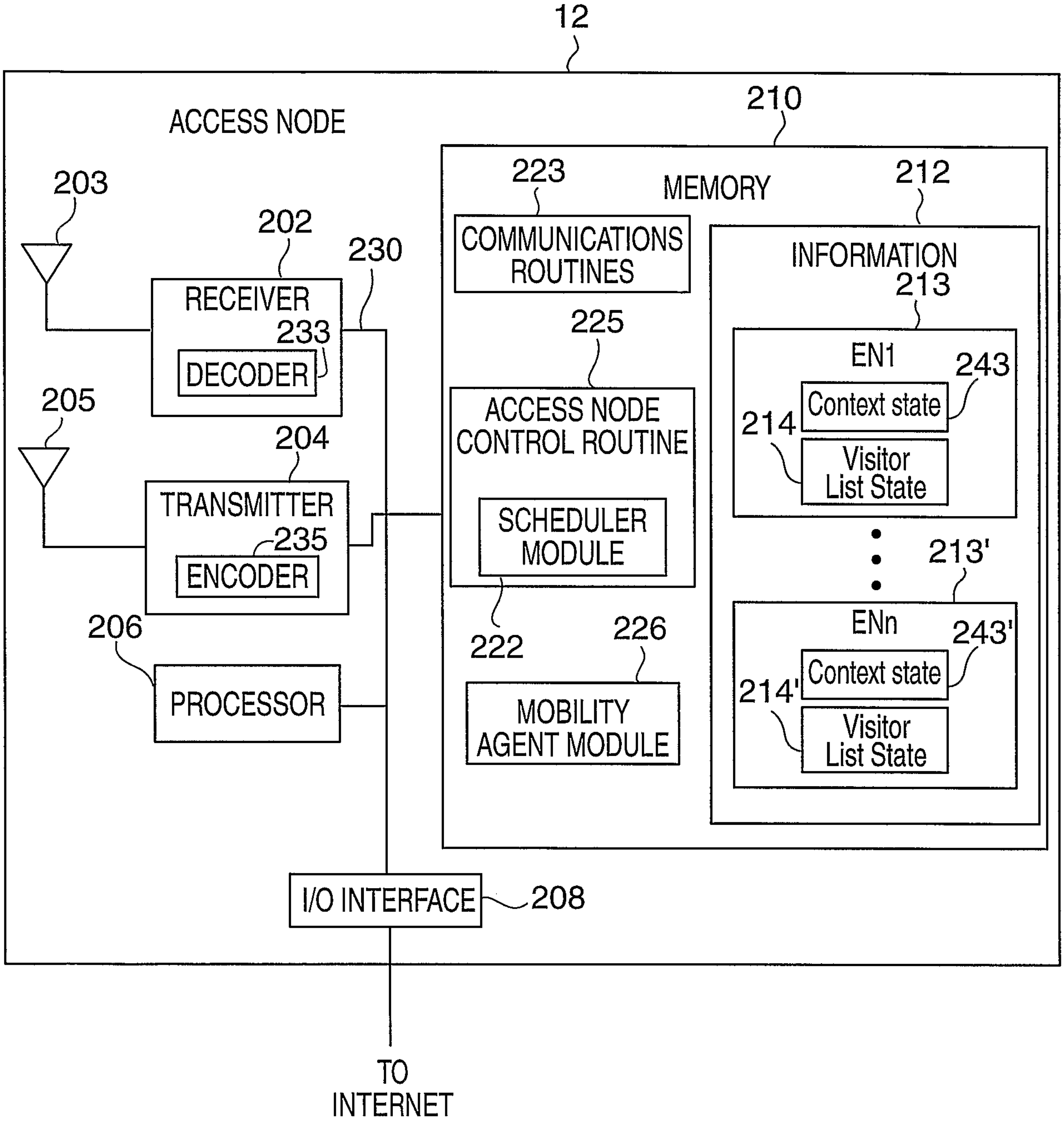

12
ACCESS NODE
210
MEMORY
203
202
RECEIVER
233
DECODER
230
205
204
TRANSMITTER
235
ENCODER
206
PROCESSOR
223
COMMUNICATIONS ROUTINES
225
ACCESS NODE CONTROL ROUTINE
SCHEDULER MODULE
222
226
MOBILITY AGENT MODULE
212
INFORMATION
213
EN1
243
Context state
214
Visitor List State
213'
ENn
243'
Context state
214'
Visitor List State
I/O INTERFACE
208
TO INTERNET

FIG. 1

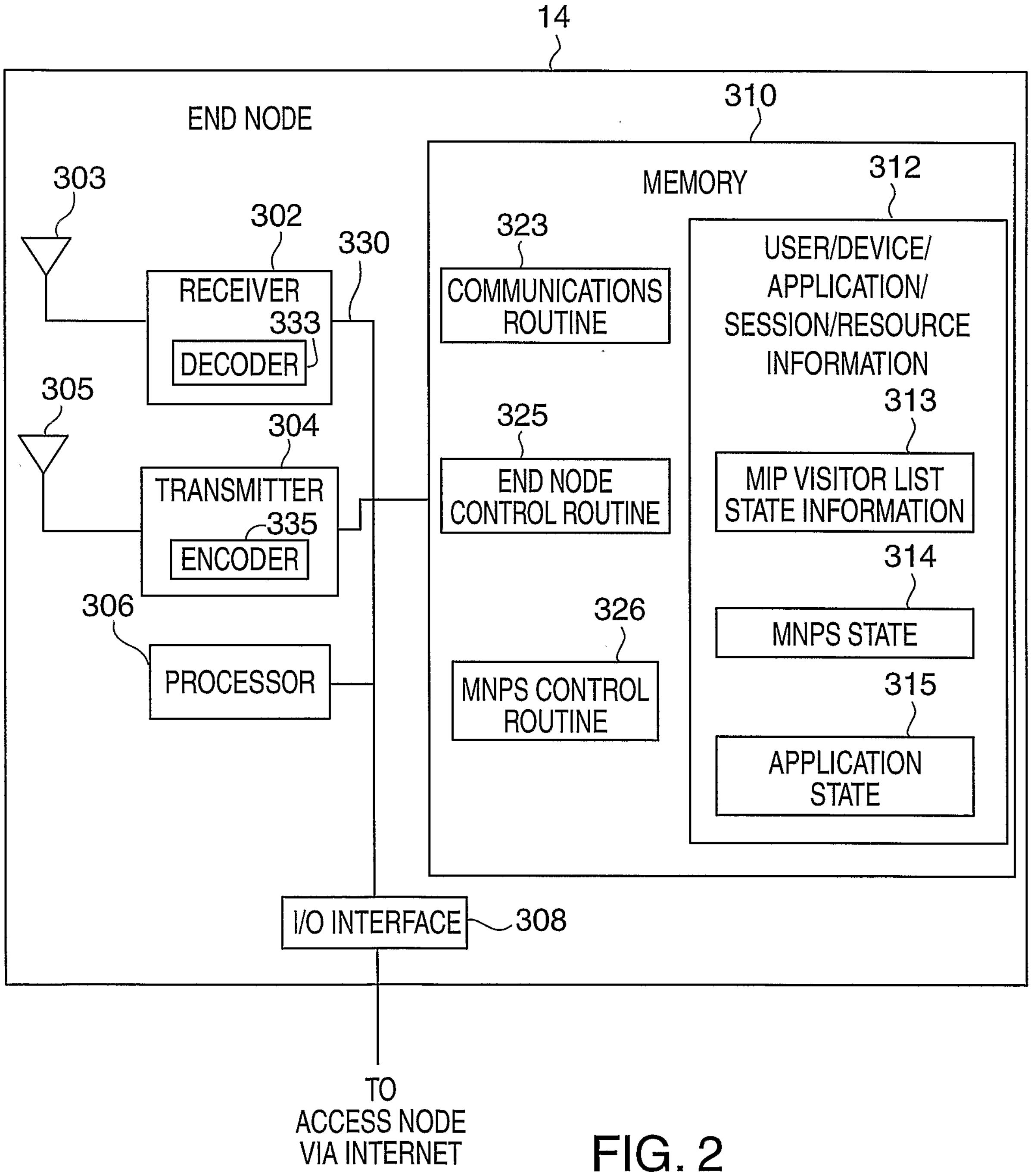

14
END NODE
303
302
RECEIVER
333
DECODER
330
305
304
TRANSMITTER
335
ENCODER
306
PROCESSOR
310
MEMORY
312
323
COMMUNICATIONS ROUTINE
325
END NODE CONTROL ROUTINE
326
MNPS CONTROL ROUTINE
USER/DEVICE/ APPLICATION/ SESSION/RESOURCE INFORMATION
313
MIP VISITOR LIST STATE INFORMATION
314
MNPS STATE
315
APPLICATION STATE
I/O INTERFACE
308
TO ACCESS NODE VIA INTERNET

FIG. 2

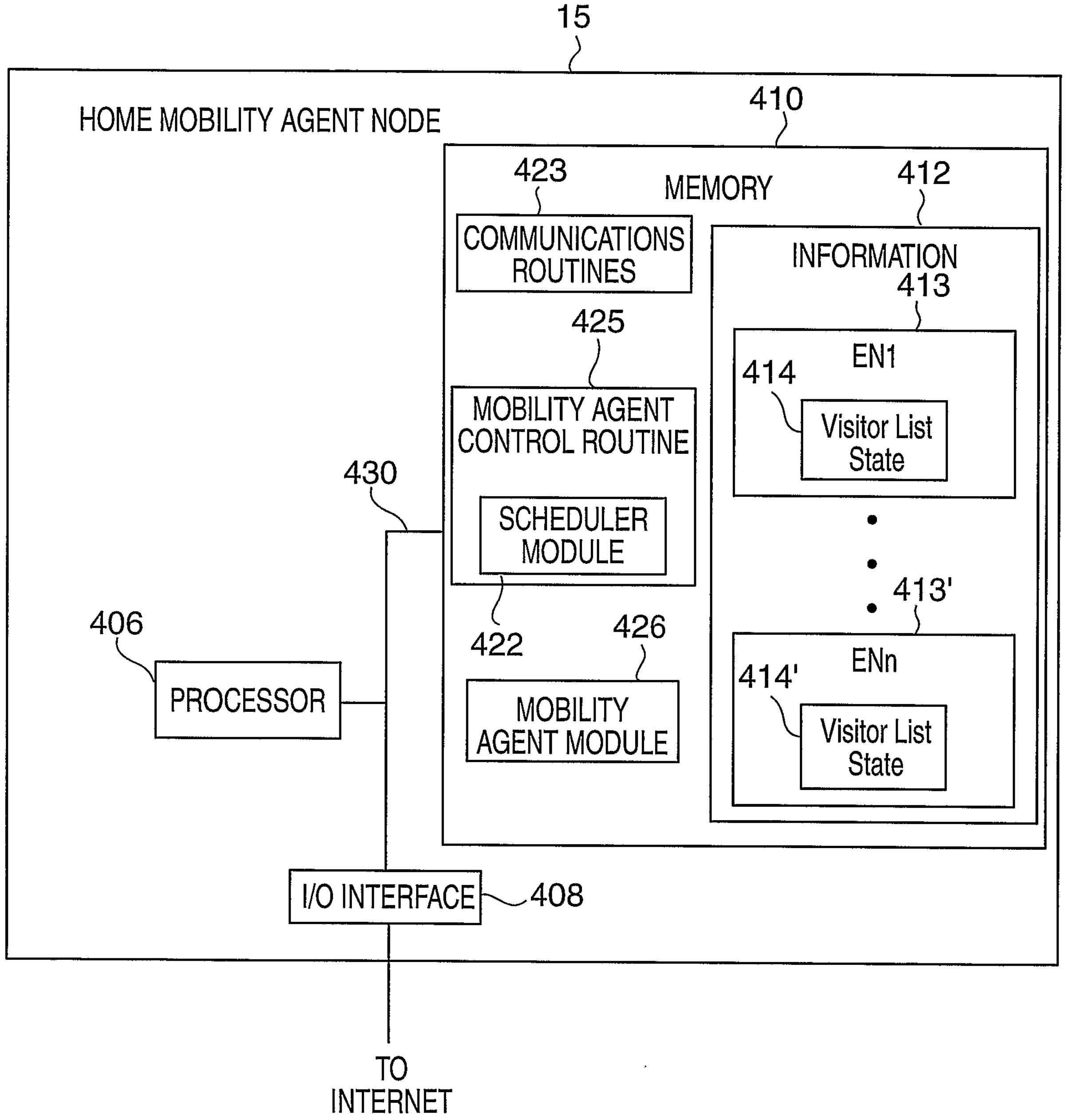

15
HOME MOBILITY AGENT NODE
410
MEMORY
423
COMMUNICATIONS ROUTINES
412
INFORMATION
413
EN1
414
Visitor List State
425
MOBILITY AGENT CONTROL ROUTINE
SCHEDULER MODULE
430
422
426
MOBILITY AGENT MODULE
413'
ENn
414'
Visitor List State
406
PROCESSOR
I/O INTERFACE
408
TO INTERNET

FIG. 3

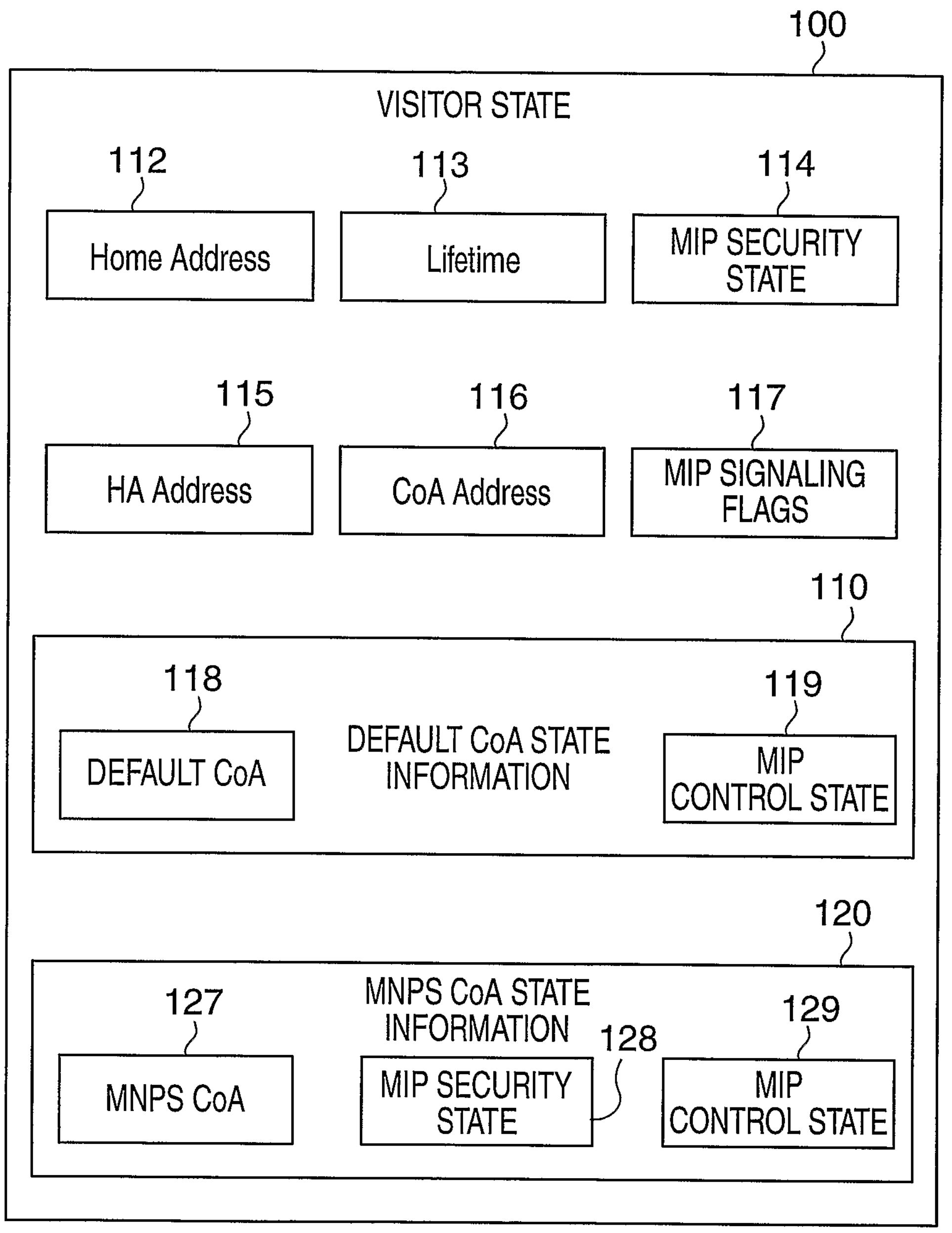

100
VISITOR STATE
112
Home Address
113
Lifetime
114
MIP SECURITY STATE
115
HA Address
116
CoA Address
117
MIP SIGNALING FLAGS
110
118
DEFAULT CoA
DEFAULT CoA STATE INFORMATION
119
MIP CONTROL STATE
120
127
MNPS CoA
MNPS CoA STATE INFORMATION
128
MIP SECURITY STATE
129
MIP CONTROL STATE

FIG. 4

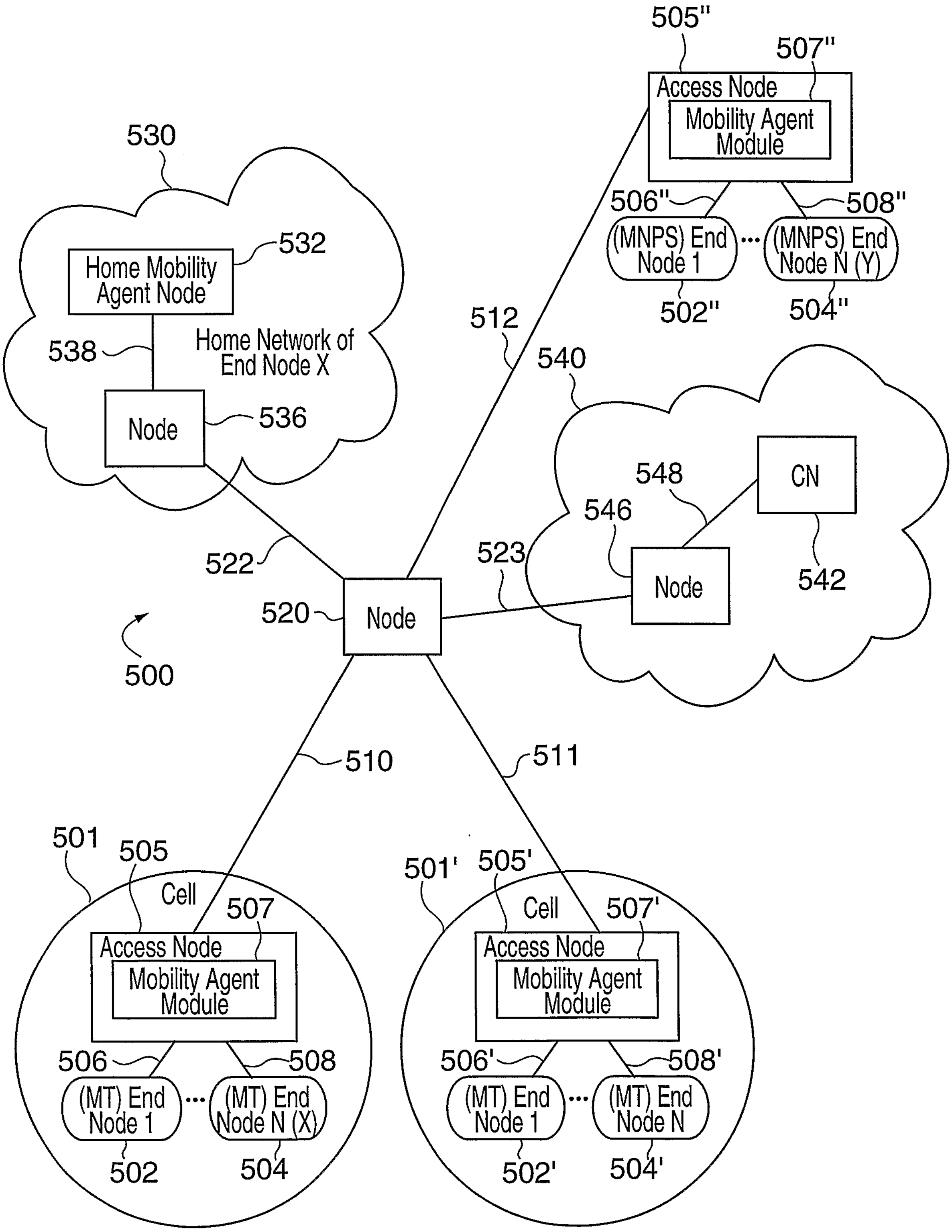

505''
507''
Access Node
Mobility Agent Module
506''
508''
(MNPS) End Node 1
(MNPS) End Node N (Y)
502''
504''
530
532
Home Mobility Agent Node
Home Network of End Node X
538
Node
536
512
540
548
CN
546
Node
542
523
522
520
Node
500
510
511
501
505
Cell
507
Access Node
Mobility Agent Module
506
508
(MT) End Node 1
(MT) End Node N (X)
502
504
501'
505'
Cell
507'
Access Node
Mobility Agent Module
506'
508'
(MT) End Node 1
(MT) End Node N
502'
504'

FIG. 5

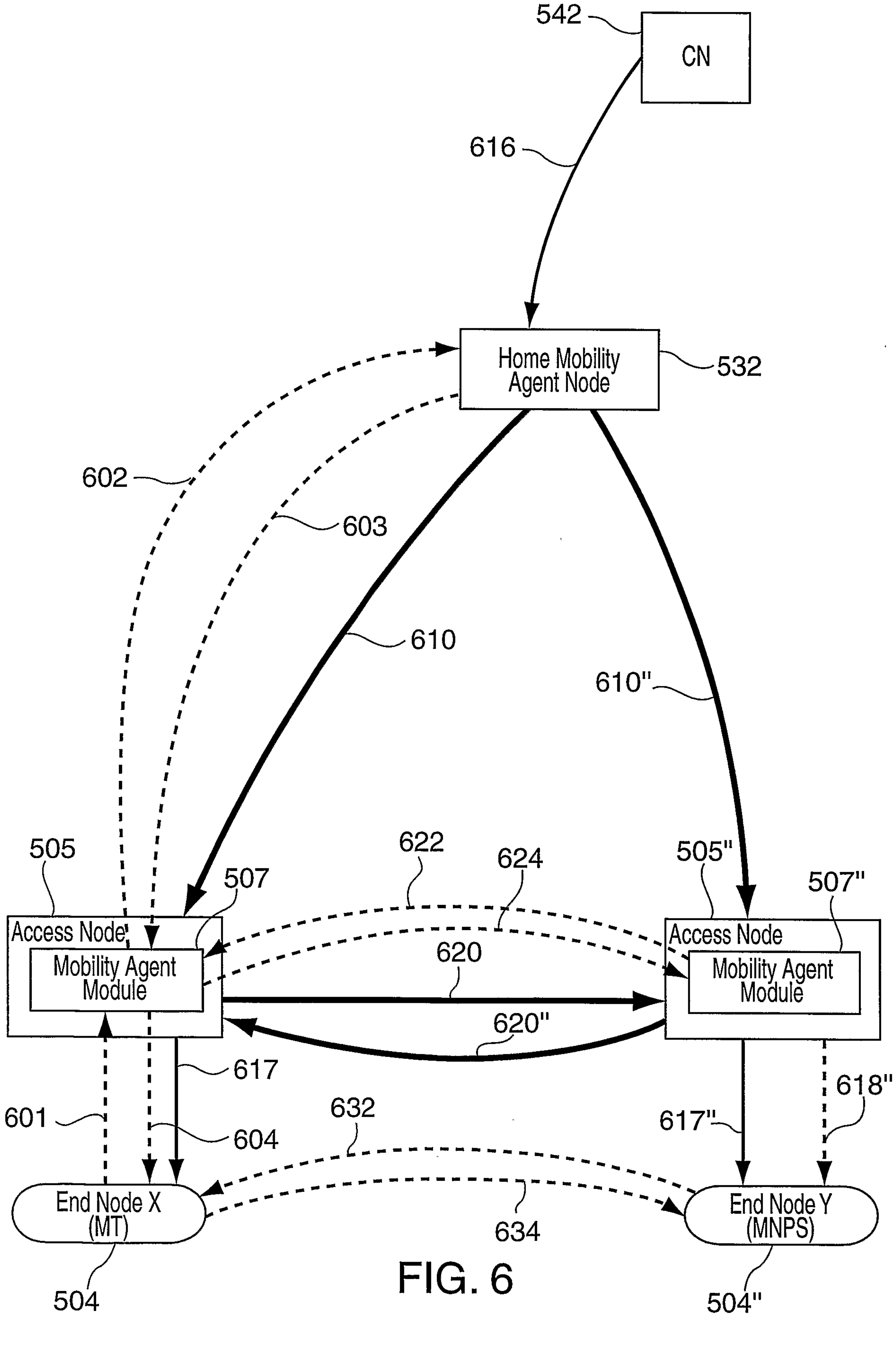

542
CN
616
Home Mobility Agent Node
532
602
603
610
610"
505
622
624
505"
507
507"
Access Node
Mobility Agent Module
620
Access Node
Mobility Agent Module
620"
617
618"
601
632
604
617"
End Node X (MT)
End Node Y (MNPS)
634
504
504"

FIG. 6

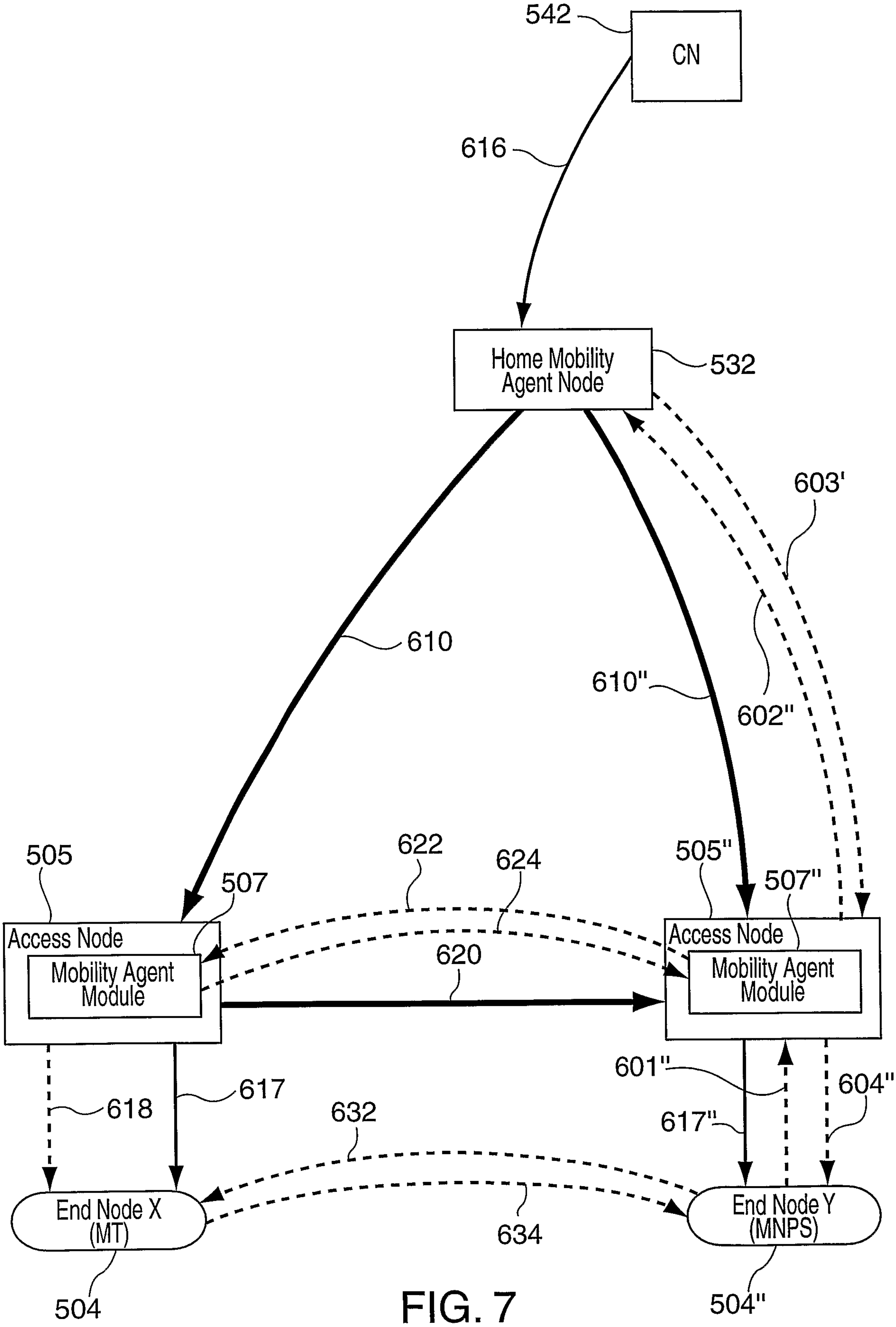

542
CN
616
Home Mobility Agent Node
532
603'
610
610''
602''
505
622
624
505''
507
507''
Access Node
Mobility Agent Module
620
Access Node
Mobility Agent Module
601''
604''
618
617
632
617''
End Node X (MT)
End Node Y (MNPS)
634
504
504''

FIG. 7

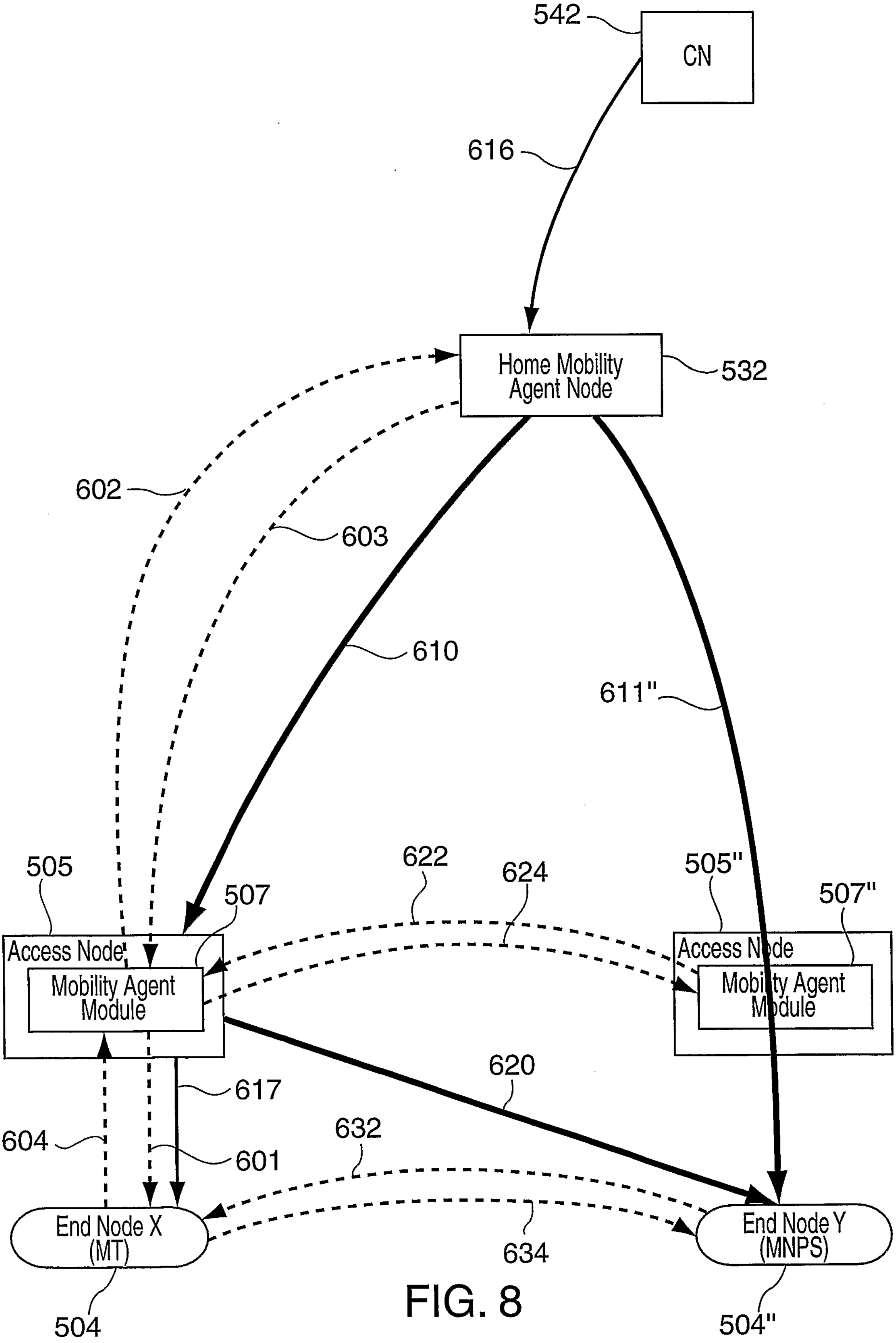

542
CN
616
Home Mobility Agent Node
532
602
603
610
611"
505
622
624
505"
507"
507
Access Node
Mobility Agent Module
Access Node
Mobility Agent Module
617
620
604
632
601
End Node X (MT)
634
End Node Y (MNPS)
504
504"

FIG. 8

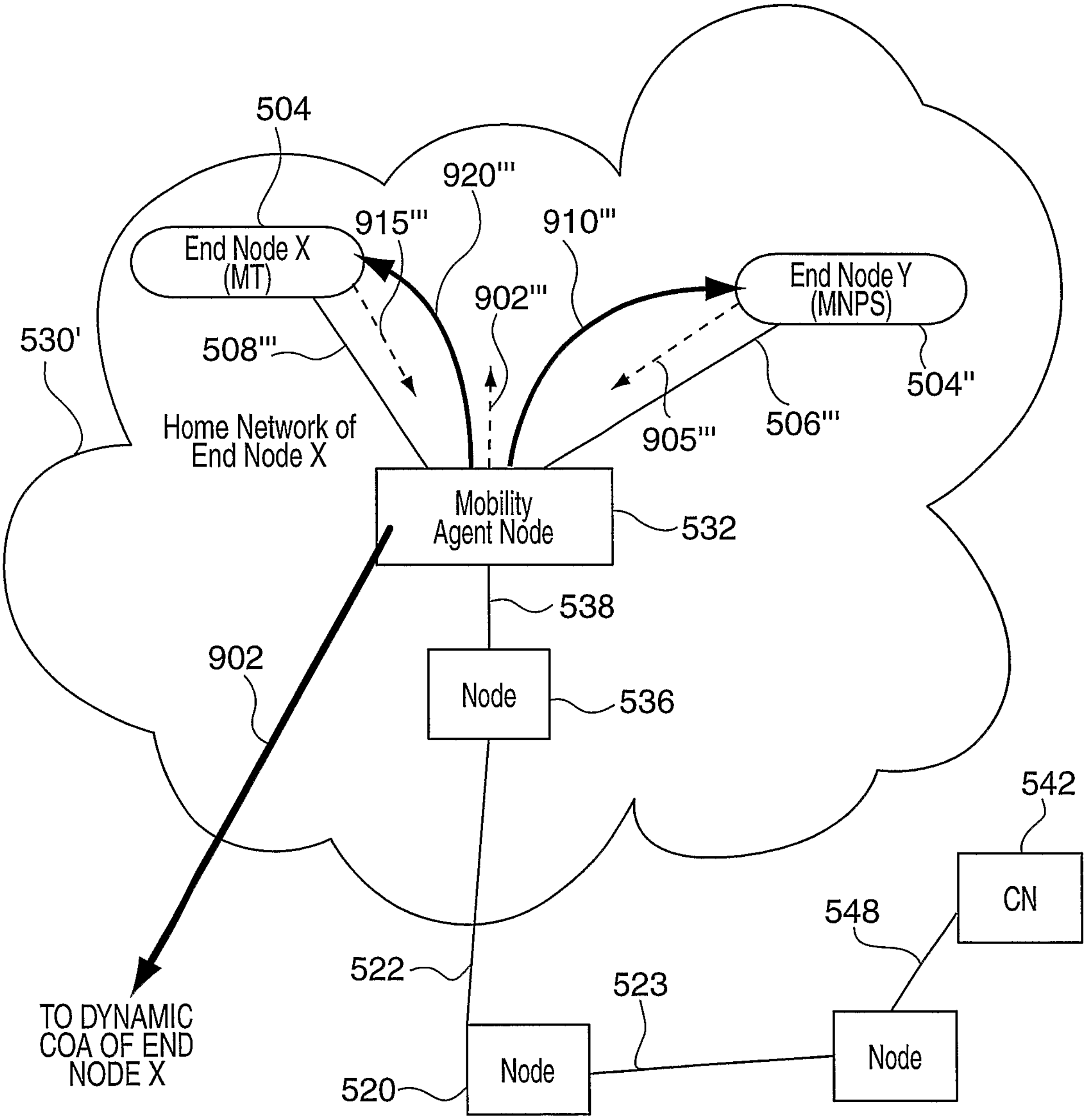

504
920'''
915'''
910'''
End Node X
(MT)
902'''
End Node Y
(MNPS)
530'
508'''
504"
Home Network of
End Node X
905'''
506'''
Mobility
Agent Node
532
538
902
Node
536
542
CN
548
522
523
TO DYNAMIC
COA OF END
NODE X
Node
Node
520

FIG. 9