Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2800236 C 2014/06/17

(11)(21) 2 800 236

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2004/04/28

(41) Mise à la disp. pub./Open to Public Insp.: 2004/11/11

(45) Date de délivrance/Issue Date: 2014/06/17

(62) Demande originale/Original Application: 2 520 501

(30) Priorité/Priority: 2003/04/28 (US10/426,106)

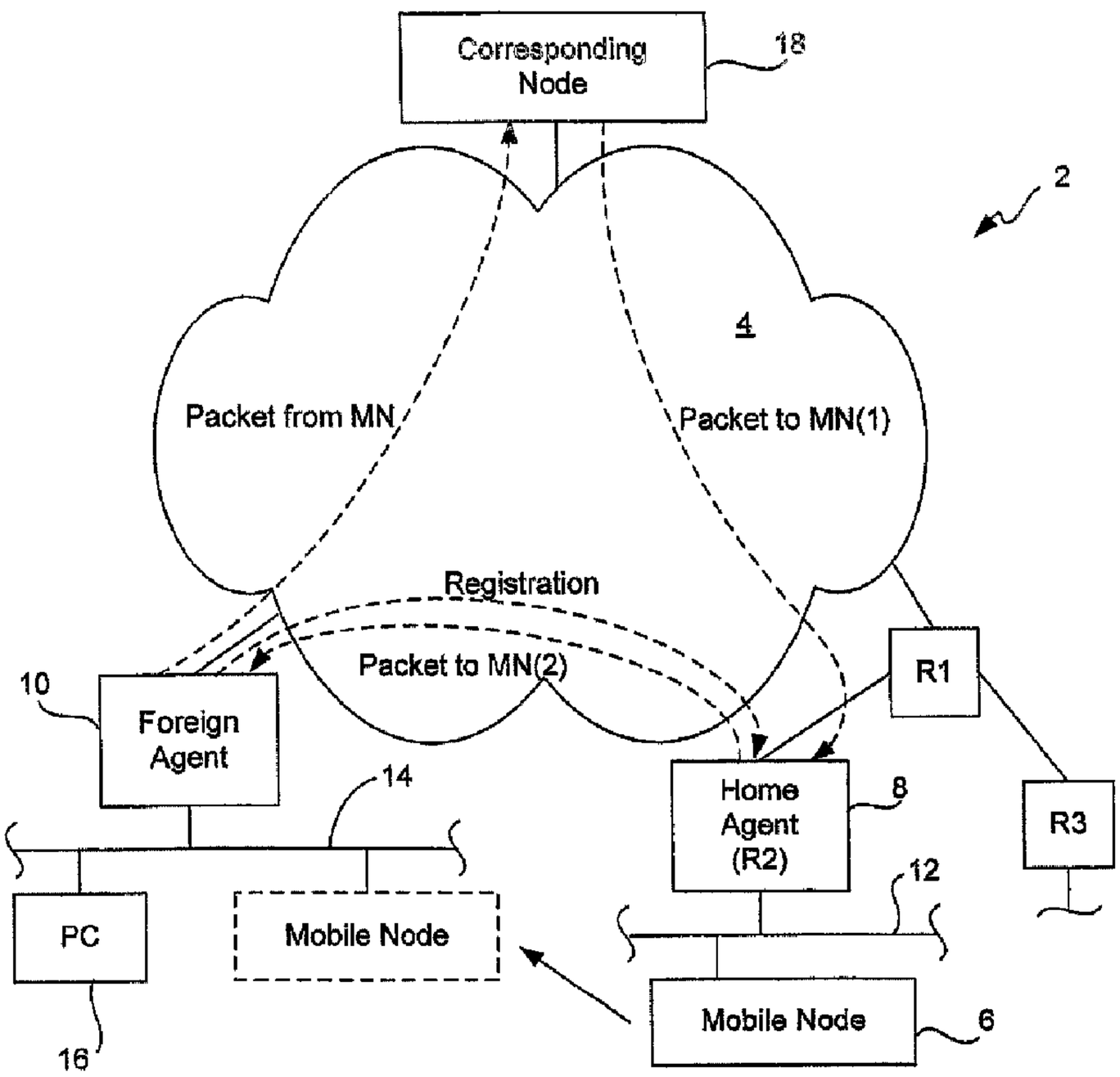
(51) Cl.Int./Int.Cl. *H04W 8/02* (2009.01), *H04W 12/08* (2009.01), *H04W 8/04* (2009.01), *H04W 8/06* (2009.01)

(72) Inventeurs/Inventors:
LEUNG, KENT K., US;
DOMMETY, GOPAL, US

(73) Propriétaire/Owner:
CISCO TECHNOLOGY, INC., US

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : METHODES ET APPAREIL POUR SECURISER UN SUPPORT IP MOBILE MANDATAIRE DE L'INVENTION
(54) Title: METHODS AND APPARATUS FOR SECURING PROXY MOBILE IP BACKGROUND OF THE INVENTION



(57) Abrégé/Abstract:
An invention is disclosed that enables proxy Mobile IP registration to be performed in a secure manner. Various security mechanisms may be used independently, or in combination with one another, to authenticate the identity of a node during the

CA 2800236 C 2014/06/17

(11)(21) 2 800 236

(13) C

(57) Abrégé(suite)/Abstract(continued):
registration process. First, an Access Point receiving a packet from a node verifies that the source MAC address identified in the packet is in the Access Point's client association table. In addition, as a second mechanism, the Access Point ensures that a one-to-one mapping exists for the source MAC address and source IP address identified in the packet in a mapping table maintained by the Access Point. As a third mechanism, a binding is not modified in the mobility binding table maintained by the Home Agent unless there is a one-to-one mapping in the mobility binding table between the source MAC address and the source IP address. Similarly, the Foreign Agent may also maintain a mapping between the source IP address and the source MAC address in its visitor table to ensure a one-to-one mapping between a source IP address and the associated MAC address. The MAC address is preferably transmitted in a MAC address extension to the registration request and registration reply packets. In this manner, the Access Point, Home Agent, and Foreign Agent may ascertain the node's MAC address and ensure a one-to-one mapping between the IP address and the MAC address during the registration process.

Abstract

An invention is disclosed that enables proxy Mobile IP registration to be performed in a secure manner. Various security mechanisms may be used independently, or in combination with one another, to authenticate the identity of a node during the registration process. First, an Access Point receiving a packet from a node verifies that the source MAC address identified in the packet is in the Access Point's client association table. In addition, as a second mechanism, the Access Point ensures that a one-to-one mapping exists for the source MAC address and source IP address identified in the packet in a mapping table maintained by the Access Point. As a third mechanism, a binding is not modified in the mobility binding table maintained by the Home Agent unless there is a one-to-one mapping in the mobility binding table between the source MAC address and the source IP address. Similarly, the Foreign Agent may also maintain a mapping between the source IP address and the source MAC address in its visitor table to ensure a one-to-one mapping between a source IP address and the associated MAC address. The MAC address is preferably transmitted in a MAC address extension to the registration request and registration reply packets. In this manner, the Access Point, Home Agent, and Foreign Agent may ascertain the node's MAC address and ensure a one-to-one mapping between the IP address and the MAC address during the registration process.

METHODS AND APPARATUS FOR SECURING PROXY MOBILE IP BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to Mobile IP network technology. More particularly, the present invention relates to authenticating the identity of a node during proxy registration performed on behalf of the node.

2. Description of the Related Art

Mobile IP is a protocol which allows laptop computers or other mobile computer units (referred to as "Mobile Nodes" herein) to roam between various sub-networks at various locations--while maintaining internet and/or WAN connectivity. Without Mobile IP or related protocol, a Mobile Node would be unable to stay connected while roaming through various sub-networks. This is because the IP address required for any node to communicate over the internet is location specific. Each IP address has a field that specifies the particular sub-network on which the node resides. If a user desires to take a computer which is normally attached to one node and roam with it so that it passes through different sub-networks, it cannot use its home base IP address. As a result, a business person traveling across the country cannot merely roam with his or her computer across geographically disparate network segments or wireless nodes while remaining connected over the internet. This is not an acceptable state-of-affairs in the age of portable computational devices.

To address this problem, the Mobile IP protocol has been developed and implemented. An implementation of Mobile IP is described in RFC 2002 of the Network Working Group, C. Perkins, Ed. , October 1996. Mobile IP is also described in the text "Mobile IP Unplugged "by J. Solomon, Prentice Hall.

The Mobile IP process and environment are illustrated in FIG. 1. As shown there, a Mobile IP environment 2 includes the internet (or a WAN) 4 over which a Mobile Node 6 can communicate remotely via mediation by a Home Agent 8 and a Foreign Agent 10.

Typically, the Home Agent and Foreign Agent are routers or other network connection devices performing appropriate Mobile IP functions as implemented by software, hardware, and/or firmware. A particular Mobile Node (e. g. , a laptop computer) plugged into its home network segment connects with the internet. When the Mobile Node roams,

it communicates via the internet through an available Foreign Agent. Presumably, there are many Foreign Agents available at geographically disparate locations to allow wide spread internet connection via the Mobile IP protocol. Note that it is also possible for the Mobile Node to register directly with its Home Agent.

As shown in FIG. 1, Mobile Node 6 normally resides on (or is "based at") a network segment 12 which allows its network entities to communicate over the internet 4. Note that Home Agent 8 need not directly connect to the internet. For example, as shown in FIG. 1, it may be connected through another router (a router R1 in this case). Router R1 may, in turn, connect one or more other routers (e.g., a router R3) with the internet.

Now, suppose that Mobile Node 6 is removed from its home base network segment 12 and roams to a remote network segment 14. Network segment 14 may include various other nodes such as a PC 16. The nodes on network segment 14 communicate with the internet through a router which doubles as Foreign Agent 10. Mobile Node 6 may identify Foreign Agent 10 through various solicitations and advertisements which form part of the Mobile IP protocol. When Mobile Node 6 engages with network segment 14, Foreign Agent 10 relays a registration request to Home Agent 8 (as indicated by the dotted line "Registration"). The Home and Foreign Agents may then negotiate the conditions of the Mobile Node's attachment to Foreign Agent 10. For example, the attachment may be limited to a period of time, such as two hours. When the negotiation is successfully completed, Home Agent 8 updates an internal "mobility binding table" which specifies the care-of address (e.g., a collocated care-of address or the Foreign Agent's IP address) in association with the identity of Mobile Node 6. Further, the Foreign Agent 10 updates an internal "visitor table" which specifies the Mobile Node address, Home Agent address, etc. In effect, the Mobile Node's home base IP address (associated with segment 12) has been shifted to the Foreign Agent's IP address (associated with segment 14).

Now, suppose that Mobile Node 6 wishes to send a message to a corresponding node 18 from its new location. An output message from the Mobile Node is then packetized and forwarded through Foreign Agent 10 over the internet 4 and to corresponding node 18 (as indicated by the dotted line "packet from MN") according to a standard internet protocol. If corresponding node 18 wishes to send a message to Mobile Node -- whether in reply to a message from the Mobile Node or for any other reason -- it addresses that message to the IP address of Mobile Node 6 on sub-network 12. The

packets of that message are then forwarded over the internet 4 and to router R1 and ultimately to Home Agent 8 as indicated by the dotted line ("packet to MN(1)"). From its mobility binding table, Home Agent 8 recognizes that Mobile Node 6 is no longer attached to network segment 12. It then encapsulates the packets from corresponding node 18 (which are addressed to Mobile Node 6 on network segment 12) according to a Mobile IP protocol and forwards these encapsulated packets to a "care of" address for Mobile Node 6 as shown by the dotted line ("packet to MN(2)"). The care-of address may be, for example, the IP address of Foreign Agent 10. Foreign Agent 10 then strips the encapsulation and forwards the message to Mobile Node 6 on sub-network 14. The packet forwarding mechanism implemented by the Home and Foreign Agents is often referred to as "tunneling."

It is often desirable to assign a unique IP address to each user or device within a network. Moreover various protocols enable automatic assignment of IP addresses within a particular network. For instance, in accordance with the Dynamic Host Configuration Protocol (DHCP), network administrators may manage a network centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. More particularly, using the Internet's set of protocols (TCP/IP), each device that is capable of connecting to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP allows a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different location within the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. DHCP is particularly useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Thus, DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

Although DHCP functions in a static environment, the assignment of a new IP address each time a computer changes its location within a network is far from ideal

within a mobile environment. More particularly, when a mobile node roams to a new location within a network, it would be desirable for the node to maintain its home address. However, provisions have not been made for a node that wishes to maintain a single IP address when it changes its location within a network using DHCP. Moreover, a node that is not mobile enabled cannot currently change its location within a network using DHCP and still maintain its assigned IP address.

It is possible to provide Internet services via a wireless link for mobile users who attach to a network via a connection such as a DHCP connection, even where the node does not support Mobile IP. Specifically, a proxy device may implement Mobile IP on behalf of a node that does not support Mobile IP functionality. One such proxy device is the access point (AP). An Access Point (AP) may be defined as the center point in an all-wireless network or serves as a connection point between a wired and a wireless network. Multiple APs can be placed throughout a facility to give users with WLAN adapters the ability to roam freely throughout an extended area while maintaining uninterrupted access to all network resources.

Patent Application Serial No. 10/080,995, entitled "METHODS AND APPARATUS FOR SUPPORTING PROXY MOBILE IP REGISTRATION IN A WIRELESS LOCAL AREA NETWORK," discloses a system for communicating subnet addresses of gateways (e.g., Home Agents) that support APs in the network. When an AP receives a data packet, the AP may compare the data packet (e.g., source address) with the AP information for one or more APs to determine whether to send a registration request on behalf of the node. More particularly, the AP determines from the source address whether the node is located on a subnet identical to a subnet of the AP. If the node is located on the subnet of the AP, no Mobile IP service is required on behalf of the node. However, when it is determined from the source address that the node is not located on the subnet identical to the subnet of the Access Point, the AP composes and sends a mobile IP registration request on behalf of the node. For instance, the mobile IP registration request may be composed using the gateway associated with the "home" AP (e.g., having a matching subnet) as the node's Home Agent.

Proxy Mobile IP allows clients to move between networks while maintaining sessions. This is accomplished through Mobile IP control messages such as those disclosed in Attorney Docket No. CISCP263, Application Serial No. 10/080,995,

entitled "METHODS AND APPARATUS FOR SUPPORTING PROXY MOBILE IP REGISTRATION IN A WIRELESS LOCAL AREA NETWORK," by inventors Wang et al, filed on February 20, 2002. In this manner, even clients that do not support Mobile IP may move between networks while maintaining sessions.

As shown in FIG. 2, proxy Mobile IP is supported by multiple Access Points within a wireless Local Area Network (WLAN). In this example, two Access Points 202 and 204 support proxy Mobile IP for sub-network A. In this example, a DHCP server assigns an IP address on sub-network A to the node 205. One of the Access Points 202 and 204 detects whether the IP address of the node 205 is on a different sub-network. Since the IP address of the node 205 is on the same sub-network as the Access Points 202 and 204, proxy registration is not required since the node 205 is in its home network.

Alternatively, if the node 205 were on a different sub-network, a registration request would be composed on behalf of the client 205 and sent to the Foreign Agent. The registration request is then processed by the Foreign Agent, shown here as router 206, and subsequently by the client's Home Agent. Upon completion of registration of the node 205 with its Home Agent, packets addressed to the node 205 are then tunneled to node 205 by its Home Agent via the Foreign Agent and Access Point.

When the node 205 subsequently roams beyond the layer 3 boundary from sub-network A to sub-network B, one of the two Access Points 208 and 210 supporting proxy Mobile IP for sub-network B composes a registration request on behalf of the client 205 once it is determined that the IP address of the node 205 is on a different sub-network. The registration request is then processed by the Foreign Agent, shown here as router 212, and forwarded to the client's Home Agent. Upon completion of registration of the node 205 with its Home Agent, packets addressed to the node 205 are then tunneled to the node 205 by the node's Home Agent via the Foreign Agent and Access Point.

While proxy Mobile IP is advantageous since it allows non-Mobile IP enabled nodes to move while maintaining a session, this method is susceptible to route poisoning and Denial of Service (DoS) attacks. Specifically, another client may send packets with various source IP addresses and MAC addresses. When this second client sends a packet with another client's IP address, the network would then direct traffic to the IP address at the location of the second client because the Access Point

would assume that the first client has moved.

In view of the above, it would be desirable if an authentication mechanism could be implemented to authenticate the identity of a client for which proxy Mobile IP registration is being performed.

SUMMARY OF THE INVENTION

An invention is disclosed that enables proxy Mobile IP registration to be performed in a secure manner. Various security mechanisms may be used independently, or in combination with one another, to authenticate the identity of a node during the registration process. This is accomplished, at least in part, by verifying and/or transmitting the MAC address assigned to the node in various steps in the registration process.

In accordance with one aspect of the invention, as a first security mechanism, an Access Point receiving a packet from a node verifies that the source MAC address identified in the packet is in the Access Point's client association table. After this security mechanism is satisfied, the Access Point may compose a registration request or require that further security mechanisms be satisfied prior to composing a registration request on behalf of the node.

In accordance with another aspect of the invention, as a second security mechanism, the Access Point ensures that a one-to-one mapping exists for the source MAC address and source IP address identified in the packet in a mapping table maintained by the Access Point. After this security mechanism is satisfied, the Access Point may compose a registration request packet. In other words, the Access Point may require that both the first and second security mechanisms be satisfied prior to composing a registration request packet on behalf of the node.

In accordance with yet another aspect of the invention, as a third mechanism, a binding is not modified in the mobility binding table maintained by the Home Agent unless there is a one-to-one mapping in the mobility binding table between the source MAC address and the source IP address. Similarly, the Foreign Agent may also maintain a mapping between the source IP address and the source MAC address in its visitor table to ensure a one-to-one mapping between a source IP address and the associated MAC address.

In accordance with yet another aspect of the invention, the MAC address is preferably transmitted in a MAC address extension to the registration request and

registration reply packets. In this manner, the Access Point, Home Agent, and Foreign Agent may ascertain the node's MAC address and ensure a one-to-one mapping between the IP address and the MAC address during the registration process. Through the use of the above technique(s), the risk of route poisoning and Denial of Service (DoS) attacks is reduced.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram illustrating a Mobile IP network segment and associated environment.

FIG. 2 is a block diagram illustrating a system in which proxy Mobile IP is supported.

FIG. 3 is a process flow diagram illustrating a method of authenticating a client during the proxy registration process in accordance with various embodiments of the invention.

FIG. 4 is a diagram illustrating a client association table maintained by an Access Point in accordance with various embodiments of the invention.

FIG. 5 is a diagram illustrating a mapping table maintained by an Access Point in accordance with various embodiments of the invention.

FIG. 6 is a diagram illustrating an exemplary mobility binding table maintained by a Home Agent in accordance with various embodiments of the invention.

FIG. 7 is a diagram illustrating an exemplary visitor table maintained by a Foreign Agent in accordance with various embodiments of the invention.

FIG. 8 is a diagram illustrating an exemplary registration request packet composed by an Access Point and transmitted in accordance with various embodiments of the invention.

FIG. 9 is a diagram illustrating an exemplary registration reply packet composed by a Home Agent and transmitted in accordance with various embodiments of the invention.

FIG. 10 is a block diagram of a network device that may be configured to implement aspects of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious,

however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps have not been described in detail in order not to unnecessarily obscure the present invention.

An invention is described herein that enables a node (e.g., a node that does not implement the Mobile IP protocol) to roam to various Foreign Agents within a network including a DHCP supported network. This is accomplished, in part, through the use of control messages sent between the access points within the network. For purposes of the following discussion, the term "mobile node" will be used to refer to a mobile node implementing the Mobile IP protocol while the term "node" will be used to refer to a node that does not implement the Mobile IP protocol.

FIG. 2 is a block diagram illustrating a system in which the present invention may be implemented. In the following description, the present invention is implemented in a wireless network. However, although the present invention is described as being implemented in a wireless network, the present invention may also be implemented in a non-wireless network. As shown, a node 205 may wish to roam from its Home Agent 200 to a first Foreign Agent 206. Similarly, once attached to the first Foreign Agent 206, the node 205 may again wish to roam to a second Foreign Agent 212. Although the node 205 may have an assigned IP address, when the node 205 roams, it is preferable for the node to maintain this assigned IP address. For instance, although a DHCP server typically dynamically assigns a new IP address to a node when its location within a network has changed, it is preferable to maintain the IP address originally assigned to the node by the DHCP server.

In a wireless network, Access Points 202, 204 and 208, 210 are coupled to the Foreign Agents 206 and 212 respectively. By way of example, in a wireless network, the Access Points 202, 204 and 208, 210 may have an antenna and receiver for receiving packets. As yet another example, the Access Points 202, 204 and 208, 210 may designate connection points in a non-wireless network. Typically, a mobile node implementing Mobile IP registers and de-registers with its Home Agent through the registration process. However, according to various embodiments of the invention disclosed in Patent Application Serial No. 10/080,995, entitled "METHODS AND APPARATUS FOR SUPPORTING PROXY MOBILE IP REGISTRATION IN A WIRELESS LOCAL AREA NETWORK,", registration is initiated by the Access

Point on behalf of the Mobile IP node. Similarly, de-registration may be initiated by the Access Point on behalf of the roaming node. For instance, node 205 that has roamed to the first Foreign Agent 206 is registered with the node's Home Agent 200 when the first Access Point 202 composes and sends a registration request packet via the first Foreign Agent 206. Thus, the first Foreign Agent's visitor table and the Home Agent's mobility binding table are updated to indicate that the node has roamed to the first Foreign Agent 206. When the node 205 roams to the second Foreign Agent 212, the node 205 is registered with the Home Agent via the second Foreign Agent 212 (e.g., by one of the Access Points 208, 210, the Foreign Agent 212 and/or the Home Agent 200). In other words, the first Foreign Agent 206 updates its visitor table to reflect the movement of the node 205. Similarly, the Home Agent's mobility binding table is updated to reflect the movement of the node 205 to the second Foreign Agent 212. Thus, the appropriate entry in the first Foreign Agent's visitor table and the Home Agent's mobility binding table may be deleted. A new entry is then entered in the Home Agent's mobility binding table and the second Foreign Agent's visitor table upon completion of registration of the mobile node with the Home Agent. Alternatively, the visitor table may be maintained and updated by the Access Point.

FIG. 3 is a process flow diagram illustrating a method of authenticating a client during the proxy registration process in accordance with various embodiments of the invention. As shown at block 302, the node associates with the Access Point. Specifically, when the node associates with the Access Point, the Access Point obtains the MAC address of the node. When a node wishes to connect with an Access Point, it first associates with the Access Point. Association is the process by which the node (e.g., including a wireless LAN card) informs the Access Point of the existence of the node (e.g., its MAC address) and its intention to connect to this Access Point. After association is completed, the node is connected to theAccess Point, but may not be able to send data before authentication of the node. During association, the Access Point receives a packet from which the Access Point ascertains the MAC address. The Access Point then updates its client association table with the obtained source MAC address at block 304. When the node subsequently sends a packet including a source MAC address and a source IP address at block 306, the Access Point learns the source IP address of the node at block 308.

The Access Point may learn the IP and MAC address of the node through other mechanisms as well as from packets received by the Access Point. For instance, during Mobile IP authentication of the node, an IP address may be allocated to the node by an entity such as the Home Agent or Foreign Agent. During this authentication process, the Access Point may therefore learn the IP and MAC address. In another embodiment, the Access Point may listen to DHCP queries from the node from which the IP and MAC address are obtained.

In order to ascertain whether proxy Mobile IP service is required, the Access Point determines whether the source IP address is on a different subnet from the Access Point at block 310. If the source IP address is not on a different subnet as shown at block 312, standard registration pursuant to RFC 3440 is performed at block 314. Otherwise, the Access Point proceeds with the proxy registration process.

First, the Access Point determines whether the source MAC address from the packet is in its client association table at block 316. An exemplary client association table will be described in further detail below with reference to FIG. 4. If it is determined at block 318 that the source MAC address is not in the client association table, the packet will be ignored at block 320 and proxy registration will not be completed. In other words, packets will be dropped if it is determined that they are coming from an invalid source MAC address.

While this first security mechanism may be used on its own, it is preferably used in combination with a subsequent security mechanism, which ensures a one-to-one mapping between the source MAC address and the source IP address identified in the packet. Thus, as a second security mechanism, the Access Point checks at block 322 whether a mapping between the source IP address and the source MAC address exists in the Access Point's mapping table. An exemplary mapping table will be described in further detail below with reference to FIG. 5. Specifically, the Access Point may check whether an entry exists or the source IP address. If the mapping table does not include an entry for the source IP address, the mapping table is updated with a mapping between the source MAC address and the source IP address. However, if a mapping does exist for the source IP address, the Access Point checks that the source MAC address and the source IP address of the packet match the entry in the mapping table.

The first and second security mechanism may each be used alone to ensure that

a registration request is sent on behalf of a valid node. However, as described above, the two security mechanisms are preferably used in combination with one another. Thus, once both security mechanisms have been satisfactorily passed as shown at block 323, the Access Point composes a registration request at block 324. The registration request preferably includes a MAC address extension including the source MAC address. An exemplary registration request will be described in further detail below with reference to FIG. 8. However, if the Access Point determines that the mapping table does not include an entry for the source IP address and the source MAC address identified in the packet, the packet is ignored at block 325, and a registration request is not composed.

Once a registration request is sent to the Foreign agent, the Foreign Agent performs standard Mobile IP processing at block 326. In addition, the Foreign Agent may also maintain a mapping table such as that illustrated in FIG. 5, either separately or in a visitor table such as that described below with reference to FIG. 7. In this manner, the Foreign Agent may check whether a mapping between an IP address and MAC address exists prior to forwarding the registration request to the Home Agent. In other words, if a mapping does not exist, the Foreign Agent may drop the registration request packet. For instance, if an entry includes the IP address but a different MAC address, the Foreign Agent may drop the registration request packet. This may be accomplished by searching for an entry including the IP address, and subsequently checking the entry to ascertain whether the entry includes the MAC address. This checking may be performed by the Foreign Agent instead of or in addition to the other security mechanisms described above with reference to the Access Point.

When the Home Agent receives the registration request packet at block 328, it updates its mobility binding table as necessary. An exemplary mobility binding table will be described in further detail below with reference to FIG. 6. In accordance with one embodiment, the Home Agent updates the mobility binding table with a mapping between the source IP address from the home address field of the registration request packet and the source MAC address from the MAC address extension of the registration request packet. Specifically, the Home Agent checks if a binding exists for the source IP address. If a binding does not exist at block 330, the Home Agent updates the mobility binding table at block 332 to map the source IP address and the

source MAC address to the care-of address identified in the registration request packet (e.g., to correlate with the new location of the node). Alternatively, if a binding in the mobility binding table exists for the source IP address, the Home Agent may perform a security check as a third security mechanism at block 334 to ensure that the entry contains a mapping between the source IP address and the source MAC address. If the mapping does not match the source IP address and the source MAC address at block 336, the registration request packet may be ignored at block 338. Otherwise, the Home Agent performs standard Mobile IP processing at block 340 and composes a registration reply at block 342. The registration reply preferably includes a MAC address extension including the source MAC address. The registration reply is then sent to the care-of address (e.g., Foreign Agent). An exemplary registration reply will be described in further detail below with reference to FIG. 9.

When the Foreign Agent receives the registration reply at block 344, it updates its visitor table as appropriate. For instance, if registration is successful, the visitor table is updated such that the Home Agent address is associated with the source IP address as well as the source MAC address. An exemplary visitor table will be described in further detail below with reference to FIG. 7. The registration reply is then forwarded to the node via the Access Point at block 346.

Once registration is completed, packets may be forwarded to the node at its new location by the Home Agent. Specifically, the Home Agent will look up the destination IP address specified in the packet in the Home Agent's mobility binding table to ascertain the node's care-of address. The packet may then be forwarded to the source IP address via the packets care-of address.

FIG. 4 is a diagram illustrating a client association table maintained by an Access Point in accordance with various embodiments of the invention. A client association table 402 includes a plurality of entries 404, each of the entries identifying a source MAC address. In other words, the table functions as a list of MAC addresses which may be searched by the Access Point maintaining the list.

FIG. 5 is a diagram illustrating a mapping table maintained by an Access Point in accordance with various embodiments of the invention. Mapping table 502 maps a source IP address 504 to a source MAC address 506 in a single entry. In this manner, valid IP/MAC address pairs may be identified by an Access Point searching the table 502.

FIG. 6 is a diagram illustrating an exemplary mobility binding table maintained by a Home Agent in accordance with various embodiments of the invention. As shown, a mobility binding table 602 typically identifies the node via a node identifier such as its home address 604 (source IP address). In addition, the mobility binding table may also include the source MAC address 606 as identified in the MAC address extension of the registration request (and registration reply) packets. Each entry will also identify the care-of address 608 and tunnel interface 610.

FIG. 7 is a diagram illustrating an exemplary visitor table maintained by a Foreign Agent in accordance with various embodiments of the invention. As described above, the visitor table 702 typically includes a node identifier such as home address 704 (source IP address). In addition, the visitor table may also include the source MAC address 706 as identified in the MAC address extension of the registration reply packet. Each entry will also identify the Home Agent address 708 and tunnel interface 710.

FIG. 8 is a diagram illustrating an exemplary registration request packet composed by an Access Point and transmitted in accordance with various embodiments of the invention. Generally, the registration request packet 802 will include a Home Address field including the source IP address, care-of address field including the care-of address, and Home Agent address field including the Home Agent address. In addition, a MAC address extension will be appended to the registration request packet. The MAC address extension will include the source MAC address as obtained from the packet received from the node.

FIG. 9 is a diagram illustrating an exemplary registration reply packet composed by a Home Agent and transmitted in accordance with various embodiments of the invention. The registration reply packet 902 includes a Home Address field including the source IP address, care-of address field including the care-of address, and Home Agent address field including the Home Agent address. In addition, a MAC address extension will be appended to the registration reply packet, enabling the Foreign Agent to update the visitor table with the information for node identified by the IP address and corresponding MAC address. The registration reply packet that is forwarded to the node need not include the MAC address extension.

Other Embodiments

Generally, the techniques of the present invention may be implemented on

software and/or hardware. For example, they can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software such as an operating system or in an application running on an operating system.

A software or software/hardware hybrid implementation of the techniques of this invention may be implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory. Such a programmable machine may be a network device designed to handle network traffic, such as, for example, a router or a switch. Such network devices may have multiple network interfaces including frame relay and ISDN interfaces, for example. Specific examples of such network devices include routers and switches. For example, the Access Points of this invention may be implemented in specially configured routers or servers, as well as Cisco Aironet Access Points, available from Cisco Systems, Inc. of San Jose, California. A general architecture for some of these machines will appear from the description given below. In an alternative embodiment, the techniques of this invention may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general-purpose computing device.

Referring now to FIG. 10, a network device 1560 suitable for implementing the techniques of the present invention includes a master central processing unit (CPU) 1562, interfaces 1568, and a bus 1567 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 1562 may be responsible for implementing specific functions associated with the functions of a desired network device. For example, when configured as an intermediate router, the CPU 1562 may be responsible for analyzing packets, encapsulating packets, and forwarding packets for transmission to a set-top box. The CPU 1562 preferably accomplishes all these functions under the control of software including an operating system (e.g. Windows NT), and any appropriate applications software.

CPU 1562 may include one or more processors 1563 such as a processor from the Motorola family of microprocessors or the MIPS family of microprocessors. In an

alternative embodiment, processor 1563 is specially designed hardware for controlling the operations of network device 1560. In a specific embodiment, a memory 1561 (such as non-volatile RAM and/or ROM) also forms part of CPU 1562. However, there are many different ways in which memory could be coupled to the system. Memory block 1561 may be used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, etc.

The interfaces 1568 are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receiving of data packets over the network and sometimes support other peripherals used with the network device 1560. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ethernet interfaces, ATM interfaces, HSSI interfaces, POS interfaces, FDDI interfaces, ASI interfaces, DHEI interfaces and the like. Generally, these interfaces may include ports appropriate for communication with the appropriate media. In some cases, they may also include an independent processor and, in some instances, volatile RAM. The independent processors may control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, these interfaces allow the master microprocessor 1562 to efficiently perform routing computations, network diagnostics, security functions, etc.

Although not shown, various removable antennas may be used for further increase range and reliability of the access points. In addition, radio transmit power e.g., 1, 5, 20, 30, 50, and 100 mW) on the Cisco Aironet –Access Point Series is configurable to meet coverage requirements and minimize interference. In addition, a Cisco Aironet AP can be configured as a redundant hot standby to another AP in the same coverage area. The hot-standby AP continually monitors the primary AP on the same channel, and assumes its role in the rare case of a failure of the primary AP.

Although the system shown in FIG. 10 illustrates one specific network device of the present invention, it is by no means the only network device architecture on which the present invention can be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc. is often used. Further, other types of interfaces and media could also be used with the

network device.

Regardless of network device's configuration, it may employ one or more memories or memory modules (such as, for example, memory block 1565) configured to store data, program instructions for the general-purpose network operations and/or other information relating to the functionality of the techniques described herein. The program instructions may control the operation of an operating system and/or one or more applications, for example.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Although illustrative embodiments and applications of this invention are shown and described herein, many variations and modifications are possible which remain within the concept, scope, and spirit of the invention, and these variations would become clear to those of ordinary skill in the art after perusal of this application. For instance, although the specification has described access points, other entities used to tunnel packets to mobile nodes on remote network segments can be used as well. For example, routers, bridges or other less intelligent packet switches may also employ the features of this invention. Moreover, although the present invention is useful for nodes that do not support Mobile IP, the invention may also be applicable for nodes that support Mobile IP. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

WHAT IS CLAIMED IS:

1. In a Home Agent, a method, comprising:

receiving a registration request, the registration request including a source MAC address and a source IP address of a node;

determining whether an entry in a mapping table indicates a one-to-one mapping between the source MAC address and the source IP address;

registering the node with the Home Agent according to whether it is determined that an entry in the mapping table indicates a one-to-one mapping between the source MAC address and the source IP address; and

composing and sending a registration reply including the source IP address and the source MAC address, wherein the registration reply includes an extension that includes the source MAC address.

2. The method as recited in claim 1, wherein the node does not support Mobile IP.

3. The method as recited in claim 1, wherein the registration request includes an extension that includes the source MAC address.

4. The method as recited in claim 1, wherein registering the node with the Home Agent comprises updating a mobility binding table with an entry for the node.

5. The method as recited in claim 1, wherein the registration request is ignored if an entry that exists for the node in the mapping table does not indicate a one-to-one mapping between the source MAC address and the source IP address.

6. A Home Agent, comprising:

a processor; and

a memory, at least one of the processor or the memory being adapted for:

receiving a registration request, the registration request including a source MAC address and a source IP address of a node;

determining whether an entry in a mapping table indicates a one-to-one mapping between the source MAC address and the source IP address;

registering the node with the Home Agent according to whether it is determined that an entry in the mapping table indicates a one-to-one mapping between the source MAC address and the source IP address; and

composing and sending a registration reply including the source IP address and the source MAC address, wherein the registration reply includes an extension that includes the source MAC address.

7. The Home Agent as recited in claim 6, wherein the node does not support Mobile IP.

8. The Home Agent as recited in claim 6, wherein the registration request includes an extension that includes the source MAC address.

9. The Home Agent as recited in claim 6, wherein registering the node with the Home Agent comprises updating a mobility binding table with an entry for the node.

10. The Home Agent as recited in claim 6, wherein the registration request is ignored if an entry that exists for the node in the mapping table does not indicate a one-to-one mapping between the source MAC address and the source IP address.

11. In a Home Agent, a method of processing a registration request, comprising:

receiving a registration request having a home address field including a source IP address, a care-of address field including a care-of address, and having a MAC address extension including a source MAC address; and

determining whether a one-to-one mapping between the source MAC address and the source IP address exists in a table; and

registering the source IP address with the Home Agent according to whether it is determined that a one-to-one mapping between the source MAC address and the source IP address exists in the table.

12. The method as recited in claim 11, wherein the source IP address and the source MAC address are associated with a node that does not support Mobile IP.

13. The method as recited in claim 11, further comprising:

updating a mobility binding table with a mapping between the source MAC address and the source IP address such that the mapping is associated with the care-of address.

14. The method as recited in claim 11, wherein the table is a mobility binding table.

15. A Home Agent, comprising:

a processor; and

a memory, at least one of the processor or the memory being configured for:

receiving a registration request having a home address field including a source IP address, a care-of address field including a care-of address, and having a MAC address extension including a source MAC address; and

determining whether a one-to-one mapping between the source MAC address and the source IP address exists in a table; and

registering the source IP address with the Home Agent according to whether it is determined that a one-to-one mapping between the source MAC address and the source IP address exists in the table.

16. The Home Agent as recited in claim 15, wherein the source IP address and the source MAC address are associated with a node that does not support Mobile IP.

17. The Home Agent as recited in claim 15, at least one of the processor or the memory being further configured for:

updating a mobility binding table with a mapping between the source MAC address and the source IP address such that the mapping is associated with the care-of address.

18. The Home Agent as recited in claim 15, wherein the table is a mobility binding table.

19. In a Foreign Agent, a method of processing a registration request, comprising:

receiving a registration request having a home address field including a source IP address, a Home Agent field including a Home Agent address, and a MAC address extension including a source MAC address;

determining whether an entry including the source IP address and the source MAC address is in a visitor table maintained by the Foreign Agent; and

forwarding the registration request according to whether an entry in the visitor table maintained by the Foreign Agent includes the source IP address and the source MAC address.

20. The method as recited in claim 19, wherein determining whether an entry including the source IP address and the source MAC address is in the visitor table maintained by the Foreign Agent includes determining whether a one-to-one mapping exists between the source IP address and the source MAC address.

21. The method as recited in claim 20, wherein when a one-to-one mapping between the source IP address and the source MAC address does not exist in the visitor table, dropping the registration request without forwarding the registration request.

22. In a Foreign Agent, a method of processing a registration request, comprising:

receiving a registration request having a home address field including a source IP address, a Home Agent field including a Home Agent address, and a MAC address extension including a source MAC address;

forwarding the registration request to the Home Agent address;

receiving a registration reply having a home address field including the source IP address, a Home Agent field including the Home Agent address, and a MAC address extension including the source MAC address; and

forwarding the registration reply to the source IP address.

23. The method as recited in claim 22, further comprising:

updating a visitor table such that the visitor table includes an entry that associates the source IP address and the source MAC address with the Home Agent address.

24. The method as recited in claim 22, further comprising:

determining whether an entry including the source IP address and the source MAC address is in a visitor table maintained by the Foreign Agent; and

forwarding the registration request to the Home Agent address according to whether an entry including the source IP address and the source MAC address is in the visitor table.

25. In an Access Point, a method of authenticating a node prior to performing proxy registration on behalf of the node, comprising:

receiving a packet from the node, the packet including a source MAC address and a source IP address;

ascertaining whether a one-to-one mapping between the source MAC address and the source IP address exists in a mapping table; and

composing a registration request including a home address field including the source IP address and sending the registration request, thereby performing proxy registration on behalf of the node.

26. The method as recited in claim 25, wherein composing and sending the registration request are performed according to whether it is ascertained that a one-to-one

mapping between the source MAC address and the source IP address exists in a mapping table.

27. The method as recited in claim 25, wherein composing a registration request comprises appending a MAC address extension to the registration request, the MAC address extension including the source MAC address.

28. An Access Point adapted for performing a method of authenticating a node prior to performing proxy registration on behalf of the node, comprising:

a processor; and

a memory, at least one of the processor and the memory being adapted for:

receiving a packet from the node, the packet including a source MAC address and a source IP address;

ascertaining whether a mapping between the source MAC address and the source IP address exists in a mapping table; and

composing a registration request including a home address field including the source IP address and sending the registration request, thereby performing proxy registration on behalf of the node.

29. In a network device supporting Mobile IP, a method, comprising:

receiving a packet, the packet including a source MAC address and a source IP address of a node;

determining whether an entry in a table indicates a one-to-one mapping between the source MAC address and the source IP address;

performing an act of composing and sending a registration request, forwarding the packet, or registering the node, wherein the act is performed according to whether it is determined that an entry in the table indicates a one-to-one mapping between the source MAC address and the source IP address.

30. The method as recited in claim 29, wherein the packet is a registration request, the network device is a Home Agent, and the act performed is registering the node.

31. The method as recited in claim 29, wherein the packet is a registration request, the network device is a Foreign Agent, and the act performed is forwarding the packet to a Home Agent.

32. The method as recited in claim 29, wherein the packet is a data packet, the network device is an Access Point, and the act performed is composing and sending a registration request.

33. In a network device supporting Mobile IP, a method, comprising:

receiving a registration request including a source MAC address and a source IP address of a node;

determining whether an entry in a table indicates a one-to-one mapping between the source MAC address and the source IP address;

forwarding the registration request or registering the node according to whether it is determined that an entry in the table indicates a one-to-one mapping between the source MAC address and the source IP address.

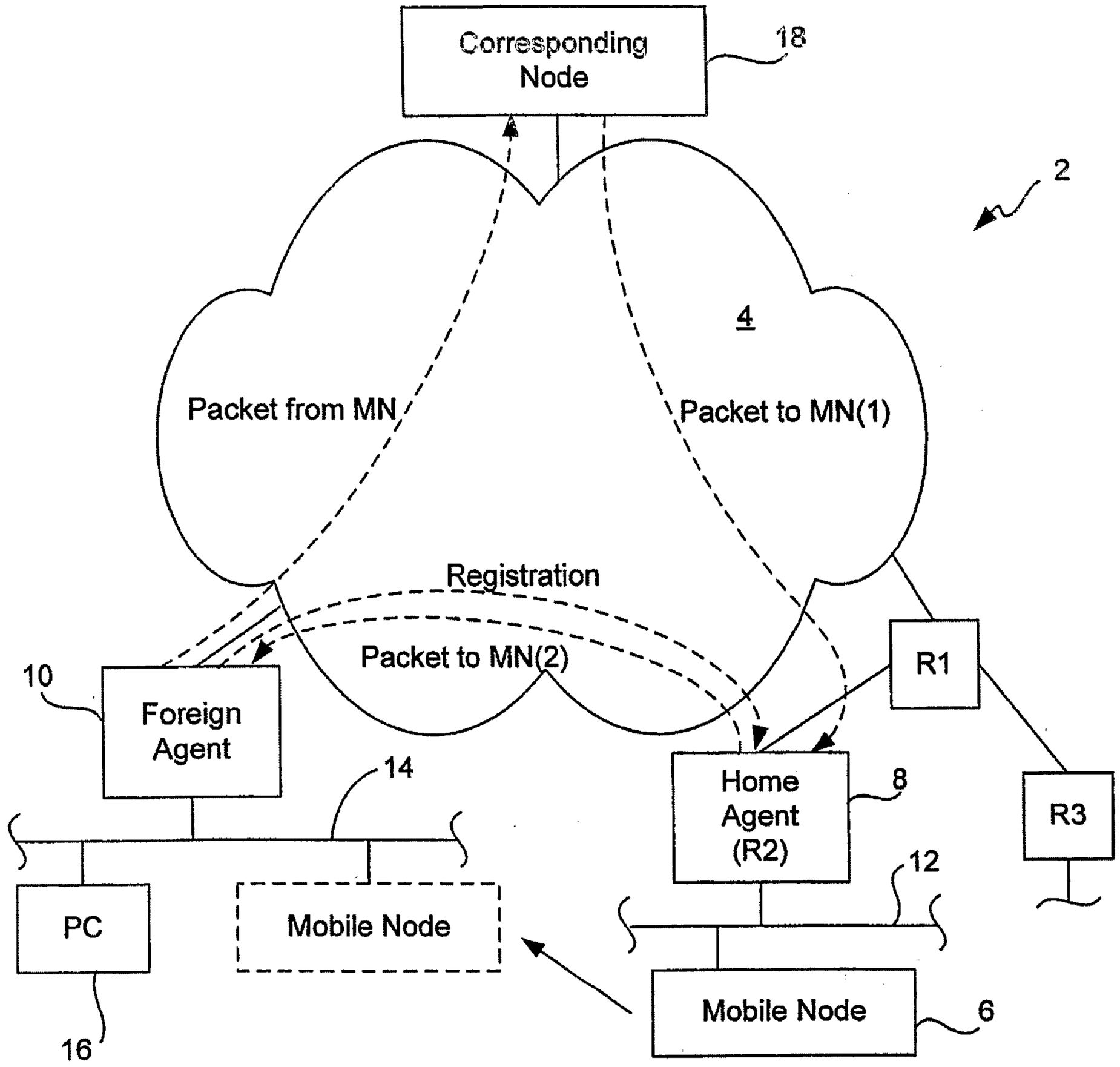

Corresponding Node
18
2
4
Packet from MN
Packet to MN(1)
Registration
Packet to MN(2)
10
Foreign Agent
14
R1
Home Agent (R2)
8
R3
12
PC
Mobile Node
16
Mobile Node
6

FIG. 1

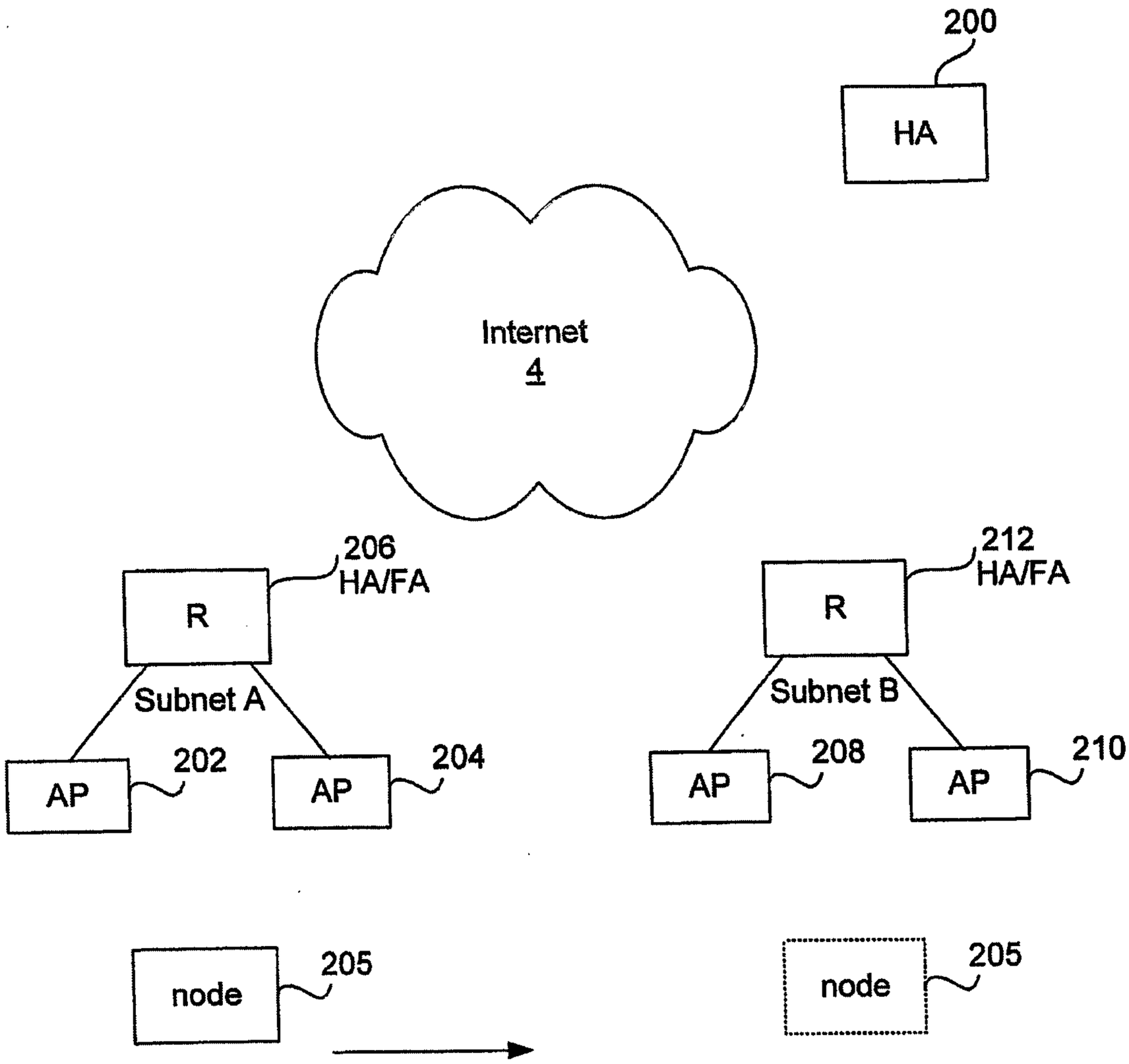

200
HA
Internet
4
206
HA/FA
R
Subnet A
202
AP
204
AP
212
HA/FA
R
Subnet B
208
AP
210
AP
node
205
node
205

FIG. 2

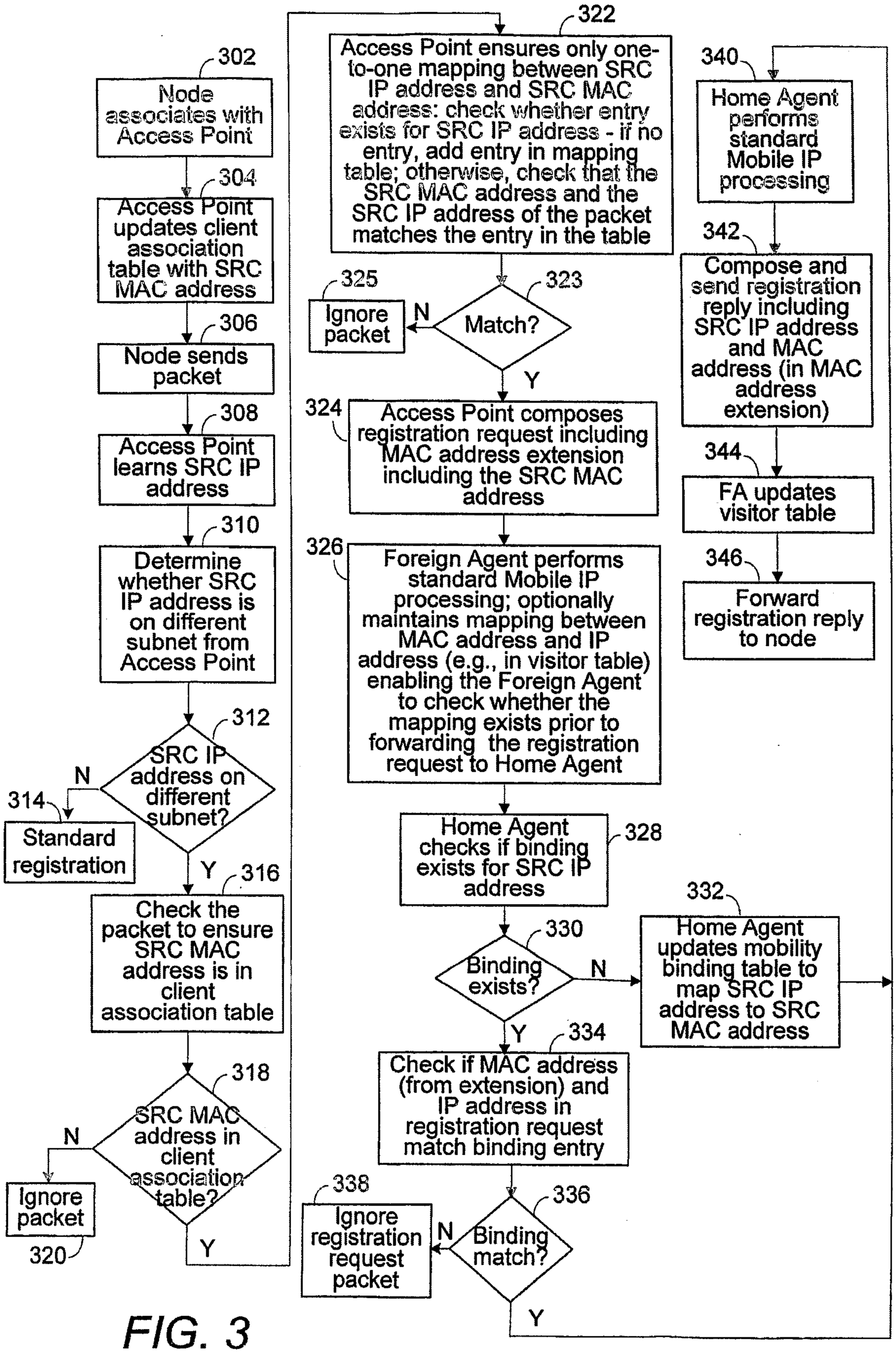

302
Node associates with Access Point
304
Access Point updates client association table with SRC MAC address
306
Node sends packet
308
Access Point learns SRC IP address
310
Determine whether SRC IP address is on different subnet from Access Point
312
SRC IP address on different subnet?
N
314
Standard registration
Y
316
Check the packet to ensure SRC MAC address is in client association table
318
SRC MAC address in client association table?
N
Ignore packet
320
Y
322
Access Point ensures only one-to-one mapping between SRC IP address and SRC MAC address: check whether entry exists for SRC IP address - if no entry, add entry in mapping table; otherwise, check that the SRC MAC address and the SRC IP address of the packet matches the entry in the table
325
Ignore packet
N
323
Match?
Y
324
Access Point composes registration request including MAC address extension including the SRC MAC address
326
Foreign Agent performs standard Mobile IP processing; optionally maintains mapping between MAC address and IP address (e.g., in visitor table) enabling the Foreign Agent to check whether the mapping exists prior to forwarding the registration request to Home Agent
Home Agent checks if binding exists for SRC IP address
328
330
Binding exists?
N
332
Home Agent updates mobility binding table to map SRC IP address to SRC MAC address
Y
334
Check if MAC address (from extension) and IP address in registration request match binding entry
336
Binding match?
N
338
Ignore registration request packet
Y
340
Home Agent performs standard Mobile IP processing
342
Compose and send registration reply including SRC IP address and MAC address (in MAC address extension)
344
FA updates visitor table
346
Forward registration reply to node

FIG. 3

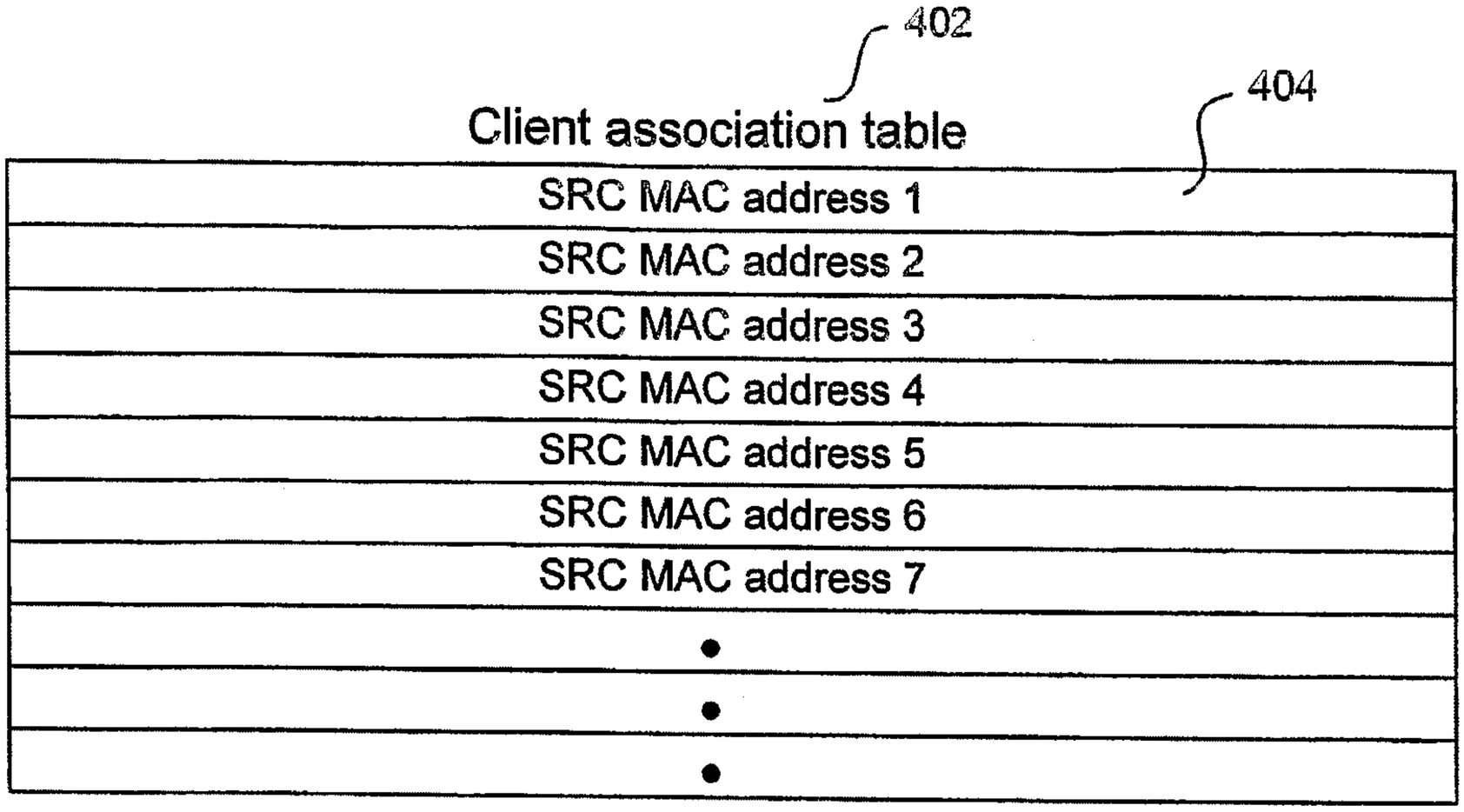

402
404
Client association table
SRC MAC address 1
SRC MAC address 2
SRC MAC address 3
SRC MAC address 4
SRC MAC address 5
SRC MAC address 6
SRC MAC address 7

FIG. 4

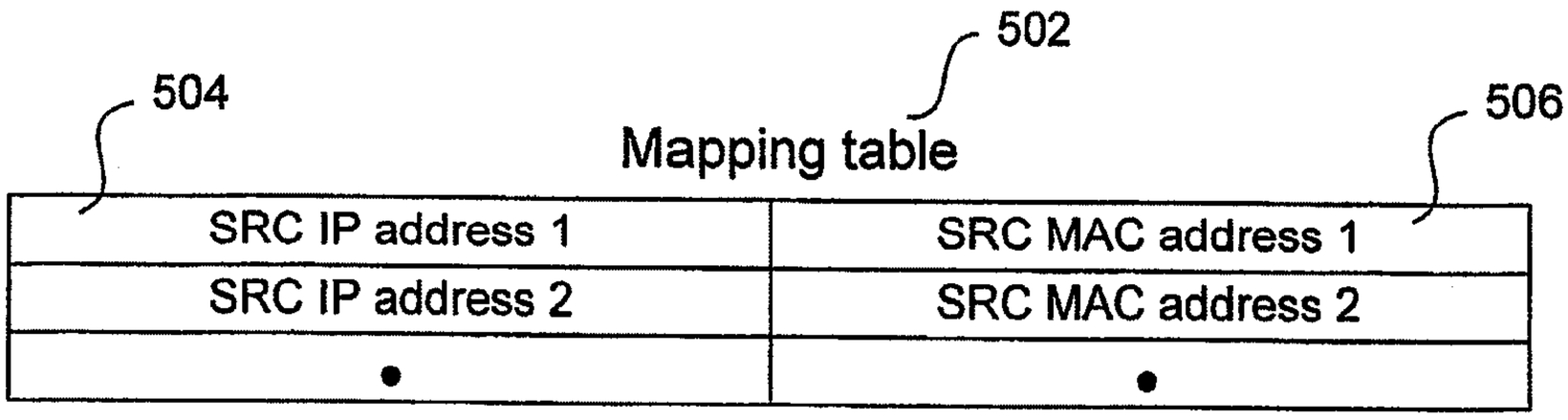

502
504
506
Mapping table
SRC IP address 1
SRC MAC address 1
SRC IP address 2
SRC MAC address 2

FIG. 5

602

Mobility binding table

604 SRC IP address (Home address)	606 SRC MAC address	608 Care-of address	610 Tunnel interface

FIG. 6

702

Visitor table

704 SRC IP address (Home address)	706 SRC MAC address	708 Home Agent address	710 Tunnel interface

FIG. 7

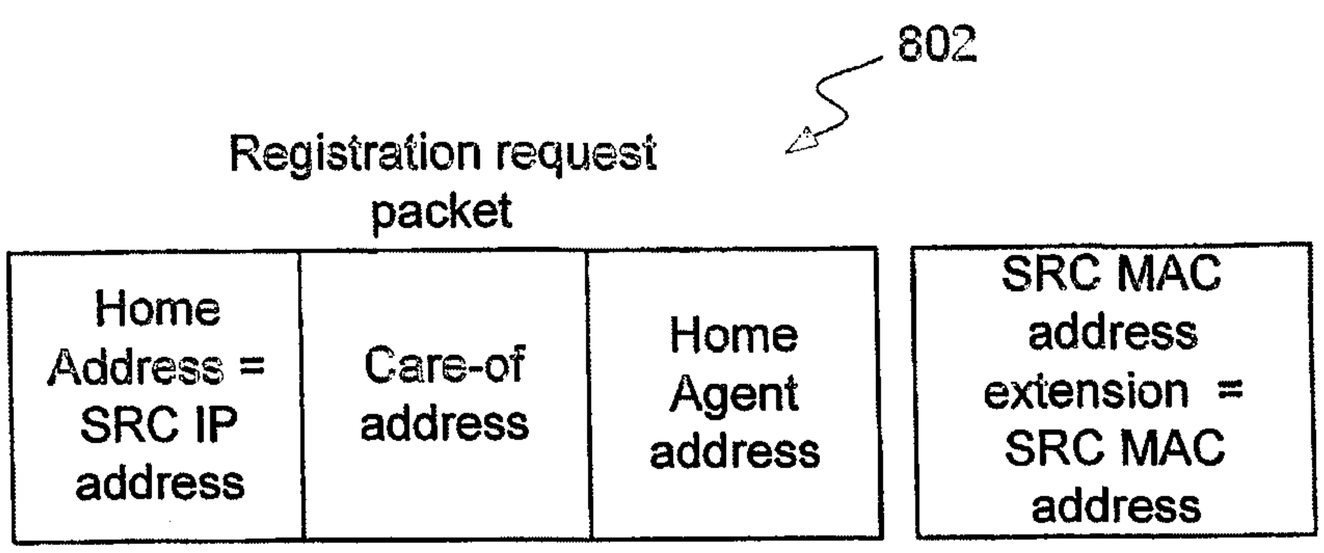

802
Registration request packet
Home Address = SRC IP address
Care-of address
Home Agent address
SRC MAC address extension = SRC MAC address

FIG. 8

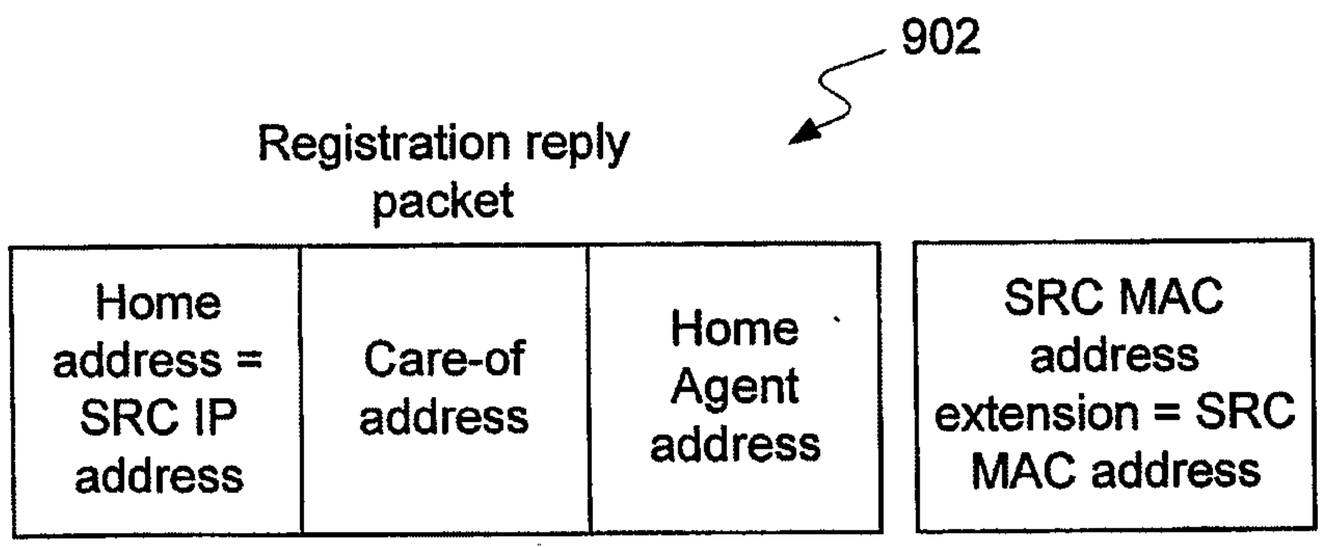

902
Registration reply packet
Home address = SRC IP address
Care-of address
Home Agent address
SRC MAC address extension = SRC MAC address

FIG. 9

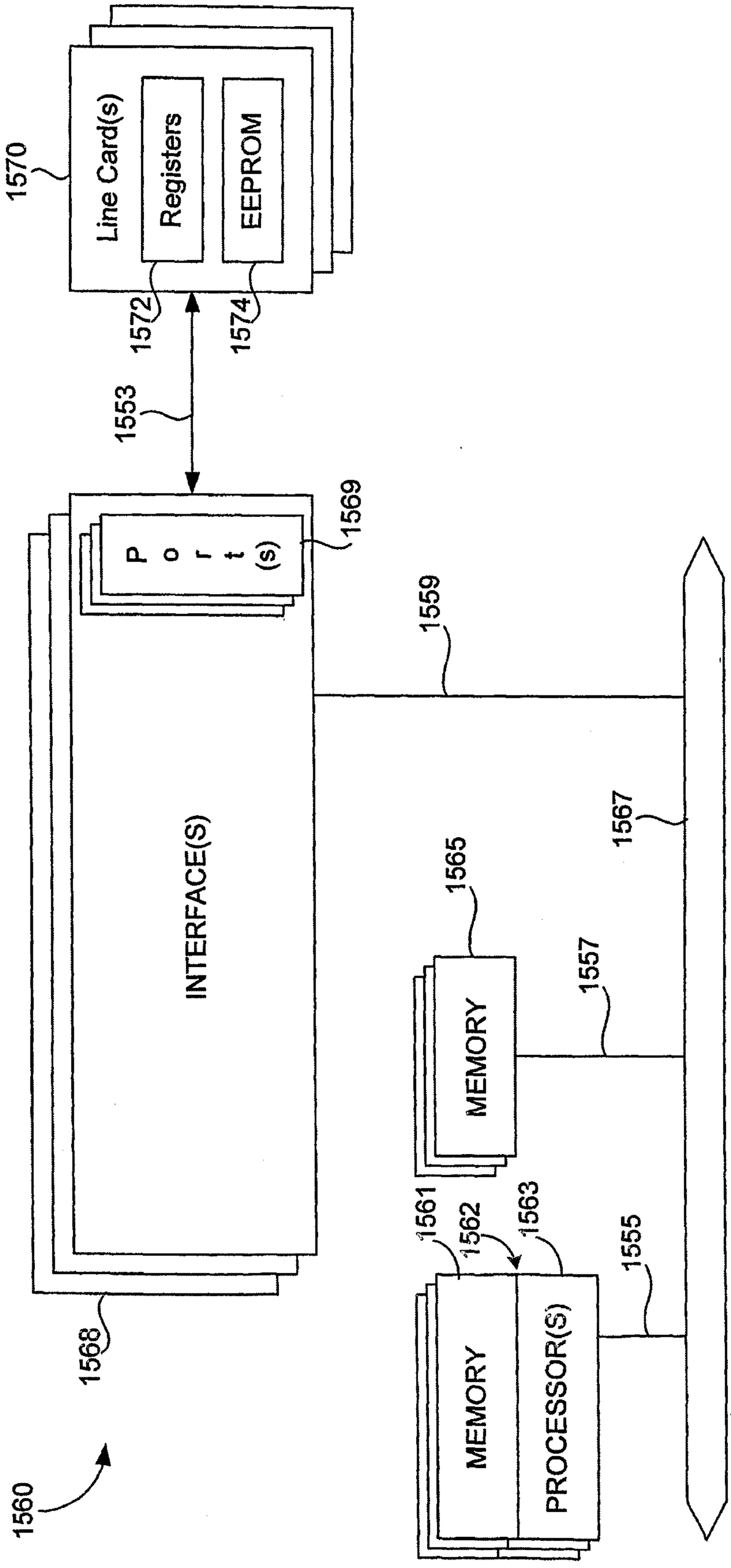
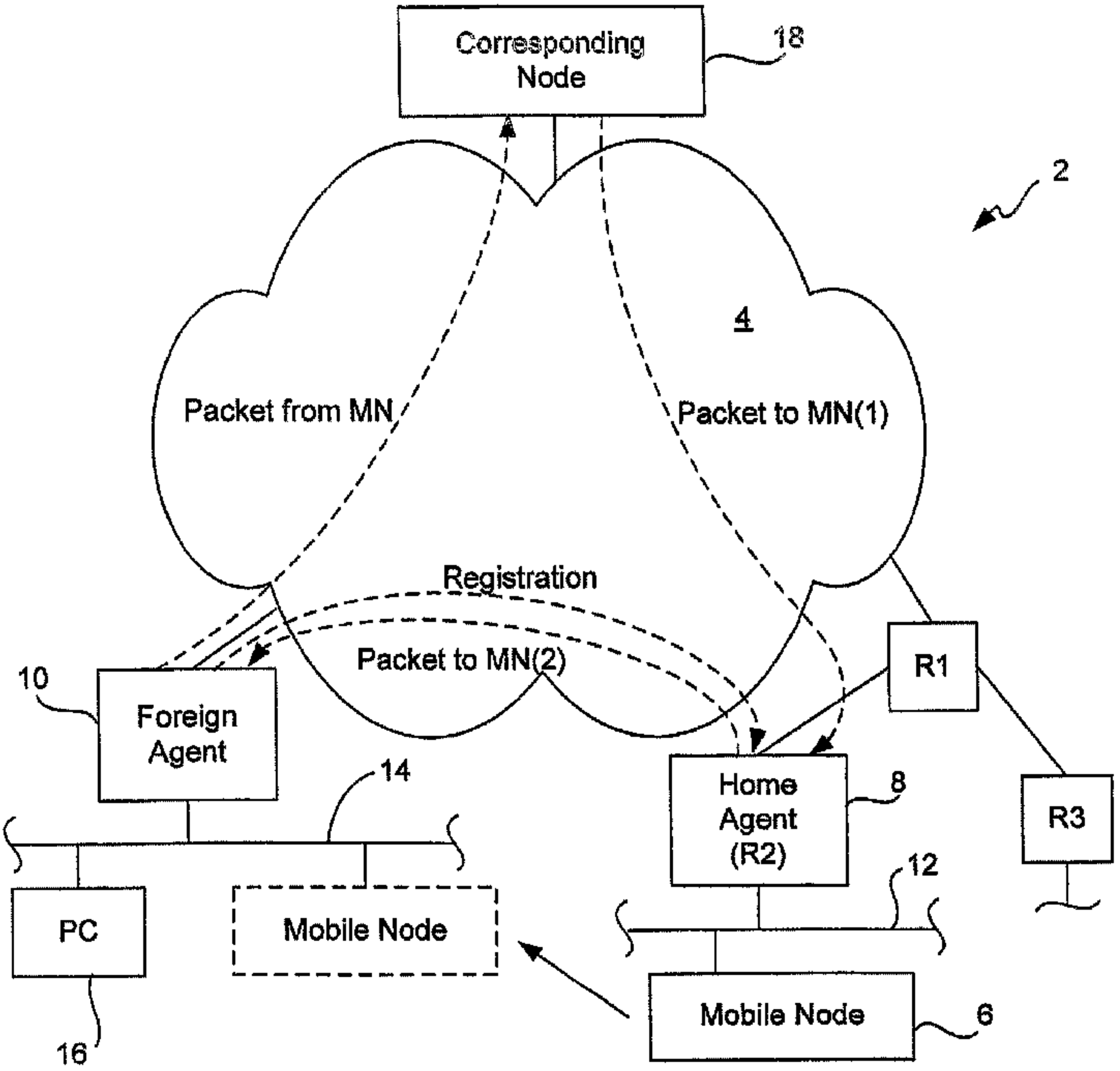

1570
Line Card(s)
Registers
EEPROM
1572
1574
1553
1569
Port(s)
1559
INTERFACE(S)
1565
MEMORY
1567
1557
1561
1562
1563
MEMORY
PROCESSOR(S)
1555
1568
1560

FIG. 10


Corresponding Node
18
2
4
Packet from MN
Packet to MN(1)
Registration
Packet to MN(2)
10
Foreign Agent
14
R1
Home Agent (R2)
8
R3
12
PC
Mobile Node
16
Mobile Node
6