US 20040190534A1

(19) **United States**
(12) **Patent Application Publication** (10) **Pub. No.: US 2004/0190534 A1**
Adrangi et al. (43) **Pub. Date: Sep. 30, 2004**

(54) **METHOD, APPARATUS AND SYSTEM FOR ENSURING RELIABLE ACCESS TO A ROAMING MOBILE NODE**

(76) Inventors: **Farid Adrangi**, Lake Oswego, OR (US); **Ranjit S. Narjala**, Hillsboro, OR (US); **Michael Andrews**, Beaverton, OR (US)

Correspondence Address:
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030 (US)

(21) Appl. No.: **10/401,896**

(22) Filed: **Mar. 28, 2003**

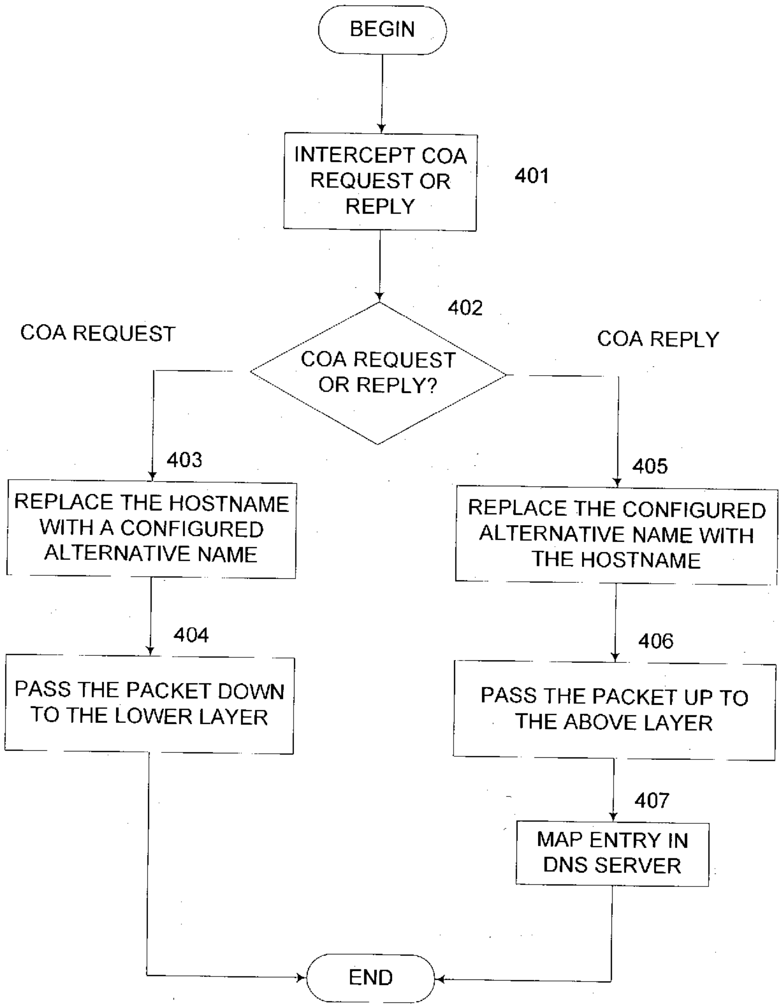
Publication Classification

(51) **Int. Cl.**^{7} **H04L 12/56**

(52) **U.S. Cl.** **370/400**; 370/338; 370/252

(57) **ABSTRACT**

A method, apparatus and system provide reliable access to a mobile node. Requests for care of addresses (COAs) are intercepted and the mobile node hostnames in the requests are replaced with alternative configured names. These altered requests are then passed down the network stack. Similarly, replies to the COA requests are also intercepted and the alternative configured names may be replaced with the mobile node hostnames. These replies may then be passed up the network stack. A mobile IP registration request extension may be used to create a mapping entry in a Domain Name Services (DNS) server between the mobile node hostname and the mobile node home address. This mapping entry ensures that the mobile node is consistently reachable via its hostname.


BEGIN
INTERCEPT COA REQUEST OR REPLY
401
402
COA REQUEST
COA REQUEST OR REPLY?
COA REPLY
403
REPLACE THE HOSTNAME WITH A CONFIGURED ALTERNATIVE NAME
405
REPLACE THE CONFIGURED ALTERNATIVE NAME WITH THE HOSTNAME
404
PASS THE PACKET DOWN TO THE LOWER LAYER
406
PASS THE PACKET UP TO THE ABOVE LAYER
407
MAP ENTRY IN DNS SERVER
END

Google Exhibit 1039
Google v. VirtaMove

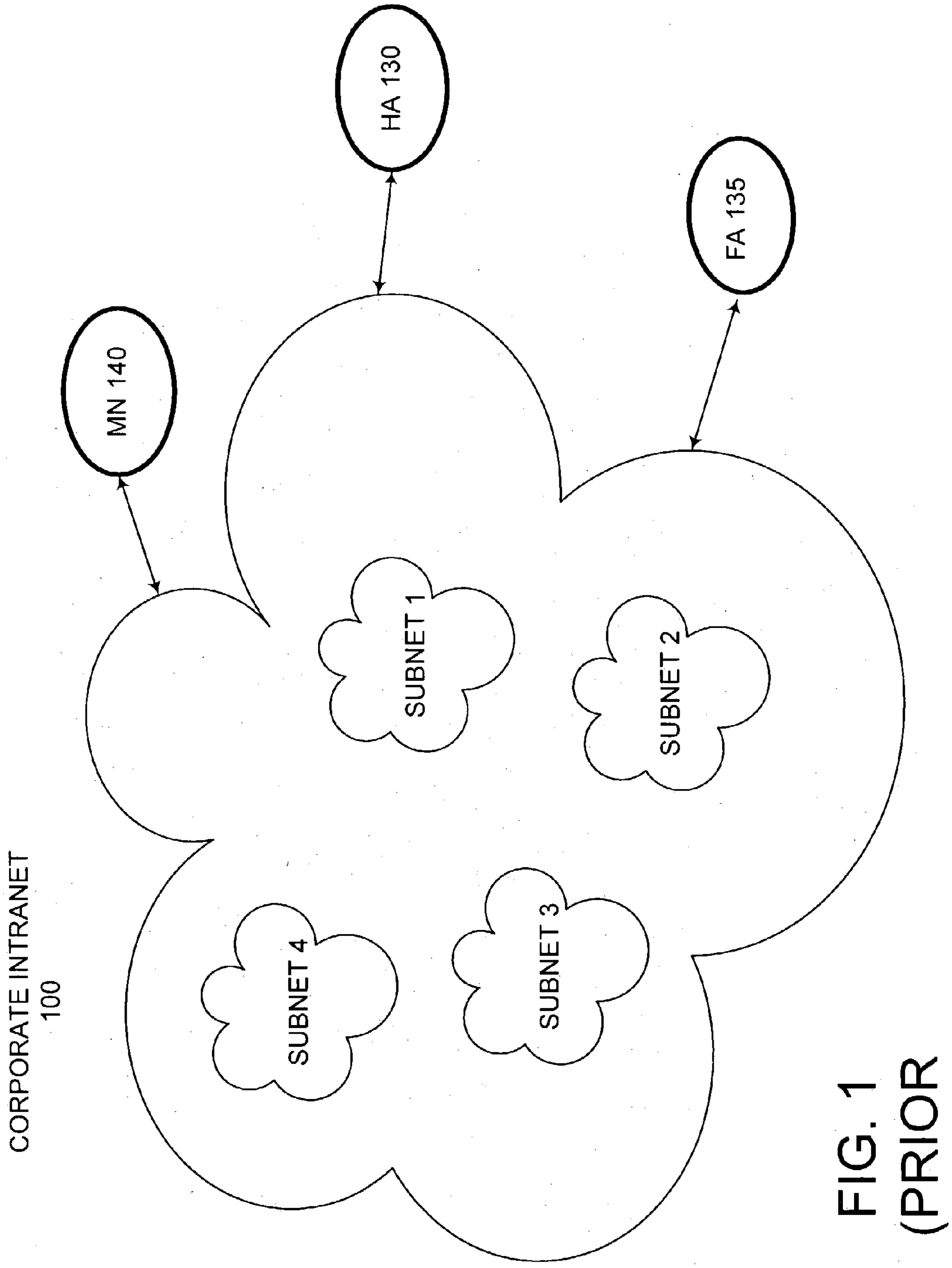
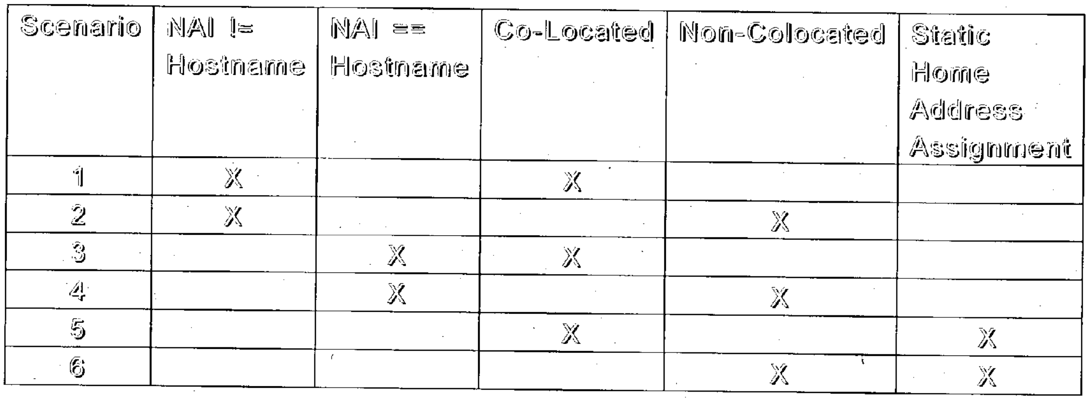


FIG. 1
(PRIOR
ART)



Scenario	NAI != Hostname	NAI == Hostname	Co-Located	Non-Colocated	Static Home Address Assignment
1	X		X		
2	X			X	
3		X	X		
4		X		X	
5			X		X
6				X	X

FIG. 2

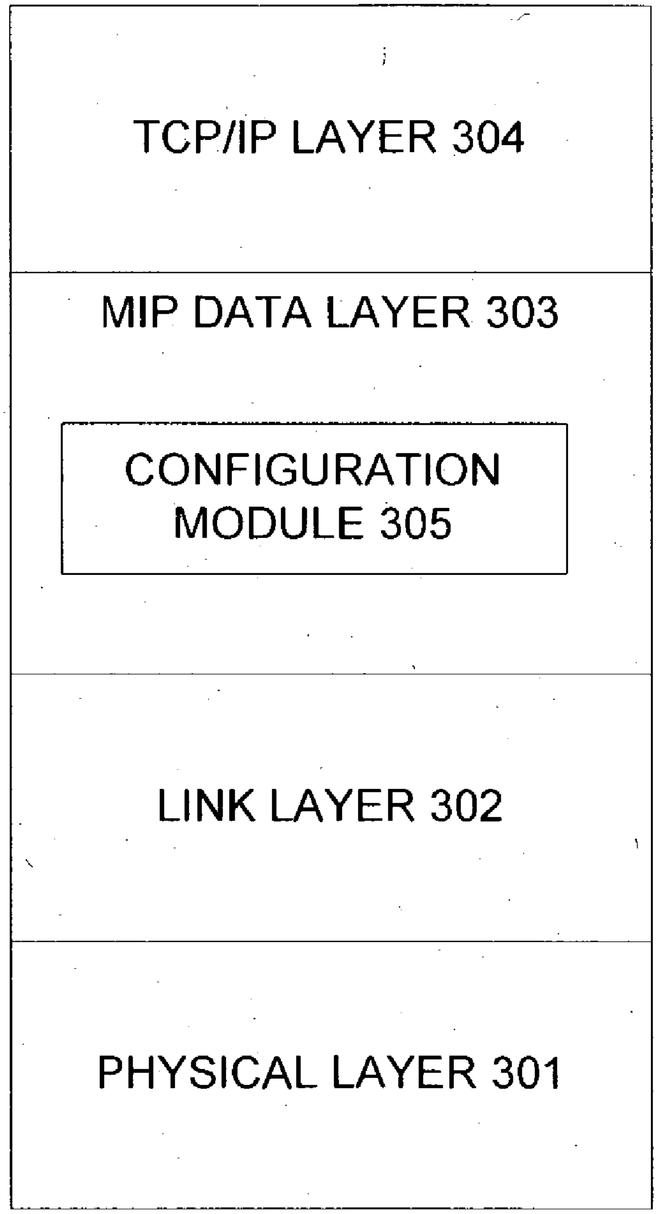

TCP/IP LAYER 304
MIP DATA LAYER 303
CONFIGURATION MODULE 305
LINK LAYER 302
PHYSICAL LAYER 301

FIG. 3

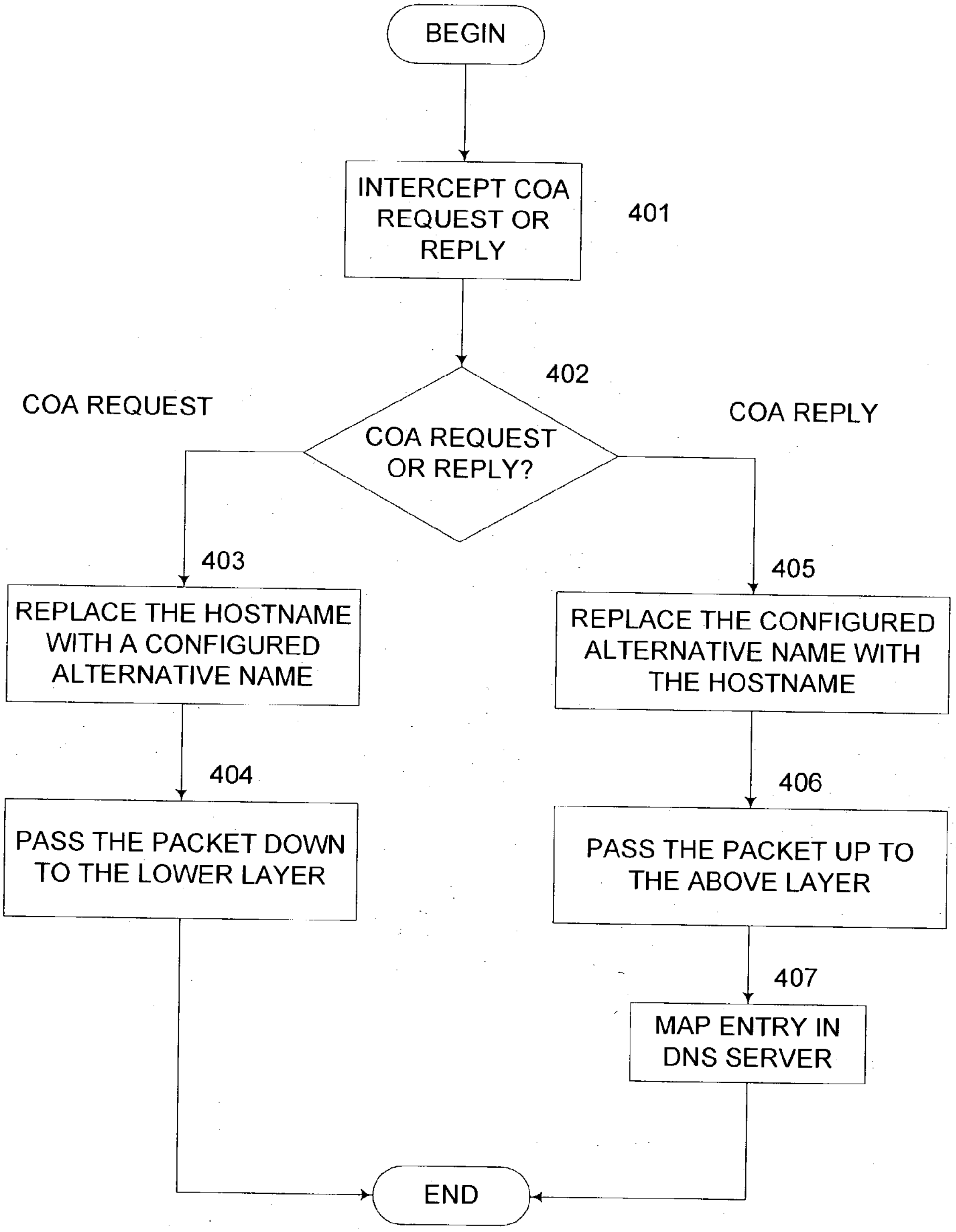

BEGIN
INTERCEPT COA REQUEST OR REPLY
401
402
COA REQUEST
COA REQUEST OR REPLY?
COA REPLY
403
REPLACE THE HOSTNAME WITH A CONFIGURED ALTERNATIVE NAME
405
REPLACE THE CONFIGURED ALTERNATIVE NAME WITH THE HOSTNAME
404
PASS THE PACKET DOWN TO THE LOWER LAYER
406
PASS THE PACKET UP TO THE ABOVE LAYER
407
MAP ENTRY IN DNS SERVER
END

FIG. 4

METHOD, APPARATUS AND SYSTEM FOR ENSURING RELIABLE ACCESS TO A ROAMING MOBILE NODE

FIELD OF THE INVENTION

[**0001**] The present invention relates to the field of mobile computing, and, more particularly to a method, apparatus and system for ensuring reliable access to a roaming mobile node.

BACKGROUND OF THE INVENTION

[**0002**] A hostname is a unique name by which a computing device may be identified on a network. Hostnames are used to simplify access to computing devices by enabling users to use unique names instead of addresses to access these devices. A hostname is typically translated into an Internet address by a Domain Name System (DNS) server.

[**0003**] Use of hostnames in mobile computing environments has introduced additional considerations. As mobile computing devices (hereafter mobile nodes) become increasingly popular, various protocols have been developed to address mobile computing requirements. For example, to enable mobile node users to move from one location to another (roam) while continuing to maintain their connectivity to the same network, the Internet Engineering Task Force (IETF) has promulgated roaming standards (Mobile IPv4, IETF RFC 3344, August 2002, hereafter Mobile IPv4, and Mobile IPv6, IETF Mobile IPv6, Internet Draft draft-ietf-mobileip-ipv6-19.txt. (Work In Progress), October 2002, hereafter Mobile IPv6).

[**0004**] Mobile IPv4 is currently the predominant standard, and many networks today are Mobile IPv4 compliant. Mobile IPv4 introduced the concept of Network Access Identifiers (NAIs). NAIs may be used in either Mobile IPv4 or Mobile IPv6 compliant networks to uniquely identify a mobile node. While a mobile node is typically identified by one hostname, it may also be associated with more than one NAI. Similar to hostnames, NAIs may also be translated into an Internet address by a DNS server.

BRIEF DESCRIPTION OF THE DRAWINGS

[**0005**] The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings in which like references indicate similar elements, and in which:

[**0006**] **FIG. 1** illustrates a known corporate intranet structure today;

[**0007**] **FIG. 2** is a table illustrating the various ways in which MN **140** may be configured;

[**0008**] **FIG. 3** illustrates a Mobile IP network stack according to embodiments of the present invention; and

[**0009**] **FIG. 4** is a flow chart illustrating an embodiment of the present invention.

DETAILED DESCRIPTION

[**0010**] Embodiments of the present invention provide a method, apparatus and system for reliably accessing a roaming mobile node. Reference in the specification to one embodiment or an embodiment of the present invention means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the phrases in one embodiment, according to one embodiment or the like appearing in various places throughout the specification are not necessarily all referring to the same embodiment.

[**0011**] **FIG. 1** illustrates a known corporate intranet (Corporate Intranet **100**) structure. Corporate Intranet **100** may include both wired and wireless networks and may comprise multiple subnets. Subnets refer to portions of networks that may share the same common address format. For example, on a Transport Control Protocol/Internet Protocol (TCP/IP) network, all subnets may use the same first three sets of numbers (such as 100.10.10).

[**0012**] As previously described, a mobile node (hereafter MN **140**) may have a hostname and a NAI associated with it. Mobile nodes that conform to Mobile IPv4 and/or Mobile IPv6 standards (hereafter collectively referred to as Mobile IP Standards) today may roam freely across subnets within Corporate Intranet **100**. When MN 140 exits its home subnet, it may continue to maintain its current transport connections and constant reachability in one of two ways. In the first scenario, MN **140** may register with a home agent (HA **130**) when it exits its home subnet. During the registration process, MN **140** informs HA **130** of MN **140** s care-of address (hereafter COA), namely MN **140** s address on its new subnet. HA **130** thereafter intercepts all IP packets addressed to MN **140** and reroutes the packets to MN **140** s COA. As MN **140** moves from one subnet to another, MN **140** may obtain new COAs via Dynamic Host Configuration Protocol (DHCP) or other similar protocols. To ensure that HA **130** is able to properly route packets to MN **140**, MN **140** must continuously update HA **130** with its new COA as it roams on Corporate Intranet **100**. This configuration is commonly referred to as a co-located communications mode.

[**0013**] Alternatively, in Mobile IPv4 compliant networks, when MN **140** leaves its home subnet, it may register with HA **130** via a foreign agent (FA **135**) on MN **140** s new (foreign) subnet. By registering with FA **135**, MN **140** may use FA **135** s IP address as its COA when registering with HA **130**. In this scenario, HA **130** continues to intercept all packets addressed to MN **140**, but these packets are now rerouted to FA **135**, namely MN **140** s COA as provided to HA **130**. FA **135** examines all packets it receives, and sends the appropriate ones to MN **140** at its current location on the foreign subnet. This configuration is commonly referred to as a non co-located communications mode. The decision of whether to use co-located or non co-located mode is well known to those of ordinary skill in the art. Certain networks may, for example, force MN **140** to register with FA **135** in order to maintain its transport connections. In other networks, MN **140** may have the option of registering with FA **135** or operating in a co-located mode.

[**0014**] In summary, when MN **140** is roaming across subnets, it may have associated with it: (i) a hostname; (ii) a NAI; (iii) an invariant home address; and (iv) a COA. As will be readily apparent to those of ordinary skill in the art, these multiple identifiers for MN **140** may cause inconsistencies as MN **140** roams. Details of these inconsistencies are described below.

[**0015**] **FIG. 2** is a table illustrating the various ways in which MN **140** may be configured to conform to Mobile

IPv4 standards. As illustrated, the mobile node may be configured according to one of six scenarios. In Scenario 1, MN **140** in a co-located mode may be assigned a NAI that is different from its hostname. When MN **140** obtains its COA (e.g., via DHCP or other similar protocols), a mapping entry may be created in a DNS server, mapping the COA to MN **140** s hostname {Hostname, COA}. This COA may change continuously as MN **140** roams across subnets. Additionally, MN **140** may be configured to obtain its home address through a NAI extension in its registration request to HA **130**. HA **130** may issue a home address to MN **140** from HA **130** s IP address pool or by requesting the home address from a DHCP server via a DHCP (or other similar protocol) request. In the latter instance, in response to HA **130** s request, the DHCP server may issue MN **140** a home address and send the DNS server an update to create a mapping entry in the DNS server {NAI, MN_H}. As previously described, a correspondent node (CN) may attempt to reach MN **140** using its NAI and/or hostname. In Scenario 1 above, however, if CN tries to access MN **140** using MN **140** s hostname, instead of being resolved to MN **140** s home address, the hostname is resolved to MN **140** s COA. Since this communication is not routed via HA **130** that is responsible for maintaining MN **140** s mobile connectivity, MN **140** may not be reached reliably via its hostname.

[**0016**] In Scenario 2, Mobile Node **140** in a non co-located mode may be assigned a NAI that is different from its hostname. MN **140** may again be configured to obtain its home address through a NAI registration, resulting in a mapping entry in the DNS server {NAI, MN_H}. In this non co-located scenario, however, MN **140** may use FA **135** s address as its COA when registering with HA **130**. Thus, unlike Scenario 1, MN **140** does not acquire a COA, which would result in a mapping between the hostname and the COA in the DNS server. As a result, there may not be a mapping entry at all for MN **140** s hostname in the DNS server, and CN may not reach MN **140** via its hostname. In addition, although this scenario does not trigger a mapping entry for MN **140** s hostname in the DNS Server, the DNS Server may nonetheless still include a stale entry in its binding table (e.g., MN **140** s hostname may still be mapped to an old COA from a previous configuration). In this situation, when CN that attempts to reach MN **140** via its hostname, the hostname will be resolved in the DNS Server to the stale COA, resulting in CN not being able to reach MN **140**.

[**0017**] According to Scenario 3, MN **140** in a co-located mode may be assigned a NAI that is the same as its hostname. As described above in Scenario 1, the DNS server may include mappings for {NAI, MN H} and {Hostname, COA}. In this situation, however, since the NAI and hostname are the same, the mapping in the DNS server may be unpredictable due to an IP address contention between MN **140** s hostname and NAI. The mappings may override each other, given the order in which the mappings are entered into the DNS server. As a result, access to MN **140** via either its hostname or NAI is likely to be unpredictable, at best.

[**0018**] In Scenario 4, MN **140** in a non co-located mode is assigned a NAI that is the same as its hostname. This scenario does not introduce any problems because, as described in Scenario 2 above, the NAI is mapped in the DNS server to MN **140** s invariant home address {NAI, MN_H}. In this situation, however, since the NAI is the same as the hostname, regardless of the fact there is no mapping for the hostname, MN **140** will nonetheless be reachable. In other words, a CN that attempts to reach MN **140** using its hostname will enter the same name as MN **140** s NAI, which will be resolved in the DNS server to MN_H.

[**0019**] In Scenario 5, MN **140** in a co-located mode may be assigned a static home address (e.g., by a corporate IT department), and a mapping may also be created in the DNS server {Hostname, MN_H}. As MN **140** roams and obtains a COA, however, a second entry may also be created in the DNS server {Hostname, COA}. The two mappings for MN **140** s hostname result in an IP address contention for the hostname. More specifically, the second mapping for hostname may overwrite the first, leaving the {Hostname, COA} mapping in the DNS server. As a result, as described in Scenario 1 above, MN **140** may no longer be reachable reliably using its hostname because the hostname may be mapped to MN **140** s COA.

[**0020**] In the final scenario, Scenario 6, MN **140** in a non co-located mode may be assigned a static home address, resulting in a mapping entry in the DNS server for {Hostname, MN_H}. As is readily apparent to those of ordinary skill in the art, this scenario presents no problems because, in a non co-located mode, no other mapping entry is created for MN **140** in the DNS server. CN may therefore reach MN **140** reliably via its hostname.

[**0021**] In summary, Scenarios 1, 2, 3 and 5 above result in various accessibility problems for MN **140** while it roams from subnet to subnet. Embodiments of the present invention resolve these problems by using a configured alternative name. More specifically, in embodiments of the invention, DHCP requests for COAs from MN **140** and replies to such requests are intercepted within MN **140** and replaced with configured alternative names and hostnames respectively. This eliminates a hostname mapping to COAs in the DNS server, thus eliminating the problems described above. This concept of using a configured alternative name is described in further detail below, in relation to **FIG. 3**.

[**0022**] **FIG. 3** illustrates a Mobile IP network stack on MN **140** according to embodiments of the present invention. The concepts of network stacks and passing messages up and down network stacks are well known to those of ordinary skill in the art and further description thereof is omitted herein in order not to unnecessarily obscure the present invention. As illustrated, the mobile IP layer (MIP Data Layer **303**) intercepts DHCP requests that are sent by MN **140** to acquire a COA (hereafter referred to as COA Requests). Instead of directly routing the request down the network stack (i.e., to Link Layer **302** and Physical Layer **301**), however, according to one embodiment of the present invention, Configuration Module **305** (illustrated conceptually as being contained within MIP Data Layer **303**) may replace MN **140** s hostname in the COA request with a configured alternative name. This configured alternative name may then be passed down the network stack to Link Layer **302** and Physical Layer **301**. In one embodiment, the COA request is a DHCP request and a DHCP server may process the request and send back a DHCP reply with a COA assignment (hereafter referred to as COA Reply). Upon receipt of this COA Reply, Configuration Module **305** may replace the configured alternative name in the reply with the actual hostname, and pass the COA Reply up the network stack, to TCP/IP Layer **304**.

[0023] As will be readily apparent to those of ordinary skill in the art, by intercepting and modifying the COA Requests and COA Replies according to the embodiments described above, MN **140** s hostname may no longer be mapped to its COA in the DNS server. Therefore, in order to ensure that there is some mapping for MN **140** s hostname in the DNS server, in one embodiment of the present invention, a new registration request extension (Hostname Extension) may be used. Hostname Extension may be created per the guidelines specified in the Mobile IPv4 standard, and may be configured to inform HA **130** to request creation of a mapping entry between MN **140** s hostname and MN s home address in the DNS server {Hostname, MN_H}. In this manner, HA **130** may ensure that MN **140** s hostname is consistently mapped to MN **140** s home address in the DNS server. MN **140** s NAI continues to be mapped to MN **140** s home address {NAI, MN_H}. According to one embodiment of the present invention, these two mappings enable MN **140** to be reachable via both its hostname and NAI, regardless of whether the hostname and the NAI are the same.

[0024] **FIG. 4** is a flow chart illustrating an embodiment of the present invention. Although the following operations may be described as a sequential process, many of the operations may in fact be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged without departing from the spirit of embodiments of the invention. In **401**, a COA Request or COA Reply may be intercepted. The request and/or reply may be examined in **402**. In the case of a COA Request, the mobile node hostname in the request may be replaced by a configured alternative name in **403** and passed down the network stack in **404**. Alternatively, in the case of a COA Reply, in **405** the configured alternative name may be replaced by the mobile node hostname and the reply may be passed up the network stack in **406**. Additionally, at any point prior to, during or after these events, the mobile node s home agent may request creation of a mapping entry in the DNS server in **407**, mapping the mobile node s hostname to the mobile node s home address.

[0025] The mobile nodes, home agents and foreign agents according to embodiments of the present invention may be implemented on a variety of data processing devices. It will be readily apparent to those of ordinary skill in the art that these data processing devices may include various software, and may comprise any devices capable of supporting mobile networks, including but not limited to mainframes, workstations, personal computers, laptops, portable handheld computers, PDAs and/or cellular telephones. In an embodiment, mobile nodes may comprise portable data processing systems such as laptops, handheld computing devices, personal digital assistants and/or cellular telephones. According to one embodiment, home agents and/or foreign agents may comprise data processing devices such as personal computers, workstations and/or mainframe computers. In alternate embodiments, home agents and foreign agents may also comprise portable data processing systems similar to those used to implement mobile nodes.

[0026] According to embodiment of the present invention, data processing devices may include various components capable of executing instructions to accomplish an embodiment of the present invention. For example, the data processing devices may include and/or be coupled to at least one machine-accessible medium. As used in this specification, a machine includes, but is not limited to, any data processing device with one or more processors. As used in this specification, a machine-accessible medium includes any mechanism that stores and/or transmits information in any form accessible by a data processing device, the machine-accessible medium including but not limited to, recordable/non-recordable media (such as read only memory (ROM), random access memory (RAM), magnetic disk storage media, optical storage media and flash memory devices), as well as electrical, optical, acoustical or other form of propagated signals (such as carrier waves, infrared signals and digital signals).

[0027] According to an embodiment, a data processing device may include various other well-known components such as one or more processors. The processor(s) and machine-accessible media may be communicatively coupled using a bridge/memory controller, and the processor may be capable of executing instructions stored in the machine-accessible media. The bridge/memory controller may be coupled to a graphics controller, and the graphics controller may control the output of display data on a display device. The bridge/memory controller may be coupled to one or more buses. A host bus host controller such as a Universal Serial Bus (USB) host controller may be coupled to the bus(es) and a plurality of devices may be coupled to the USB. For example, user input devices such as a keyboard and mouse may be included in the data processing device for providing input data.

[0028] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be appreciated that various modifications and changes may be made thereto without departing from the broader spirit and scope of embodiments of the invention, as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

What is claimed is:

1. A method for ensuring reliable access to a mobile node, comprising:

intercepting a a care of address (COA) request, the COA request including a mobile node hostname;

replacing the mobile node hostname in the COA request with an alternative configured name; and

transmitting the COA request with the alternative configured name to a server.

2. The method according to claim 1 further comprising:

intercepting a COA reply from the server, the COA reply including the alternative configured name;

replacing the alternative configured name with the mobile node hostname; and

transmitting the COA reply with the mobile node hostname to the mobile node.

3. The method according to claim 2 further comprising transmitting a registration request to map an entry for the mobile node hostname and the mobile node home address in a Domain Name Services (DNS) server.

4. The method according to claim 3 wherein transmitting the registration request comprises transmitting a Mobile IP registration request with a hostname extension.

5. The method according to claim 1 wherein the server comprises a dynamic host control protocol (DHCP) server and the COA request includes a DHCP request.

6. A system for ensuring reliable access to a mobile node, comprising:

a mobile node capable of transmitting a care of address (COA) request, the COA request including a mobile node hostname;

a configuration module capable of intercepting the COA request and replacing the mobile node hostname with an alternative configured name, the configuration module further capable of retransmitting the COA request; and

a server capable of receiving the COA request.

7. The system according to claim 6 wherein the server is further capable of responding to the COA request and transmitting a COA reply to the mobile node wherein the reply includes the alternative configured name.

8. The system according to claim 7 wherein the configuration module is further capable of intercepting the COA reply and replacing the alternative configured name with the mobile node hostname, the configuration module additionally capable of transmitting the COA reply with the mobile node hostname to the mobile node.

9. The system according to claim 6 further comprising a Domain Name Services (DNS) server capable of mapping an entry for the mobile node hostname and the mobile node home address.

10. The system according to claim 6 wherein the server comprises a dynamic host control protocol (DHCP) server, and the COA request comprises a DHCP request.

11. The system according to claim 6 wherein the mobile node includes the configuration module.

12. A system for ensuring reliable access to a mobile node, comprising:

a mobile node capable of transmitting a care of address (COA) request, the COA request including a mobile node hostname; and

a configuration module capable of intercepting the COA request and replacing the mobile node hostname with an alternative configured name, the configuration module further capable of retransmitting the COA request to a server.

13. The system according to claim 12 wherein the configuration module is capable of intercepting a COA reply from the server wherein the COA reply includes the alternative configured name, the configuration module further capable of replacing the alternative configured name with the mobile node hostname, the configuration module additionally capable of transmitting the COA reply with the mobile node hostname to the mobile node.

14. The system according to claim 12 wherein the server comprises a dynamic host control protocol (DHCP) server, and the COA request comprises a DHCP request.

15. The system according to claim 12 wherein the mobile node includes the configuration module.

16. An apparatus for ensuring reliable access to a mobile node, comprising:

a configuration module capable of intercepting a care of address (COA) request from the mobile node wherein the COA request includes a mobile node hostname, the configuration module further capable of replacing the mobile node hostname with an alternative configured name and retransmitting the COA request.

17. The apparatus according to claim 16 wherein the configuration module is capable of intercepting a COA reply, and wherein the COA reply includes the alternative configured name, the configuration module further capable of replacing the alternative configured name with the mobile node hostname, the configuration module additionally capable of retransmitting the COA reply with the mobile node hostname to the mobile node.

18. An article comprising a machine-accessible medium having stored thereon instructions that, when executed by a machine, cause the machine to:

intercept a care of address (COA) request from the mobile node, the COA request including a mobile node hostname;

replace the mobile node hostname with an alternative configured name; and

transmit the COA request with the alternative configured name to a server.

19. The article according to claim 18 wherein the instructions, when executed by the machine, further cause the machine to:

intercept a COA reply from the server wherein the reply COA includes the alternative configured name;

replace the alternative configured name with the mobile node hostname; and

transmit the COA reply with the mobile node hostname to the mobile node.

20. The article according to claim 19 wherein the instructions, when executed by the machine, further cause the machine to transmit a registration request to map an entry for the mobile node hostname and the mobile node home address in a Domain Name Services (DNS) server.

21. The article according to claim 20 wherein the instructions, when executed by the machine, further cause the machine to transmit a Mobile IP registration request with a hostname extension.

22. The article according to claim 19 wherein the server comprises a dynamic host control protocol (DHCP) server and the COA request includes a DHCP request.

* * * * *