John B. Sganga, Jr. (SBN 116,211)
john.sganga@kmob.com
Douglas G. Muehlhauser (SBN 179,495)
doug.muehlhauser@kmob.com
Perry D. Oldham (SBN 216,016)
perry.oldham@kmob.com
Mark Lezama (SBN 253,479)
mark.lezama@kmob.com
Alan G. Laquer (SBN 259,257)
alan.laquer@kmob.com
KNOBBE, MARTENS, OLSON & BEAR, LLP
2040 Main Street
Fourteenth Floor
Irvine, CA 92614
Phone: (949) 760-0404
Facsimile: (949) 760-9502

Attorneys for Plaintiff
NOMADIX, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

CV10-0381 AHM (CWx)

NOMADIX, INC.,
a Delaware corporation,

Plaintiff,

v.

SOLUTIONINC TECHNOLOGIES LIMITED,
a Canadian corporation,

Defendant.

Civil Action No.

COMPLAINT FOR PATENT INFRINGEMENT OF U.S. PATENT NOS. 6,130,892, 7,088,727, 7,554,995, 6,636,894, 7,194,554, 6,868,399, AND 6,857,009

DEMAND FOR JURY TRIAL

Plaintiff Nomadix, Inc. ("Nomadix") hereby complains of Defendant SolutionInc Technologies Limited ("SolutionInc") and alleges as follows:

JURISDICTION AND VENUE

1. This Complaint states causes of action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 100 *et seq.*, and, more particularly, 35 U.S.C. §§ 271 and 281. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

2. Upon information and belief, SolutionInc conducts business throughout the United States, including in this judicial district, and has committed the acts complained of in this judicial district and elsewhere.

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b) and (c) and 1400(b).

PARTIES

4. Nomadix is a Delaware corporation having its principal place of business at 30851 Agoura Road, Suite 102, Agoura Hills, California 91301.

5. Upon information and belief, SolutionInc Technologies Limited is a Canadian corporation having its principal place of business at 5692 Bloomfield Street, Halifax, Nova Scotia, B3K 1T2, Canada.

ALLEGATIONS FOR ALL CLAIMS OF RELIEF

6. On October 10, 2000, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 6,130,892 ("the '892 patent"), titled "Nomadic Translator or Router." Nomadix owns the '892 patent by assignment. A copy of the '892 patent is attached hereto as Exhibit 1. Reexamination of the '892 patent was requested on or around February 15, 2005, and the ensuing reexamination resulted in confirmation of the patentability, without amendment, of Claims 1–8 of the '892 patent. A copy of the *Ex Parte* Reexamination Certificate for the '892 patent is attached hereto as Exhibit 2.

7. On August 8, 2006, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 7,088,727 ("the '727 patent"), titled "System and Method for Establishing Network Connection with Unknown Network and/or User Device." Nomadix owns the '727 patent by assignment. A copy of the '727 patent is attached hereto as Exhibit 3.

8. On June 30, 2009, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 7,554,995 ("the '995 patent"), titled "System and Method for Establishing Network Connection with Unknown Network and/or User Device." Nomadix owns the '995 patent by assignment. A copy of the '995 patent is attached hereto as Exhibit 4.

9. On October 21, 2003, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 6,636,894 ("the '894 patent"), titled "Systems and Methods for Redirecting Users Having Transparent Computer Access to a Network Using a Gateway Device Having Redirection Capability." Nomadix owns the '894 patent by assignment. A copy of the '894 patent is attached hereto as Exhibit 5. Reexamination of the '894 patent was requested on or around September 24, 2004, and the ensuing reexamination resulted in confirmation of the patentability, without amendment, of Claims 1–11 of the '894 patent. A copy of the *Ex Parte* Reexamination Certificate for the '894 patent is attached hereto as Exhibit 6.

10. On March 20, 2007, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 7,194,554 ("the '554 patent"), titled "Systems and Methods for Providing Dynamic Network Authorization Authentication and Accounting." Nomadix owns the '554 patent by assignment. A copy of the '554 patent is attached hereto as Exhibit 7.

11. On March 15, 2005, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 6,868,399 ("the '399 patent"), titled "Systems and Methods for Integrating a Network Gateway Device with

Management Systems." Nomadix owns the '399 patent by assignment. A copy of the '399 patent is attached hereto as Exhibit 8.

12. On February 15, 2005, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 6,857,009 ("the '009 patent"), titled "System and Method for Network Access Without Reconfiguration." Nomadix owns the '009 patent by assignment. A copy of the '009 patent is attached hereto as Exhibit 9.

13. Nomadix has marked the gateway devices it has manufactured and sold under the '892, '727, '894, '554, '399, and '009 patents with the numbers of those patents in accordance with 35 U.S.C. § 287(a).

CLAIM 1: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 6,130,892 BY SOLUTIONINC

14. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–13 of this Complaint.

15. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

16. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '892 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '892 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices incorporating SolutionInc's SolutionIP product and/or network gateway devices that connect computers and mobile devices to networks.

17. Upon information and belief, SolutionInc's infringement of the '892

patent will continue unless enjoined by this Court.

18. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '892 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '892 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

19. Unless SolutionInc is enjoined from infringing the '892 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

CLAIM 2: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 7,088,727 BY SOLUTIONINC

20. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–19 of this Complaint.

21. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

22. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '727 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '727 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices incorporating SolutionInc's SolutionIP product and/or network gateway devices that connect computers and mobile devices to networks.

23. Upon information and belief, SolutionInc's infringement of the '727

patent will continue unless enjoined by this Court.

24. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '727 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '727 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

25. Unless SolutionInc is enjoined from infringing the '727 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

CLAIM 3: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 7,554,995 BY SOLUTIONINC

26. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–25 of this Complaint.

27. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

28. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '995 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '995 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices incorporating SolutionInc's SolutionIP product and/or network gateway devices that connect computers and mobile devices to networks.

29. Upon information and belief, SolutionInc's infringement of the '995

patent will continue unless enjoined by this Court.

30. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '995 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '995 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

31. Unless SolutionInc is enjoined from infringing the '995 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

CLAIM 4: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 6,636,894 BY SOLUTIONINC

32. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–31 of this Complaint.

33. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

34. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '894 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '894 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices incorporating SolutionInc's SolutionIP product and/or network gateway devices that connect computers and mobile devices to networks, and that facilitate related functions including, *inter alia*, redirection.

35. Upon information and belief, SolutionInc's infringement of the '894 patent will continue unless enjoined by this Court.

36. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '894 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '894 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

37. Unless SolutionInc is enjoined from infringing the '894 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

CLAIM 5: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 7,194,554 BY SOLUTIONINC

38. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–37 of this Complaint.

39. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

40. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '554 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '554 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices incorporating SolutionInc's SolutionIP product and/or network gateway devices that connect computers and mobile devices to networks, and that facilitate related

functions including, *inter alia*, authentication.

41. Upon information and belief, SolutionInc's infringement of the '554 patent will continue unless enjoined by this Court.

42. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '554 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '554 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

43. Unless SolutionInc is enjoined from infringing the '554 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

CLAIM 6: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 6,868,399 BY SOLUTIONINC

44. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–43 of this Complaint.

45. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

46. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '399 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '399 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices incorporating SolutionInc's SolutionIP product and/or network gateway devices

that connect computers and mobile devices to networks, and that facilitate related functions including, *inter alia*, integrated billing.

47. Upon information and belief, SolutionInc's infringement of the '399 patent will continue unless enjoined by this Court.

48. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '399 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '399 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

49. Unless SolutionInc is enjoined from infringing the '399 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

CLAIM 7: CLAIM FOR INFRINGEMENT OF U.S. PATENT NO. 6,857,009 BY SOLUTIONINC

50. Nomadix repeats, realleges and incorporates by reference the allegations set forth in paragraphs 1–49 of this Complaint.

51. This is a claim for patent infringement arising under the patent laws of the United States; Title 35 of the United States Code.

52. Without authority, SolutionInc, through its agents, employees and servants, has manufactured, used, promoted, offered for sale, and/or sold within the United States, and/or imported into the United States products covered by one or more claims of the '009 patent, has actively induced others to do the same and/or has contributed to others' performance of the same. SolutionInc has thereby infringed, actively induced others to infringe and/or contributed to others' infringement of one or more claims of the '009 patent in violation of 35 U.S.C. § 271, including 35 U.S.C. §§ 271(a), (b) and/or (c). This infringement is currently ongoing. The products relating to SolutionInc's infringement include devices

incorporating SolutionInc's SolutionIP product and/or network gateway devices that connect computers and mobile devices to networks, and that facilitate related functions including, *inter alia*, proxy service.

53. Upon information and belief, SolutionInc's infringement of the '009 patent will continue unless enjoined by this Court.

54. Upon information and belief, SolutionInc has derived, received, and will continue to derive and receive gains, profits and advantages from the aforesaid acts of infringement of the '009 patent in an amount that is not presently known to Nomadix. Due to the infringement of the '009 patent by SolutionInc, Nomadix has been damaged and is entitled to monetary relief in an amount to be determined at trial.

55. Unless SolutionInc is enjoined from infringing the '009 patent, Nomadix will continue to suffer irreparable injury for which it has no adequate remedy at law.

PRAYER FOR RELIEF

Nomadix respectfully prays for:

A. An order adjudging SolutionInc to have infringed each of the '892, '727, '995, '894, '554, '399, and '009 patents;

B. A permanent injunction enjoining SolutionInc, as well as its officers, agents, servants, employees, and attorneys and those persons in active concert or participation with SolutionInc, from infringing the '892, '727, '995, '894, '554 '399, and '009 patents;

C. An accounting of all gains, profits, and advantages derived by SolutionInc's infringement of the '892, '727, '995, '894, '554, '399, and '009 patents and an award of damages adequate to compensate Nomadix for SolutionInc's infringement of the '892, '727, '995, '894, '554, '399, and '009 patents;

D. An award of pre-judgment and post-judgment interest and costs of this action against SolutionInc;

E. An award to Nomadix of its attorneys' fees incurred in connection with this action; and

F. Such other and further relief as the Court deems just and proper.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 1/19/2010 By: _____

John B. Sganga, Jr.
Douglas G. Muehlhauser
Perry D. Oldham
Mark Lezama
Alan G. Laquer

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff Nomadix, Inc. hereby demands a trial by jury on all issues so triable.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 1/19/2010

By: _____
John B. Sganga, Jr.
Douglas G. Muehlhauser
Perry D. Oldham
Mark Lezama
Alan G. Laquer

8391974

US006130892A

United States Patent [19]

Short et al.

[11] **Patent Number: 6,130,892**

[45] **Date of Patent: Oct. 10, 2000**

[54] **NOMADIC TRANSLATOR OR ROUTER**

[75] Inventors: **Joel E. Short**; **Leonard Kleinrock**, both of Los Angeles, Calif.

[73] Assignee: **Nomadix, Inc.**, Westlake Village, Calif.

[21] Appl. No.: **09/041,534**

[22] Filed: **Mar. 12, 1998**

Related U.S. Application Data

[63] Continuation-in-part of application No. 08/816,174, Mar. 12, 1997, abandoned.

[51] **Int. Cl.**[7] **H04L 12/56**; H04J 3/16

[52] **U.S. Cl.** **370/401**; 370/338; 370/466

[58] **Field of Search** 370/338, 389, 370/390, 392, 393, 395, 397, 400, 401, 402, 404, 406, 409, 465, 463, 466, 467, 350, 252, 254, 255, 408; 455/432, 433, 456; 340/825.07, 825.2, 825.21; 709/220, 221, 222, 223, 219, 226, 229, 230, 245

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	10/1992	Perkins	370/338
5,309,437	5/1994	Perlman	370/408
5,371,852	12/1994	Attanasio	370/402
5,412,654	5/1995	Perkins	370/338
5,557,748	9/1996	Norris	709/219
5,586,269	12/1996	Kubo .	
5,636,216	6/1997	Fox et al.	370/402
5,708,655	1/1998	Toth et al.	370/313
5,751,971	5/1998	Dobbins	709/225
5,781,552	7/1998	Hashimoto	370/447
5,790,541	8/1998	Patrick et al.	370/392
5,793,763	8/1998	Mayes et al.	370/389
5,798,706	8/1998	Kraemer et al.	370/401
5,841,769	11/1998	Okanoue et al.	370/338
5,854,901	1/1999	Cole	709/222
5,862,345	1/1999	Okanoue et al.	370/312
5,909,549	6/1999	Complement	709/223
5,915,119	6/1999	Cone	709/223
5,918,016	7/1999	Brewer	709/220
5,920,699	7/1999	Bare	709/223
6,006,272	12/1999	Aravamudan et al.	709/245
6,012,088	2/2000	Li et al.	709/219

OTHER PUBLICATIONS

Egevang, IP Network Address Translator, Network Working Group RFC 1631, pp. 1–10, May 1994.

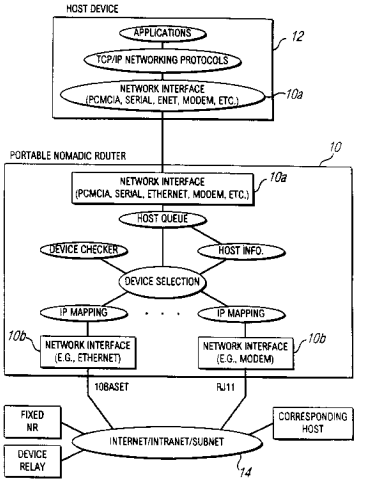
Joel E. Short; "Auto–Porting and Rapid Protyping with Application to Wireless and Nomadic Network Algorithms, A dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Computer Science," University of California, Los Angeles; Published Oct. 26, 1996; pp. xv, 118–124; Copyright Jan. 16, 1997.

Primary Examiner—Ricky Ngo
Assistant Examiner—Steven Nguyen
Attorney, Agent, or Firm—Brooks & Kushman P.C.

[57] **ABSTRACT**

A nomadic router or translator enables a laptop computer or other portable terminal which is configured to be connected to a home network to be connected to any location on the internet or other digital data communication system. The router automatically and transparently re-configures the terminal to its new location and processes outgoing and incoming data. The router includes a processor which appears as the home network to the terminal, and appears as the terminal to the communication system. The terminal has a permanent address, the router has a router or translator address, and the terminal transmits outgoing data to the system including the permanent address as a source address. The processor translates the outgoing data by replacing the permanent address with the router address as the source address. The terminal receives incoming data from the system including the router address as a destination address, and the processor translates the incoming data by replacing the router address with the permanent address as the destination address. Alternatively, the terminal can be directly connected to a point on a local network, and the router connected to another point on the network. The router can be employed to implement numerous applications including nomadic e-mail, network file synchronizer, database synchronizer, instant network, nomadic internet and trade show router and can also be utilized as a fixed nomadic router.

8 Claims, 10 Drawing Sheets



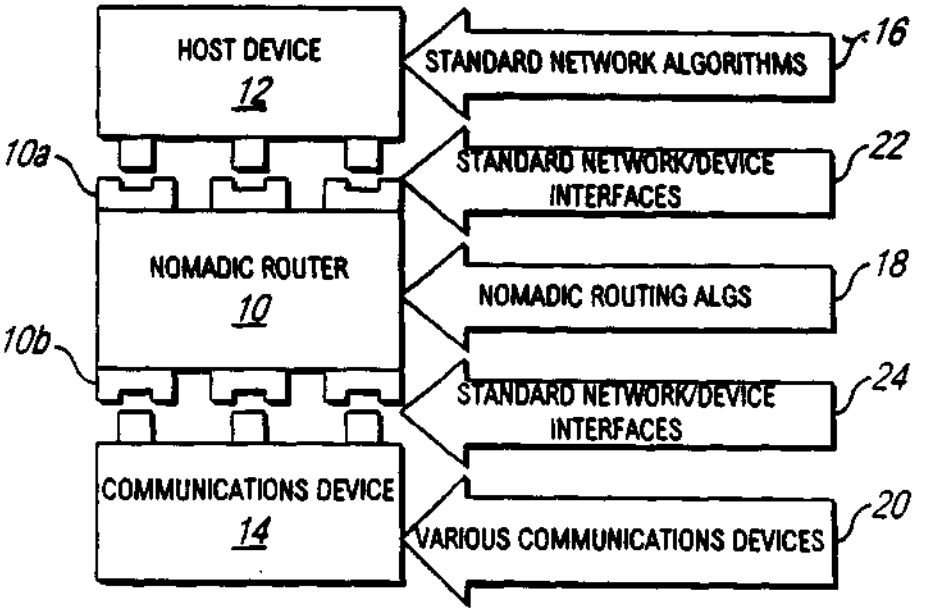

HOST DEVICE
12
10a
NOMADIC ROUTER
10
10b
COMMUNICATIONS DEVICE
14
STANDARD NETWORK ALGORITHMS
16
STANDARD NETWORK/DEVICE INTERFACES
22
NOMADIC ROUTING ALGS
18
STANDARD NETWORK/DEVICE INTERFACES
24
VARIOUS COMMUNICATIONS DEVICES
20

FIG. 1

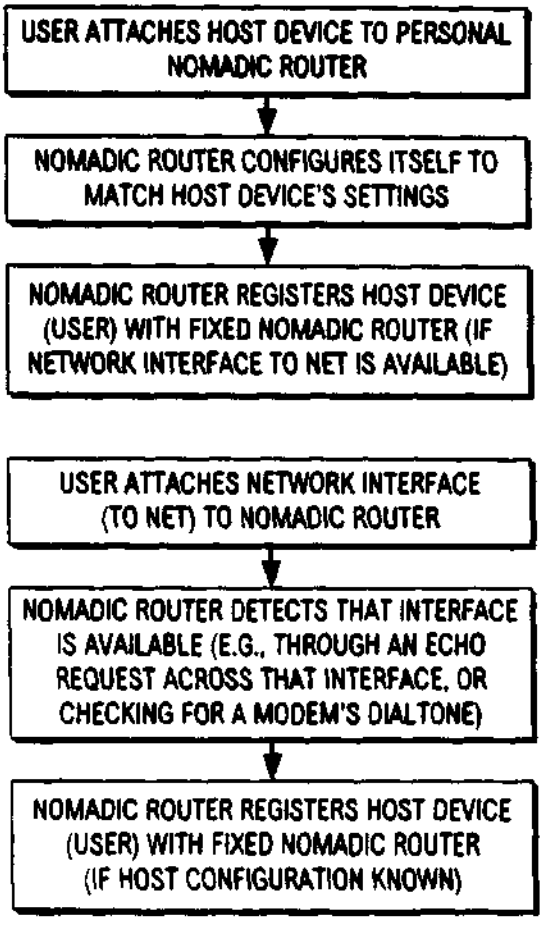

USER ATTACHES HOST DEVICE TO PERSONAL NOMADIC ROUTER
NOMADIC ROUTER CONFIGURES ITSELF TO MATCH HOST DEVICE'S SETTINGS
NOMADIC ROUTER REGISTERS HOST DEVICE (USER) WITH FIXED NOMADIC ROUTER (IF NETWORK INTERFACE TO NET IS AVAILABLE)
USER ATTACHES NETWORK INTERFACE (TO NET) TO NOMADIC ROUTER
NOMADIC ROUTER DETECTS THAT INTERFACE IS AVAILABLE (E.G., THROUGH AN ECHO REQUEST ACROSS THAT INTERFACE, OR CHECKING FOR A MODEM'S DIALTONE)
NOMADIC ROUTER REGISTERS HOST DEVICE (USER) WITH FIXED NOMADIC ROUTER (IF HOST CONFIGURATION KNOWN)

FIG. 3

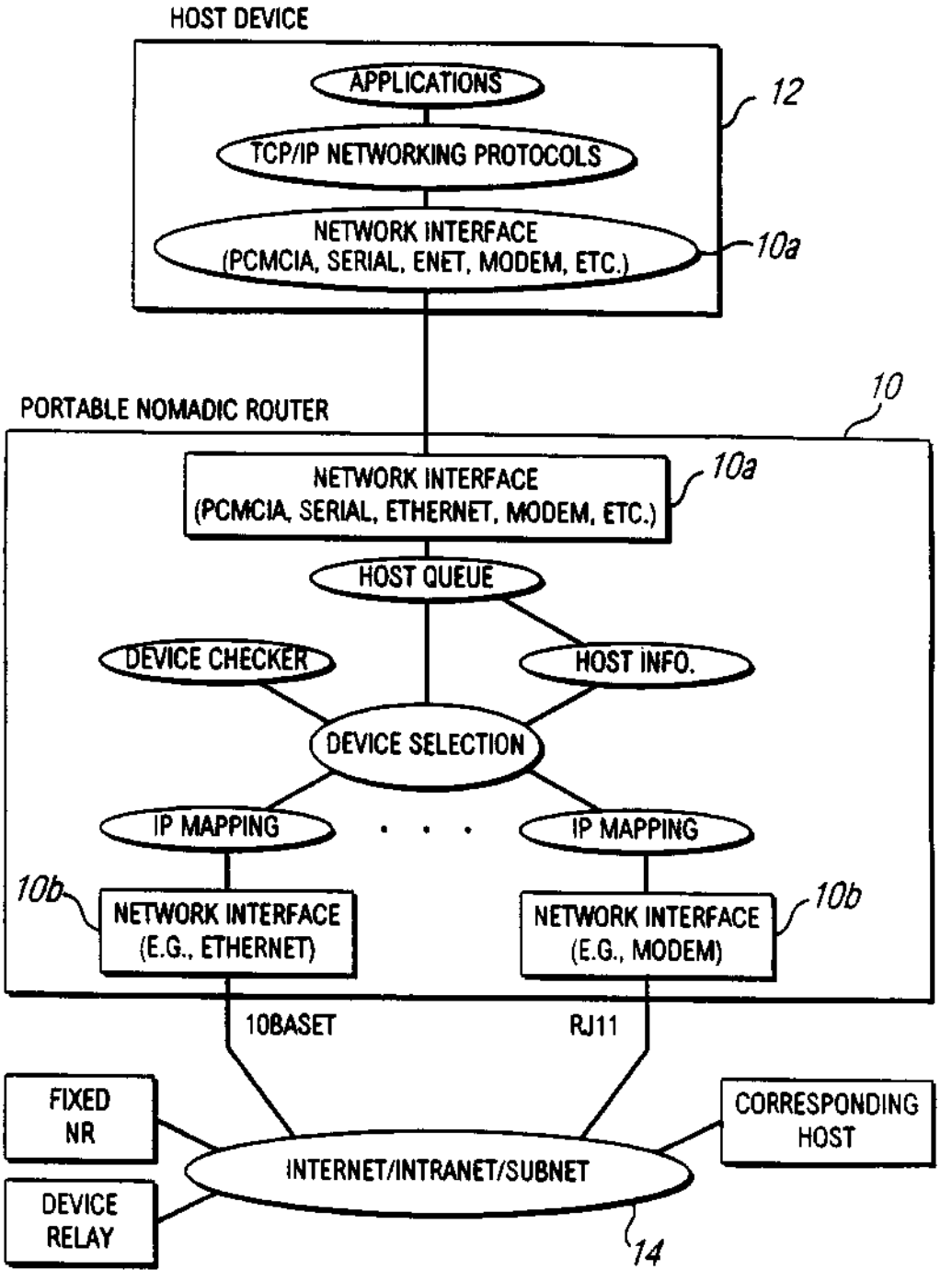

HOST DEVICE
APPLICATIONS
TCP/IP NETWORKING PROTOCOLS
NETWORK INTERFACE
(PCMCIA, SERIAL, ENET, MODEM, ETC.)
12
10a
PORTABLE NOMADIC ROUTER
10
NETWORK INTERFACE
(PCMCIA, SERIAL, ETHERNET, MODEM, ETC.)
10a
HOST QUEUE
DEVICE CHECKER
HOST INFO.
DEVICE SELECTION
IP MAPPING
IP MAPPING
10b
NETWORK INTERFACE
(E.G., ETHERNET)
NETWORK INTERFACE
(E.G., MODEM)
10b
10BASET
RJ11
FIXED
NR
DEVICE
RELAY
INTERNET/INTRANET/SUBNET
CORRESPONDING
HOST
14

FIG. 2

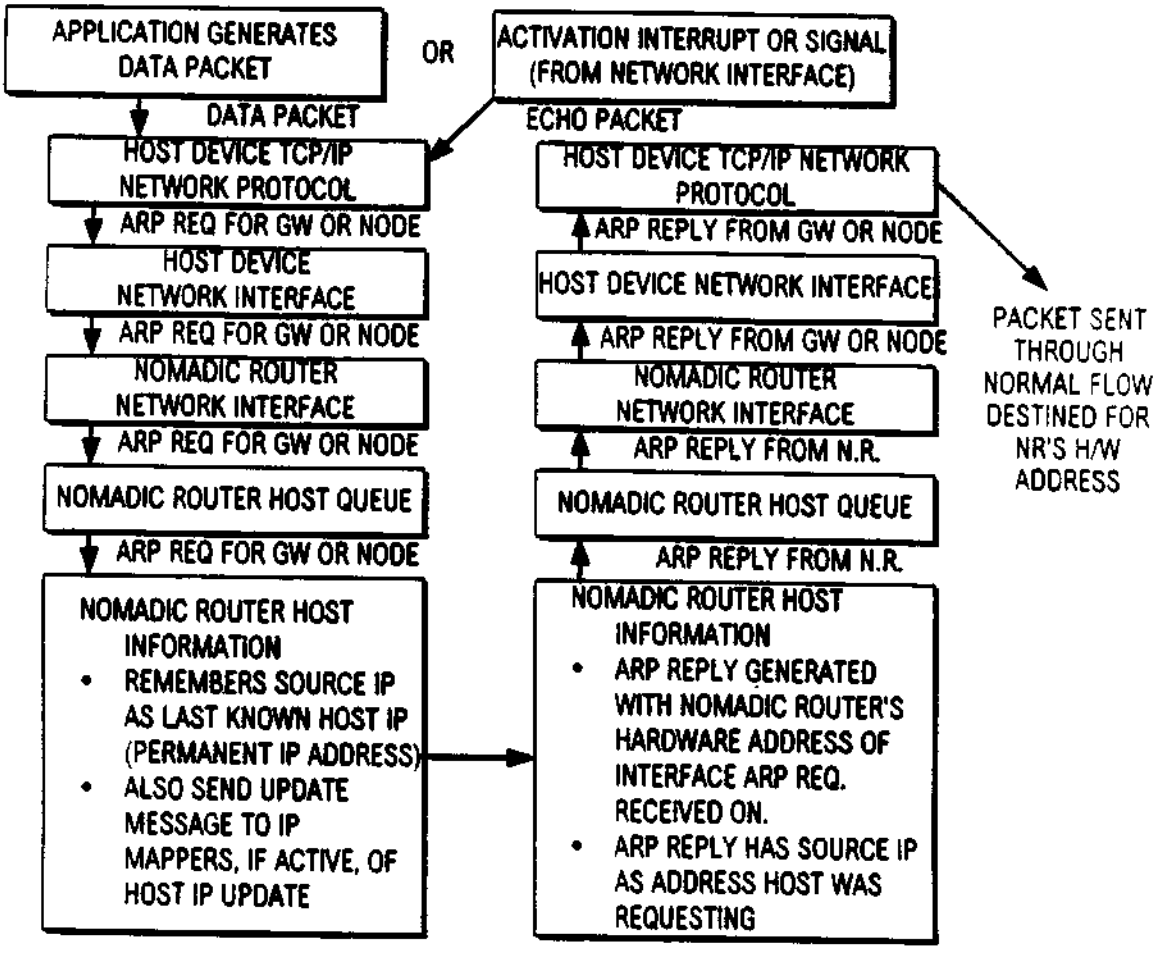

APPLICATION GENERATES DATA PACKET
OR
ACTIVATION INTERRUPT OR SIGNAL (FROM NETWORK INTERFACE)
DATA PACKET
ECHO PACKET
HOST DEVICE TCP/IP NETWORK PROTOCOL
ARP REQ FOR GW OR NODE
HOST DEVICE NETWORK INTERFACE
ARP REQ FOR GW OR NODE
NOMADIC ROUTER NETWORK INTERFACE
ARP REQ FOR GW OR NODE
NOMADIC ROUTER HOST QUEUE
ARP REQ FOR GW OR NODE
NOMADIC ROUTER HOST INFORMATION
• REMEMBERS SOURCE IP AS LAST KNOWN HOST IP (PERMANENT IP ADDRESS)
• ALSO SEND UPDATE MESSAGE TO IP MAPPERS, IF ACTIVE, OF HOST IP UPDATE
HOST DEVICE TCP/IP NETWORK PROTOCOL
ARP REPLY FROM GW OR NODE
HOST DEVICE NETWORK INTERFACE
ARP REPLY FROM GW OR NODE
NOMADIC ROUTER NETWORK INTERFACE
ARP REPLY FROM N.R.
NOMADIC ROUTER HOST QUEUE
ARP REPLY FROM N.R.
NOMADIC ROUTER HOST INFORMATION
• ARP REPLY GENERATED WITH NOMADIC ROUTER'S HARDWARE ADDRESS OF INTERFACE ARP REQ. RECEIVED ON.
• ARP REPLY HAS SOURCE IP AS ADDRESS HOST WAS REQUESTING
PACKET SENT THROUGH NORMAL FLOW DESTINED FOR NR'S H/W ADDRESS

FIG. 4

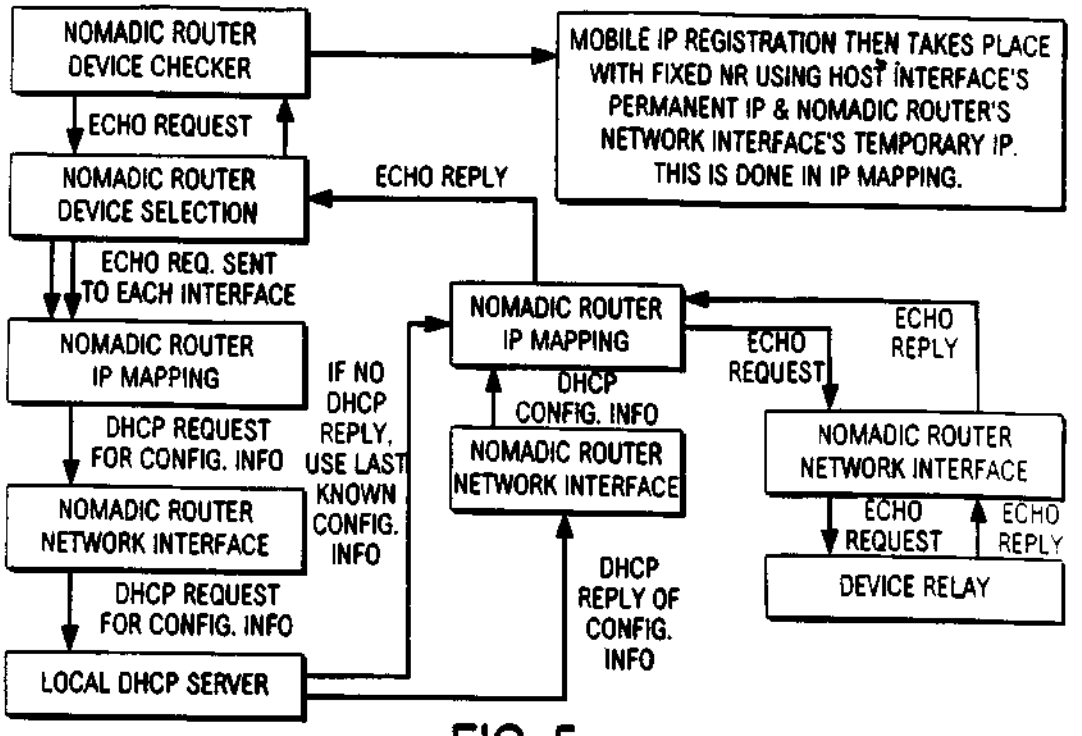

NOMADIC ROUTER DEVICE CHECKER
ECHO REQUEST
NOMADIC ROUTER DEVICE SELECTION
ECHO REQ. SENT TO EACH INTERFACE
NOMADIC ROUTER IP MAPPING
DHCP REQUEST FOR CONFIG. INFO
NOMADIC ROUTER NETWORK INTERFACE
DHCP REQUEST FOR CONFIG. INFO
LOCAL DHCP SERVER
ECHO REPLY
MOBILE IP REGISTRATION THEN TAKES PLACE WITH FIXED NR USING HOST INTERFACE'S PERMANENT IP & NOMADIC ROUTER'S NETWORK INTERFACE'S TEMPORARY IP. THIS IS DONE IN IP MAPPING.
IF NO DHCP REPLY, USE LAST KNOWN CONFIG. INFO
NOMADIC ROUTER IP MAPPING
DHCP CONFIG. INFO
NOMADIC ROUTER NETWORK INTERFACE
DHCP REPLY OF CONFIG. INFO
ECHO REQUEST
ECHO REPLY
NOMADIC ROUTER NETWORK INTERFACE
ECHO REQUEST
ECHO REPLY
DEVICE RELAY

FIG. 5

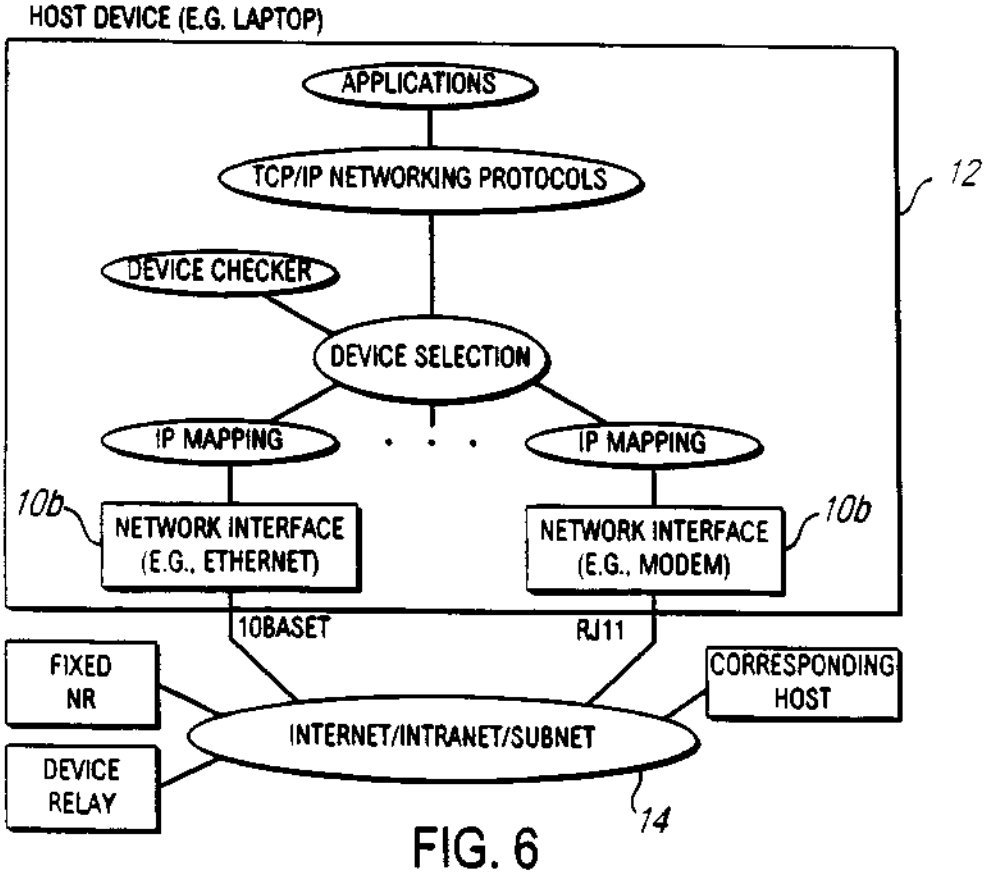

HOST DEVICE (E.G. LAPTOP)
APPLICATIONS
TCP/IP NETWORKING PROTOCOLS
12
DEVICE CHECKER
DEVICE SELECTION
IP MAPPING
IP MAPPING
10b
NETWORK INTERFACE (E.G., ETHERNET)
NETWORK INTERFACE (E.G., MODEM)
10b
10BASET
RJ11
FIXED NR
DEVICE RELAY
INTERNET/INTRANET/SUBNET
CORRESPONDING HOST
14

FIG. 6

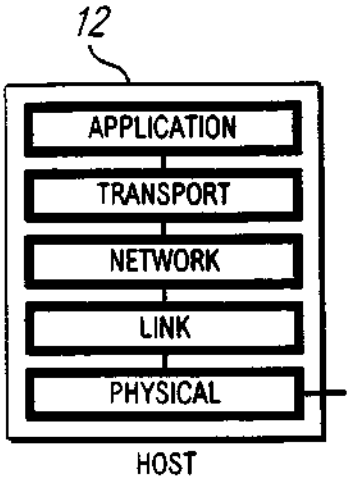


FIG. 7A

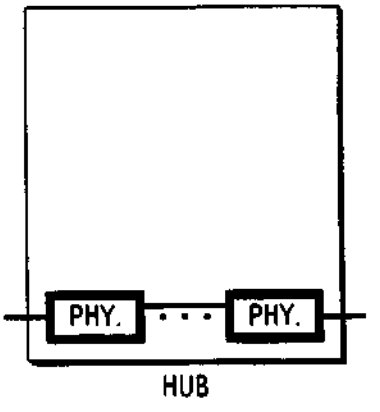


FIG. 7B

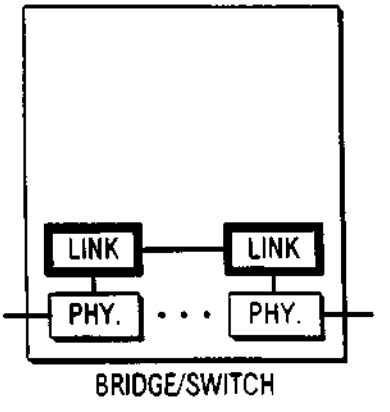


FIG. 7C

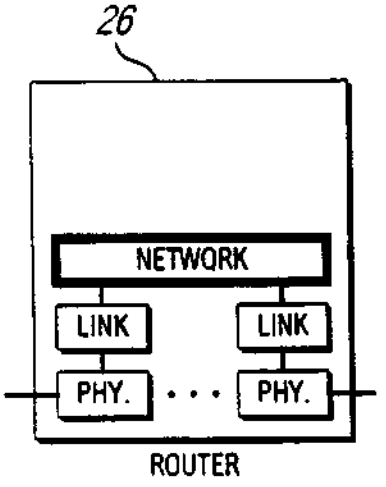


FIG. 7D

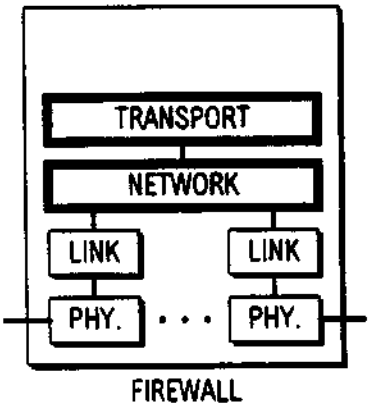


FIG. 7E

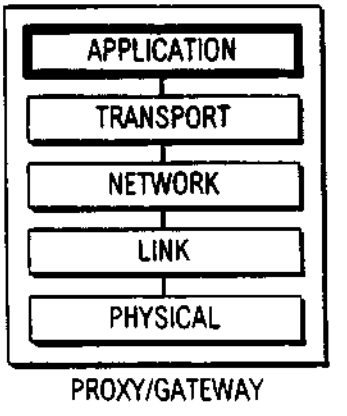


FIG. 7F

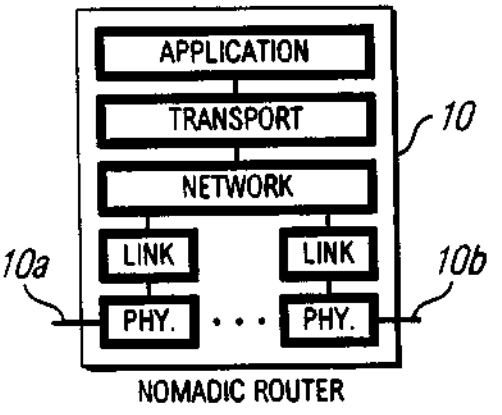


FIG. 7G

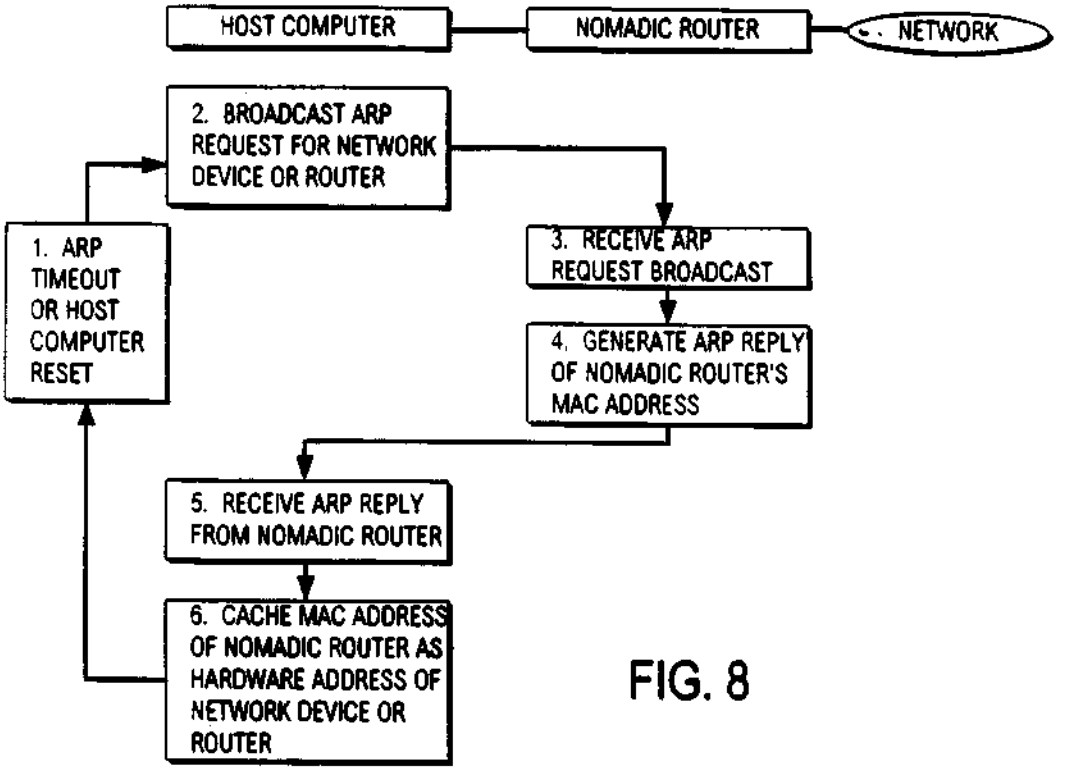

HOST COMPUTER
NOMADIC ROUTER
NETWORK
2. BROADCAST ARP REQUEST FOR NETWORK DEVICE OR ROUTER
1. ARP TIMEOUT OR HOST COMPUTER RESET
3. RECEIVE ARP REQUEST BROADCAST
4. GENERATE ARP REPLY OF NOMADIC ROUTER'S MAC ADDRESS
5. RECEIVE ARP REPLY FROM NOMADIC ROUTER
6. CACHE MAC ADDRESS OF NOMADIC ROUTER AS HARDWARE ADDRESS OF NETWORK DEVICE OR ROUTER

FIG. 8

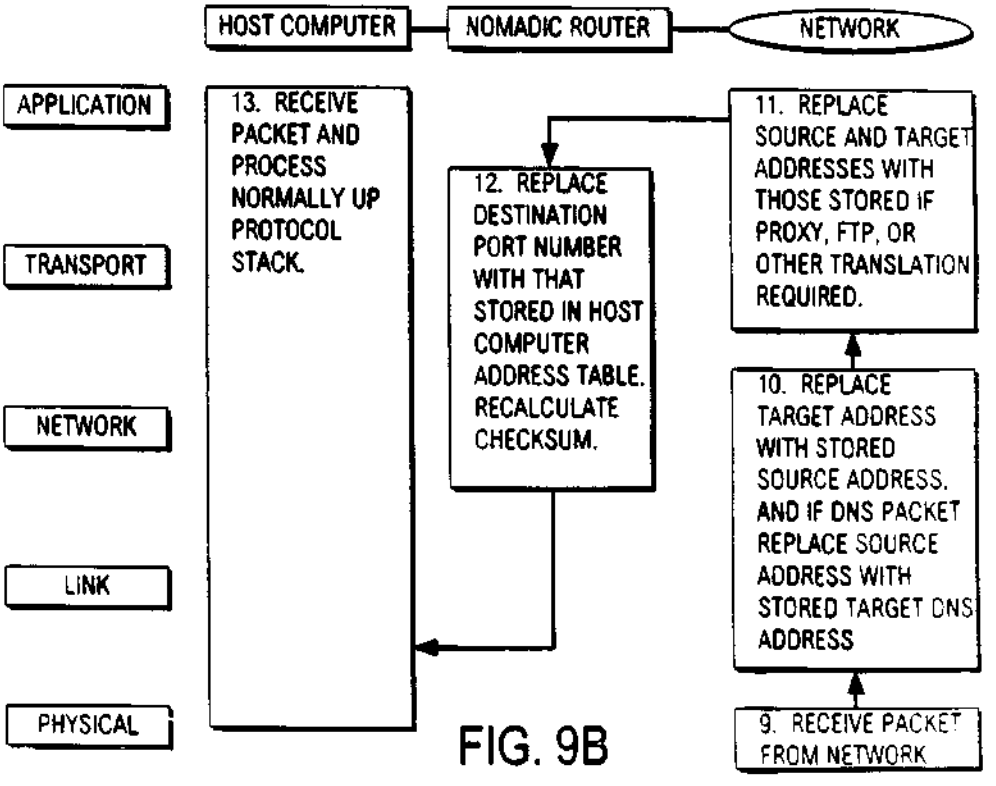

HOST COMPUTER
NOMADIC ROUTER
NETWORK
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
13. RECEIVE PACKET AND PROCESS NORMALLY UP PROTOCOL STACK.
12. REPLACE DESTINATION PORT NUMBER WITH THAT STORED IN HOST COMPUTER ADDRESS TABLE. RECALCULATE CHECKSUM.
11. REPLACE SOURCE AND TARGET ADDRESSES WITH THOSE STORED IF PROXY, FTP, OR OTHER TRANSLATION REQUIRED.
10. REPLACE TARGET ADDRESS WITH STORED SOURCE ADDRESS. AND IF DNS PACKET REPLACE SOURCE ADDRESS WITH STORED TARGET DNS ADDRESS
9. RECEIVE PACKET FROM NETWORK

FIG. 9B

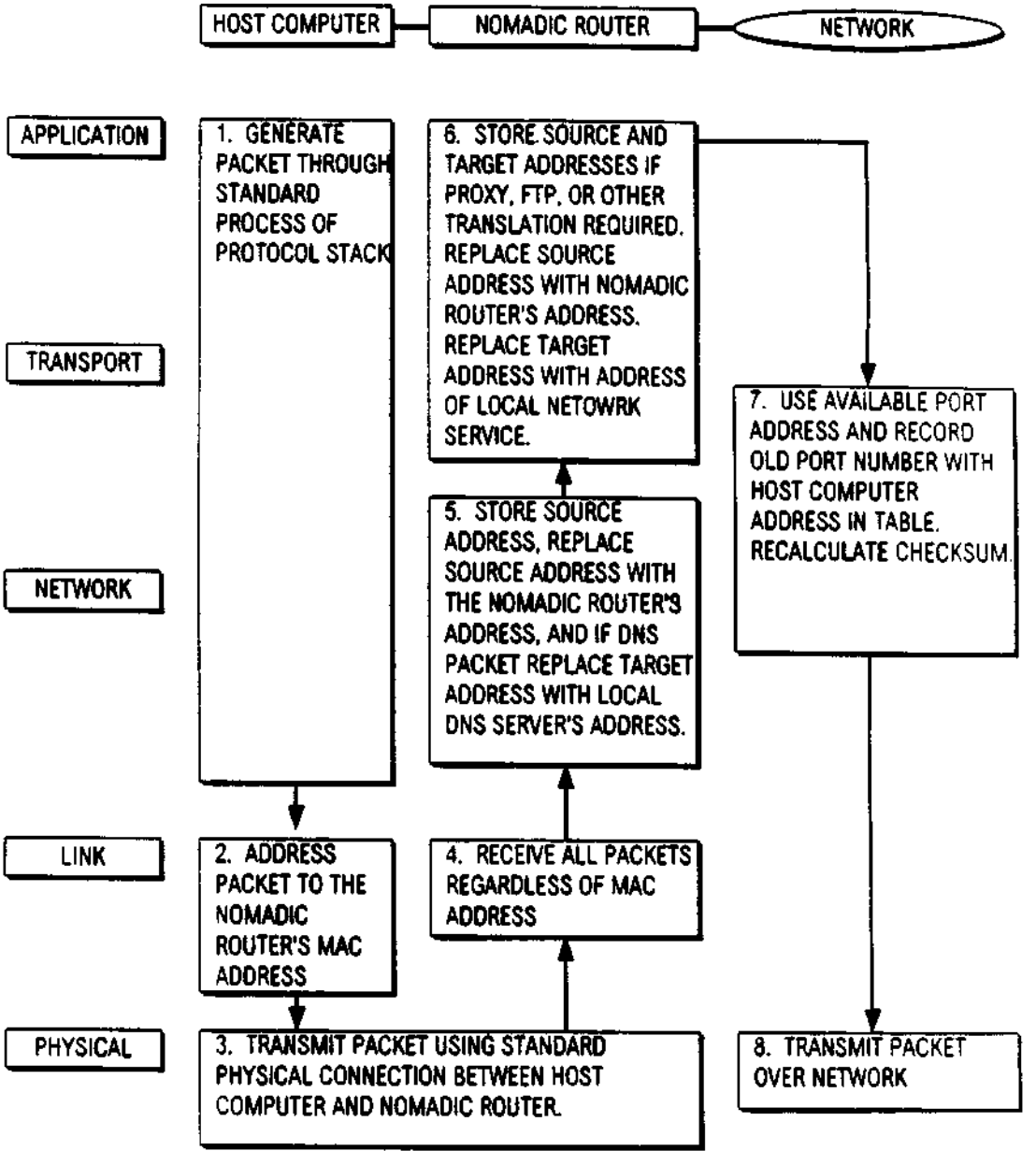

HOST COMPUTER
NOMADIC ROUTER
NETWORK
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
1. GENERATE PACKET THROUGH STANDARD PROCESS OF PROTOCOL STACK
2. ADDRESS PACKET TO THE NOMADIC ROUTER'S MAC ADDRESS
3. TRANSMIT PACKET USING STANDARD PHYSICAL CONNECTION BETWEEN HOST COMPUTER AND NOMADIC ROUTER.
4. RECEIVE ALL PACKETS REGARDLESS OF MAC ADDRESS
5. STORE SOURCE ADDRESS, REPLACE SOURCE ADDRESS WITH THE NOMADIC ROUTER'S ADDRESS, AND IF DNS PACKET REPLACE TARGET ADDRESS WITH LOCAL DNS SERVER'S ADDRESS.
6. STORE SOURCE AND TARGET ADDRESSES IF PROXY, FTP, OR OTHER TRANSLATION REQUIRED. REPLACE SOURCE ADDRESS WITH NOMADIC ROUTER'S ADDRESS. REPLACE TARGET ADDRESS WITH ADDRESS OF LOCAL NETOWRK SERVICE.
7. USE AVAILABLE PORT ADDRESS AND RECORD OLD PORT NUMBER WITH HOST COMPUTER ADDRESS IN TABLE. RECALCULATE CHECKSUM.
8. TRANSMIT PACKET OVER NETWORK

FIG. 9A

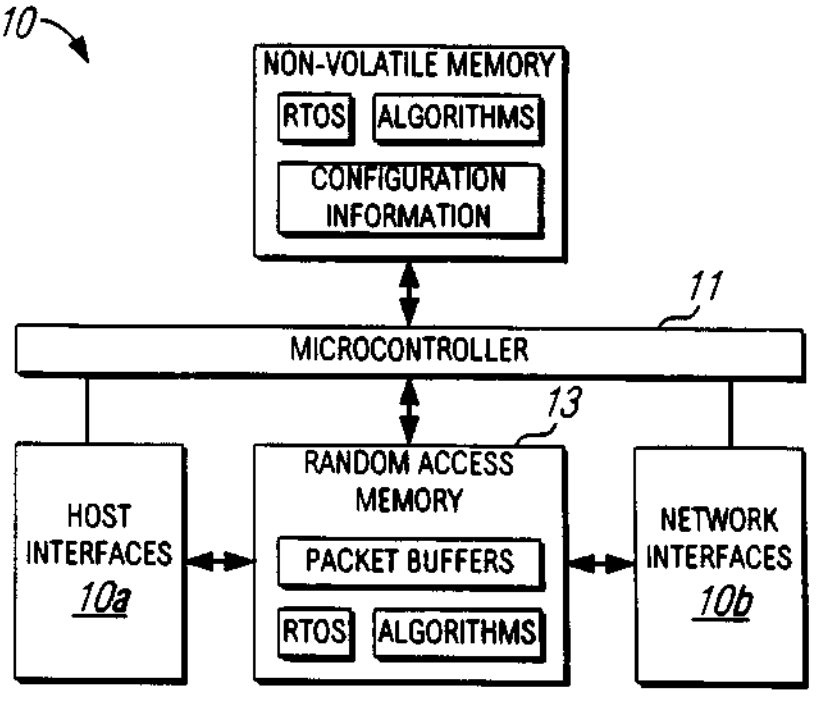

10
NON-VOLATILE MEMORY
RTOS
ALGORITHMS
CONFIGURATION INFORMATION
11
MICROCONTROLLER
13
RANDOM ACCESS MEMORY
PACKET BUFFERS
RTOS
ALGORITHMS
HOST INTERFACES
10a
NETWORK INTERFACES
10b

FIG. 10

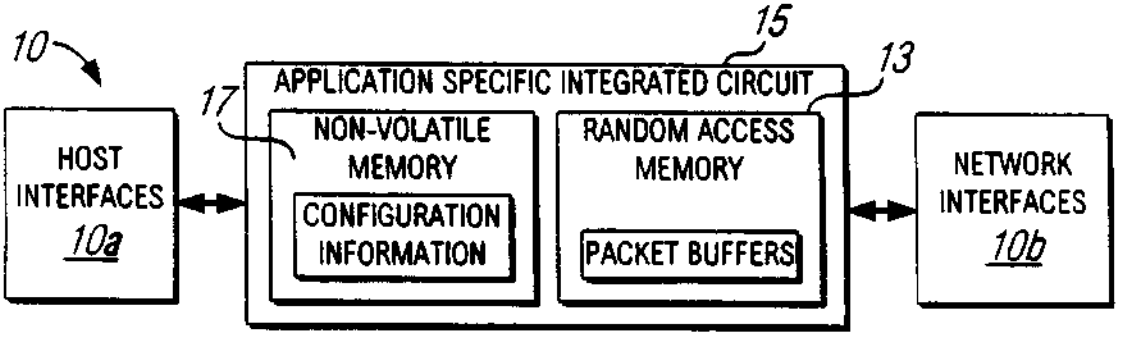

10
15
13
17
APPLICATION SPECIFIC INTEGRATED CIRCUIT
NON-VOLATILE MEMORY
CONFIGURATION INFORMATION
RANDOM ACCESS MEMORY
PACKET BUFFERS
HOST INTERFACES
10a
NETWORK INTERFACES
10b

FIG. 11

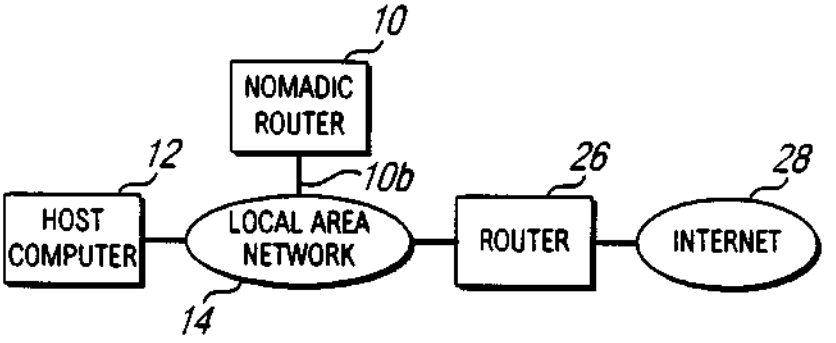


FIG. 12A

FIG. 12B

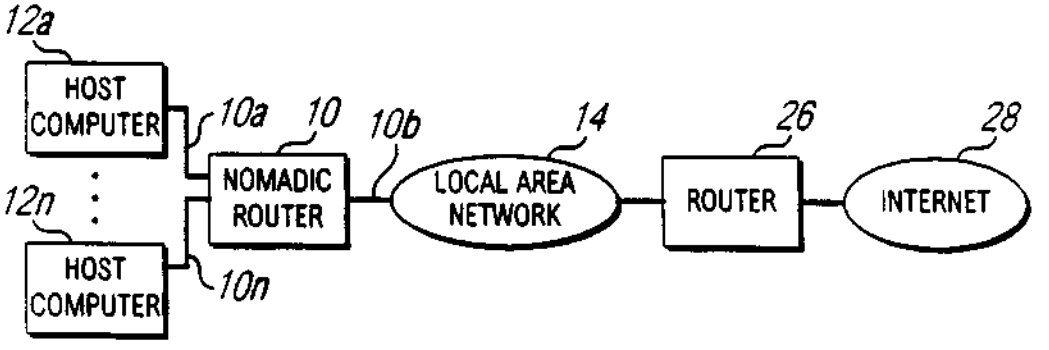


FIG. 12C

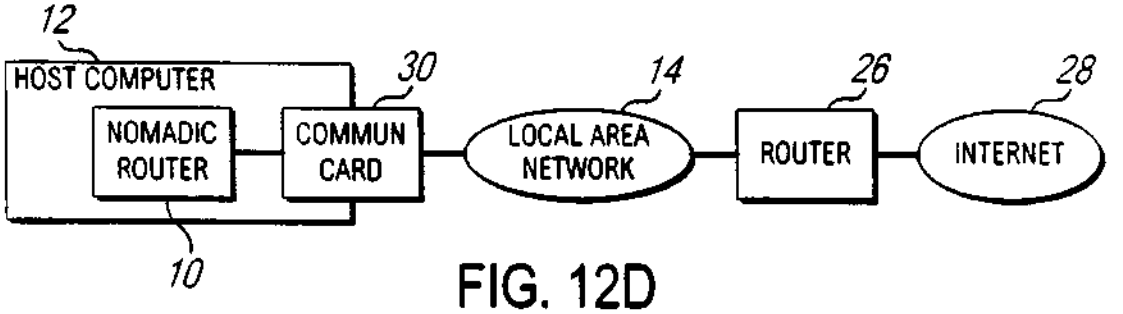


FIG. 12D

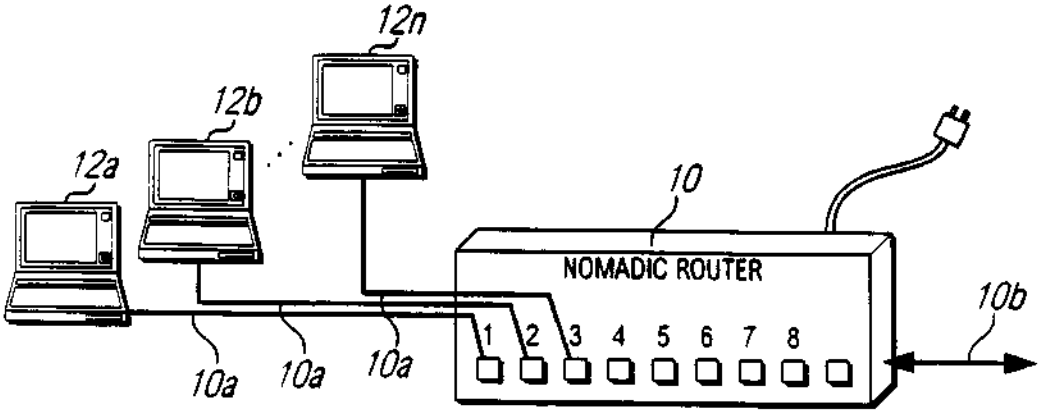


FIG. 13

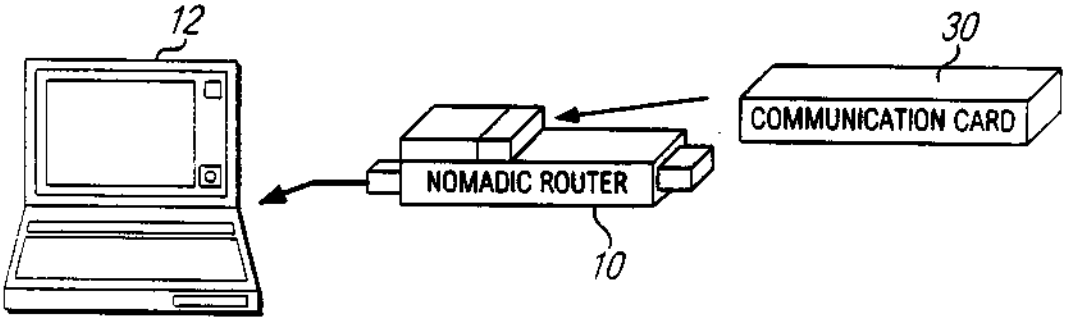


FIG. 14

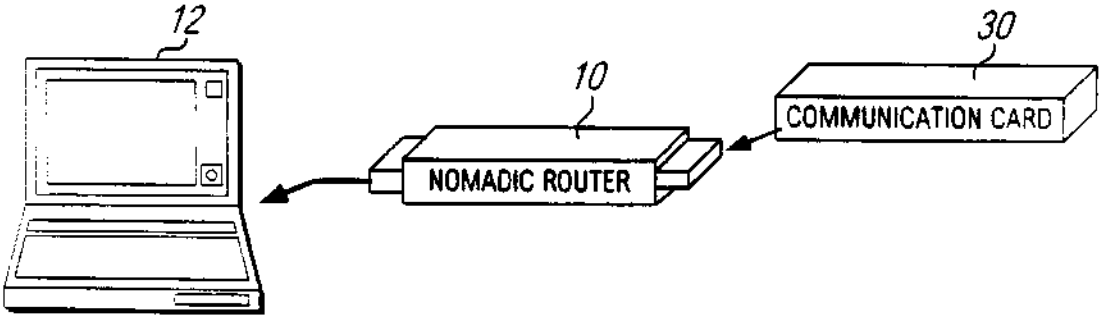


FIG. 15

NOMADIC TRANSLATOR OR ROUTER

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation-in-part of U.S. patent application Ser. No. 08/816,174, entitled "NOMADIC ROUTER", filed Mar. 12, 1997, by Joel E. Short et al, now abandoned.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

The U.S. government may have rights in this invention as provided for by the terms of Contract No. DAAH01-97-C-R179 awarded by DARPA.

TECHNICAL FIELD

The present invention generally relates to the art of digital communications, and more specifically to a portable translator or router which enables a user digital communication terminal to be location and device transparent.

BACKGROUND ART

User digital communication addresses such as internet or IP addresses are conventionally associated with a fixed physical location, such as a user's business telephone line. However, portable communication devices such as laptop computers are becoming increasingly popular, and it is common for a user to access the internet from locations as diverse as hotel rooms and airplanes.

Digital communication networks are set up to route communications addressed to a communication address to the associated physical location. Thus, if a laptop computer is connected to a remote location, communications to and from the computer will not be associated with the user's communication address.

In order for a computer (host) to communicate across a network (e.g., the internet), software protocols (e.g., Transport Control Protocol/Internet Protocol (TCP/IP)) must be loaded into the host. A host computer sends information (i.e., packets of data) to devices on the network (routers) which receive the packets and send the packets back to the destination host.

The destination host will route replies back using a similar process. Each host computer and router must be configured so it will know who to send the packets of data to. A router will receive the packets only if the host computers specifically send (address) the packets to that router. If a host is configured incorrectly (bad address), then the host computer and router will be unable to communicate.

With the advent of mobile computers (laptops) and the desire to plug them into various networks to gain access to the resources on the network and internet, a mobile computer must be configured for each network it plugs into. Traditionally this new configuration can be done either (i) manually in software on the mobile computer (usually causing the mobile computer to be restarted to load in the new configuration), or (ii) with a new set of protocols which must be utilized on the mobile computer to obtain the configuration information from a device on the network to which the computer is being connected. When new services (protocols) are created to add functionality to the host computers, these new protocols must be updated in the host computers or routers, depending upon the type of new functionality being added.

DISCLOSURE OF INVENTION

In accordance with the present invention, a portable "Nomadic" router or translator enables a laptop computer or other portable terminal which is configured to be connected to a local home network to be connected to any location on the internet or other digital data communication system. The nomadic router automatically and transparently re-configures the terminal to its new location and processes outgoing and incoming data.

The nomadic router includes a processor which appears as the home network to the terminal, and appears as the terminal to the communication system. The terminal has a permanent address, the nomadic router has a router address, and the terminal transmits outgoing data to the system including the permanent address as a source address. The processor translates the outgoing data by replacing the permanent address with the router address as the source address. The terminal receives incoming data from the system including the router address as a destination address, and the processor translates the incoming data by replacing the router address with the permanent address as the destination address.

The terminal can be directly connected to a point on a local network, and the nomadic router connected to another point on the network. The nomadic router can be employed to implement numerous applications including nomadic e-mail, network file synchronizer, database synchronizer, instant network, nomadic internet, mobile virtual private network and trade show router, and can also be utilized as a fixed nomadic router.

The nomadic router can be implemented as software and/or hardware. The nomadic router establishes location and device transparency for a digital communication terminal such as a laptop computer. The terminal can be connected to any of a variety of networks and locations which can employ a variety of communication interface devices.

The nomadic router automatically converts the actual location address to a unique communication address for the user such as an internet address, such that the terminal performs communications originating from the communication address regardless of the physical location of the terminal.

The nomadic router also automatically configures the terminal to utilize a selected one of the interface devices, and switches from one to another if the first device malfunctions or becomes otherwise unavailable.

The nomadic router includes software and services which can be packaged in a personal portable device to support a rich set of computing and communications capabilities and services to accommodate the mobility of nomads (users) in a transparent, integrated, and convenient form. This is accomplished by providing device transparency and location transparency to the user.

There is a vast array of communication device alternatives such as Ethernet, Wireless LAN, and dialup modem among which the users switches when in the office, moving around the office, or on the road (such as at a hotel, airport, or home). The device transparency in the nomadic router provides seamless switching among these devices (easily, transparently, intelligently, and without session loss). The location transparency support in the nomadic router prevents users from having to reconfigure (e.g., IP and gateway address) their network device (laptop) each time they move to a new network or subnetwork.

The present nomadic router provides a separation of location and identity by providing a permanent IP address to the network device (host). The nomadic router provides independence between the location, communication device, and the host operating system. There are no new standards

which need to be adopted by the networking community. All specialized processing is stored internally to the nomadic router with standard interfaces to the host device and various communication devices.

The nomadic router supports the migration to Network Computers by providing identity and security services for the user. The nomadic router also supports multiple parallel communication paths across the communications network for soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates.

A portable router for enabling a data communication terminal to be location and device transparent according to the present invention, comprises: a first module for storing a digital communication address of a user; a second module for detecting a data communication network location to which the terminal is connected; a third module for detecting communication devices that are connected to the terminal; a fourth module for establishing data communication between the terminal and the network such that the communication address of the location from the second module is automatically converted to the communication address of the user from the first module; and a fifth module for automatically selecting a communication device which was detected by the third module for use by the fourth module.

The present nomadic router utilizes a unique process embodied in a self-contained apparatus which manipulates the packets of data being sent between the host computers and routers. This process provides an intelligent active universal translation of the content of the packets being transmitted between the host computer and nomadic router. The translation allows the host computer to communicate with the nomadic router even when the host computer is not configured to communicate with the nomadic router.

This is achieved by the nomadic router pretending to be the router which the host is configured for, and by the nomadic router pretending to be the host which the router expects to communicate with. Therefore, the nomadic router supports the mobility of computers in that it enables these computers to plug into the network at different locations (location independence) without having to install, configure, or utilize any new protocols on the mobile computer.

The mobile computer continues to operate without being aware of the change in location or new configuration, and the nomadic router translates the data allowing the host to think that it is communicating with the router. By putting this process in a self-contained apparatus, the deployment of new protocols can be performed independently of the host computer and its operating system (host independent).

All specialized processing and translation is stored internally in the nomadic router with standard interfaces to the host device and various communication devices. Thus, no new standards need be adopted. By removing the complexity of supporting different network environments out of the mobile computer and into this self-contained apparatus, the nomadic router allows the host computer to maintain a very minimal set of software protocols and functionality (e.g., the minimum functionality typically installed in network computers) to communicate across the network.

The nomadic router translation ability also enables the use of alternate communication paths (device independence) without the host computer being aware of any new communication device that utilizes an alternate communication path. The translation of the packets is done not just at the physical, link, or network layer of the protocol stack but at the transport and application layers as well. This allows the network card, protocol stack, and application running on the host computer to be independent of the network environment and configuration.

As an example of the communication device independence, the translation allows soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates. In addition, the nomadic router translation ability provides a flexible process for deploying enhanced nomadic and mobile computing software and services such as filtering of packets and determining which packets should be allowed to be transmitted between the mobile computer and the nomadic router or local area network (Internal Firewall).

The router apparatus can be: (i) carried with the mobile user (e.g., using an external box); (ii) attached to the mobile computer (e.g., PCMCIA card); (iii) installed inside the mobile computer (e.g., a chip in the laptop); (iv) or installed into the network infrastructure so it will already be there when the mobile computer user arrives (e.g., a box which plugs into the local area network translating packets being sent between the host and nomadic router, or a chip which is installed in routers on the network). The nomadic router can also be provided in the form of software which is loaded and executed in the mobile computer or another computer or router on a network.

These and other features and advantages of the present invention will be apparent to those skilled in the art from the following detailed description, taken together with the accompanying drawings, in which like reference numerals refer to like parts.

BRIEF DESCRIPTION OF DRAWINGS

FIG. **1** is a diagram illustrating the implementation of the present nomadic router between the host computing device and various communication devices through standard interfaces;

FIG. **2** is a diagram illustrating the basic nomadic router architecture, which is referred to as the hardware implementation architecture;

FIG. **3** is a flowchart illustrating a configuration overview of the basic steps performed when a host device is attached to the present nomadic router and when a network interface is attached to the router;

FIG. **4** is a flowchart illustrating the router's automatic adaptation to the host device when the first data packet from the host is sent to the attached router or when an activation interrupt or signal is received;

FIG. **5** is a flowchart illustrating the process by which the router initializes and checks the various communication device interfaces for initialization, activation, etc.;

FIG. **6** is a diagram illustrating the basic nomadic router architecture when implemented as software in the host device;

FIGS. **7***a* to **7***g* are diagrams illustrating protocol stack implementations for various network devices, and the translation function happening at all layers of the protocol stack in the nomadic router;

FIG. **8** is a flowchart illustrating the nomadic router's proxy ARP packet interception and host reconfiguration process;

FIGS. **9***a* and **9***b* in combination constitute a flowchart illustrating the nomadic router's translation process which takes place in the host computer and nomadic router at various levels in the protocol stack;

FIG. **10** is a diagram illustrating the architecture of the nomadic router implemented as a hardware device including

a microcontroller and a non-volatile memory for storing algorithms implementing the translation function;

FIG. **11** is a diagram illustrating the architecture of the nomadic router apparatus implemented as an Application Specific Integrated Circuit (ASIC) chip;

FIGS. **12***a* to **12***d* are diagrams illustrating host and network interface modes in which the nomadic router is able to operate;

FIG. **13** is a simplified perspective view illustrating the nomadic router as implemented in a self-contained box which connects onto a local area network via a network interface port and has multiple ports to connect to host computers;

FIG. **14** is a simplified perspective view illustrating the nomadic router apparatus as implemented on a PCMCIA Type III card where the nomadic router plugs into the host computer's type II slot and the communication card device, of Type II, plugs directly into the nomadic router so both may be powered and stored in the portable host computer; and

FIG. **15** is a simplified perspective view illustrating the nomadic router as implemented on a PCMCIA Type II card where the nomadic router plugs into the host computer via a type II interface slot and where the communication card device, Type II, plugs into the nomadic router type II card.

MODE(S) FOR CARRYING OUT THE INVENTION

Basic Nomadic Router

Well-defined Standard Interfaces:

FIG. **1** illustrates a "Nomadic" translator or router **10** embodying the present invention as being connected between a host device or computer **12** and a communications device **14**. The host device **12** is a laptop computer or other fixed or mobile digital data communication terminal which is sufficiently portable or mobile that it can be carried from one location to another. A laptop computer, for example, can be used in any convenient location such as an airplane, customer's office, home, etc.

The communications device **14** can be part of any type of communication system to which the host computer **12** can be connected. Such communication systems include, but are not limited to, local networks, wide area networks, dial-up and direct internet connections, etc. In a typical application, the communications device will connect the host computer to a local network which itself is connected to the internet. Thus, the host device **12** is able to communicate with an unlimited number of networks and nodes which are themselves interconnected with routers, switches, bridges, etc. in any known manner.

The present router **10** includes a terminal interface **10***a* which normally is used to connect the router **10** to the host device **12**, and a system interface **10***b* which connects the router **10** to the communications device **14**. As will be further described below, the router **10** generally includes a processor consisting of hardware and/or software which implements the required functionality. The router **10** is further configured to operate in an alternate mode in which the host device **12** is connected directly to a network, and the router **10** is also connected to a point in the network via the system interface **10***b*. In this case, the terminal interface **10***as* is unused.

Although the device **10** is described herein as being a router, it will be understood that the router **10** is not a conventional router in that it includes the capability for providing interconnectability between networks. Instead, the present router **10** is essentially a translator which enables the host device **12** to be automatically and transparently connected to any communications device **14**, and process incoming and outgoing data for the device **12**.

The host device **12** is provided with a permanent internet address which is conveniently not changed in accordance with the present invention. The device **12** is also initially configured to communicate with a particular gateway or other home device at its base location. The gateway has a home address which the device **12** attempts to locate when it is connected to any communication system. Without the functionality of the present nomadic router **10**, the host device **12** would not be able to operate at a remote location because it would not find its gateway.

It will be understood that the term "home" does not relate to a residence, but is the network, gateway or other communication device or system to which the terminal is normally connected and which corresponds to the home internet or IP address.

FIG. **1** further illustrates a top protocol layer **16** representing the host computing device **12** which generates and consumes data that is transferred through the communications device **14**. This interface **16** is done just below the IP layer, and above the link layer in the typical OSI/ISO model. In the middle is a layer **18** which represents the router **10** and whose function it is to adaptively configure and utilize the underlying communications device and provide the router support described herein. A lower layer **20** is a physical communication which carries out the communication (potentially wire-lined Internet based, ad-hoc or wireless) as made available and determined for use by the nomadic router or user. Between the router layer **18** and the layers **16** and **20** are interfaces **22** and **24** which the router **10** identifies and configures dynamically.

The present router operates with host computers, routers, and other network devices through well-defined standard interfaces such as specified by the IETF (Internet Engineering Task Force) and IEEE standardization committees. These standards specify the packet format, content, and physical communication characteristics. As shown in FIG. **7***a,* host computers have to be configured at various layers of the protocol stack depending on the communication capabilities and configuration of the current network.

Hubs, as shown in FIG. **7***b,* provide a well defined interface to connect host computers and network devices by transmitting packets across multiple physical connections. Hubs do not provide any manipulation or translation of the content of the packets being transmitted.

Bridges or switches, as shown in FIG. **7***c,* provide an intelligent filtering mechanism by which they only transmit packets across multiple physical connections based upon which physical connection the device is connected to, according to the link layer addressing (Media Access Control Address). Bridges and switches do not manipulate the content of the packet and do not provide any higher layer protocol functionality.

Routers, as shown in FIG. **7***d,* accept packets based upon the destination address at the network layer in the packet. The host computer must explicitly address the packet at the link layer to the router. The router will then retransmit the packet across the correct physical connection based upon how it is configured. No modification or translation of the packet is performed at any layer of the protocol stack other than the network layer.

Firewalls, as shown in FIG. **7***e,* filter packets at the network and transport layers to only allow certain packets to be retransmitted on to the other physical connection. Fire-

walls do not manipulate the content of the packet, only forward it on to the next hop in the network if it passes the transport (port) or network (IP address) filter.

Proxys and gateways, as show in FIG. **7***f*, only receive packets explicitly addressed to them by host computers. They only manipulate packets at the application level. The present nomadic router **10**, as shown in FIG. **7***g*, manipulates the content of the packets at the link, network, transport, and application layers of the protocol stack to provide a translation between how the host computer is configured and the configuration of the network to which the host computer is currently attached to.

Unlike all other devices shown in FIGS. **7***a* to **7***f*, the router **10** will automatically intercept and translate packets without the other devices being aware of the router **10** or being configured to use it. The translation algorithms in the router **10** which provide this location independence are provided completely internal to the router **10**. Thus no new standards need to be developed, accepted, or implemented in host computers **12** or routers **26** to deploy new network services when using the nomadic router.

Whenever a new or different communication device (which includes the link and physical layers) is utilized in a host computer **12**, the host computer's network layer must be aware of this new communication device. Since the router **10** has it's own network interface to the communication device, alternate communication devices can be utilized in the router **10** which the host computer **12** can utilize but does not have to be configured to use.

Permanent Addressing not Location Based

Today we communicate with individuals in terms of the location of their communications instruments (for instance, their computer's IP address or their fax machine's phone number). In order to support mobility and changing communication environments and devices, it is necessary to create an environment where people communicate with other people, and not specifically with the devices they use. To transparently support mobility and adaptivity in a wireless, potentially ad-hoc, communication internetwork, a common virtual network must be provided by an intelligent device or agent which supports the various computing hosts and communication devices.

The present nomadic router **10** provides the mapping between the location based IP address used in the Internet today and the permanent user based address housed in the host CPU in the device **12**. This is illustrated in FIG. **2** as "IP Mapping". This mapping is done without support or knowledge of such mapping by the host CPU or user.

The Internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU but rather are internal to the nomadic router. The host configuration information such as its IP number are discovered or determined as illustrated in FIG. **4** and stored in the nomadic router **10** as illustrated in FIG. **2** as "Host Info." This configuration process is overviewed in FIG. **3**.

Optional Off-loaded Processing

As illustrated in FIG. **2**, the nomadic router **10** can provide off-load communication processing for the host CPU by being physically separate from the host device **12**. The adaptation, selection, and transportation of information across the network is performed by the nomadic router **10**. This allows the host terminal or device **12** to utilize the network without having to directly support the network protocols. By having the nomadic router be responsible for adapting to the current network substrate, the host CPU can maintain a higher performance by not having to run the routing, adaptation, packetization, etc. algorithms or packet processing.

The nomadic router can also queue, transmit, and receive data independent of whether or not the host device **12** is available or even attached. The CPU **11** built into the nomadic router **10** provides all necessary computing routines to be a fully functional network co-processor independent of the host CPU. This will allow increased battery for the user since the nomadic router does not have numerous user I/O devices as does the host device **12**.

Location Independence

The instant network nomadic router provides the ability to provide ubiquitous and reliable support in a location independent fashion. This removes any burden on the user for device reconfiguration (e.g., IP address configuration, gateway or next hop router address, netmask, link level parameters, and security permissions) or data transmission.

The problem with existing protocol stacks is that communicating devices have to be reconfigured every time the communication environment changes. TCP/IP requires a new network, node and gateway number. Appletalk will automatically choose an unused node number and discover the network number, but all open communications are lost and services have to be restarted to begin using the new information.

This occurs, for example, when a PowerBook is plugged into a network, put to sleep, and then powered up in a different network. All network services are restarted upon wakeup, and network applications get confused if they are not restarted. The nomadic router solves this problem by providing temporary as well as permanent network and node numbers similar to that provided by Mobile IP. However, the nomadic router will also work with other protocol stacks (e.g., AppleTalk).

Mobile IP provides location independence at the network level and not at the link level. All link level parameters, which are device specific, will be automatically configured as illustrated in FIG. **5** when a new communications (network interface) device is attached to the nomadic router. The nomadic router completely eliminates the need for manual configuration by adaptively supporting device independence.

Multiple Substrates (Device Independence)

Another innovative feature of the nomadic router is the support for simultaneous use of multiple communication substrates. This is illustrated in FIG. **2** as "Device Selection". Users should be able to utilize two or more communication substrates, either to increase throughput or to provide soft-handoff capability. This functionality is not supported in today's typical protocol stacks (e.g., TCP/IP or AppleTalk).

For example, via the "network" control panel, the user can select between communications substrates such as EtherTalk, LocalTalk, Wireless, ARA, etc., but cannot remotely login across EtherTalk while trying to print via LocalTalk. Routers are typically able to bridge together various communication substrates, but merging the LocalTalk and EtherTalk networks together is often not desirable for many reasons, including performance and security.

A problem with existing routers today is that they require manual configuration and exist external to the node. To overcome this, the nomadic router can support automatic configuration and full router functionality internally. This allows a mobile or nomadic node to adapt to various communication and network devices dynamically, such as when the user plugs in a PCMCIA card or attaches a communications device to the serial port.

Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use, is shown in FIG. **2** and FIG. **5** as part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface.

There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Another feature of the nomadic router is the support for alternate or simultaneous use of various communication substrates. This is performed as part of step **5** in FIG. **6** when the source address is that of the communication substrate that the nomadic router is going to send the packet out on. Host computers will now indirectly be able to utilize two or more communication substrates, either to increase throughput or to provide soft-handoff capability.

This functionality is not supported in today's typical protocol stacks (e.g., TCP/IP or AppleTalk). Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use is part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface.

There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Hardware Specification

The nomadic router can run completely in software without any special hardware as shown in FIG. **6**, or without a CPU separate from the main host, or packaged in the form of a hardware device as shown in FIG. **2**. The nomadic router can also be provided as a digital storage medium which stores the software program that implements the functionality of the router's translation processing. Examples of digital storage media include optical media (e.g. CD-ROM), magnetic media (e.g. floppy disks), nonvolatile or read-only memories, or any combination thereof. The program is loaded into and run on the mobile terminal **12**, or alternatively into any other computer or router which is connected to a network.

One potential implementation of the nomadic router device is Embedded PC Technology. As an example, the rugged PC/104 standard modules have a form-factor of 3.550" by 3.775" and typically 0.6" per module and weigh approximately 7 oz. per module. The PC/104 module's utilization of a self-stacking bus with minimum component count and power consumption (typically 1–2 Watts per module) eliminates the need for a backplane or card cage.

The nomadic router can run on a **16** bit bus with an 80486 processor, for example. The standard network access devices can support burst rates up to 10 Mbps with typical user data throughput around 1–2 Mbps. The user bandwidth is less depending on the available wireless communication device. For example, Proxim's 2 Mbps wireless LAN typically covers 500 yards with user data throughput around 500 Kbps. As illustrated in FIG. **1**, the nomadic router typically includes 3 modules; a processor **10**, host device or terminal interface **10***a*, and communication device or system interface **10***b*.

Another potential hardware implementation is with the CARDIO S-MOS System technology. This CPU board is basically the same size as a PCMCIA credit card adapter. It is 3.55×3.775×0.6 inches. The power requirements are +5V DC+/–10% with an operating temperature of 0 to 70° C., a storage temperature of –40 to 85° C., and relative humidity of 10% to 85% non-condensing.

The CARDIO is the most compact PC/104 compatible system available which meets the one-stack mechanical and electrical PC/104 Rev. 2.2 specifications. Power fail indicator, battery backup and automatic switchover are also possible.

The nomadic router can also be implemented on a small portable device such as a PCMCIA card or partially on a PCMCIA card. In the case of a full implementation on a PCMCIA card, the host CPU and power supply are used to execute the Nomadic Routing and other protocols, algorithms, operating system, and application services. A hybrid implementation of part PCMCIA card and part other hardware implementation can also be used.

Apparatus Components

By performing packet translation in a self-contained apparatus, processing done on the packets in the nomadic router does not affect and is off-loaded from the host computer. All specific translation of the packets to match the network's configuration and services available is done internally to the nomadic router. The nomadic router can queue, transmit, and receive data independent of whether or not the host computer is available or even attached. The algorithms and microcontroller built into the nomadic router provides all necessary computing routines to be a fully functional network co-processor independent of the host computer.

By allowing the nomadic router to process packets independently of the host computer, the host computer can be powered down or asleep while processing is taking place, providing an increase in battery life for the mobile host computer.

The nomadic router can be configured with various components in several different ways. In FIG. **10**, the nomadic router contains a processor or microcontroller **11** to translate the packets stored in packets buffers in random access memory. The translation functions are stored in non-volatile memory **13** with the Real Time Operating System (RTOS) and configuration information on what types of translation need to be performed.

Upon startup (boot) of the nomadic router, the RTOS and translation algorithms are loaded from non-volatile memory into RAM where they are then executed. There may be zero, one, or more host interfaces in which host computers are connected. There are one or more network interfaces. If no host interface is available, then the nomadic router gets the packets via the host computer from the network interface.

In FIG. **11**, the nomadic router **10** is implemented as an Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA) **15**. These chips embed the algorithms for packet translation. The chip can include storage for non-volatile memory **17** which stores the configuration information such as when manually configured for the current network. The chip **15** can also include random access memory to buffer packets for translation in the nomadic router before being sent off to the host or network interface.

Apparatus Packaging

As described above, the nomadic router can be packaged in several different hardware configurations. The nomadic router can be embedded in the host computer, or network device such as a switch or router. It can also be implemented

as a PCMCIA card which plugs into the host computer or as a self-contained external box.

Each nomadic router can have from one to many interfaces. If the router **10** is put into the network infrastructure, it doesn't have to be carried around with the mobile user. As shown in FIG. **12***a,* the nomadic router **10** is attached to a Local Area Network (LAN) of the network infrastructure which constitutes the communications device **14** through the system interface **10***b*. The LAN **14** is connected through a conventional router **26** to the internet **28**. In this case, the host computer interface **10***a* of the nomadic router **10** is not needed since packets from the host computer **12** are received through the LAN **14**.

To provide a secure interface between the host computer **12** and network **14** to prevent host computers from being able to watch (sniff) packets on the network **14**, the nomadic router **10** can have one interface to the host computer **12** (terminal interface **10***a*) and a second interface (**10***b*) to the network **14** as shown in FIG. **12***b,* and provide filtering of packets retransmitted between the various interfaces thus providing a firewall type of security device which operates internally on the network.

In order to support multiple host computers **12***a* . . . **12***n* with a single nomadic router **10**, the nomadic router **10** may have multiple host interfaces $\mathbf{10}a_1 \ldots \mathbf{10}a_n$ as shown in FIG. **12***c* and in FIG. **13** and a network or system interface **10***b*.

If the nomadic router is carried around by the mobile user, it can take the form of a PCMCIA card. In FIG. **12***d,* the nomadic router **10** is implemented as a PCMCIA card. The processing and translation capability is stored inside the card and the interface to the host computer **12** is through a PCMCIA BUS interface or communication card **30**.

As shown in FIG. **14**, the PCMCIA card can fit in a type III slot where there is a connector on the nomadic router **10** which accepts the communication card **30** (a type II PCMCIA card.) In this mode, the nomadic router does not have to have the communication device specific components inside the PCMCIA card.

The nomadic router **10** can also take the form of a type II PCMCIA card. In this form, the communication device or card **30** plugs into the opposite end of the nomadic router card **10** as illustrated in FIG. **15**.

Translation Operation of The Nomadic Router

Initialization and Self Configuration

The nomadic router initialization and self configuration process provides the means by which the nomadic router is able to learn about the host computer and network so it knows what translation is necessary.

Host Learning

The nomadic router **10** is able to learn about how the host computer **12** is configured by looking at the content of the packets being sent from the host computer **12**. Rather than the host computer **12** sending packets directly to the router **26** or other network device, which is what it is initially configured to do, the nomadic router **10** is able to redirect all outbound packets from the host computer **12** to itself. This redirection can be accomplished in several ways as described below.

1. Proxy ARP Packet Interception and Host Reconfiguration

Whenever a host computer **12** has an IP packet which it needs to send to a router **26** or other network device, it uses the Address Resolution Protocol (ARP) to obtain the link layer Media Access Control address (MAC address). As illustrated in FIG. **8**, when the host computer **12** broadcasts an ARP request for the MAC address of a destination node, the nomadic router **10** receives this ARP request broadcast and responds with its MAC address (not that of the destination node).

When the host computer **12** receives this ARP reply from the nomadic router **10**, which contains the MAC address of the nomadic router **10**, the host computer **12** will cache this MAC address in the host computer **12** and send all packets destined for the configured router or network device to the nomadic router **10**. The host computer **12** will think that the MAC address is that of the configured IP network device, but in reality, the nomadic router **10** is pretending (proxying) to be the device (its home gateway) that the host computer **12** expects to find.

The nomadic router **10** is also able to reconfigure and intercept return packets from a router or other network device using the same process.

2. Promiscuous Mode Packet Interception

Since the MAC address is cached in the host computer **12** for a short period of time, the host computer **12** will not send out a new ARP request to obtain the MAC address again unless a timeout period occurs or the cache is cleared such as when the computer **12** is restarted.

When a conventional network device receives or hears a packet with a MAC address which does not match its own, it will ignore or drop the packet. Since it is possible to rapidly switch from one network environment to another using a portable computer, the nomadic router **10** must be able to intercept packets even when the MAC address is not that of the nomadic router's home gateway or device.

This is accomplished by placing the nomadic router's network connection in promiscuous mode. In this mode, the network connection on the nomadic router accepts all packets being transmitted on the communication link, not just ones being broadcasted or addressed specifically to it.

3. Dynamic Host Configuration Protocol (DHCP) Service

A host computer is able to utilize the DHCP service to obtain the configuration information rather than being manually configured. The host computer utilizing the DHCP service requires that a DHCP server be installed on the network segment to which it is currently attached. If the host computer **12** is utilizing this service and requests configuration information using DHCP, the nomadic router **10** will intercept these requests and respond with configuration information for the host computer **12** to use.

Network Learning

The nomadic router is able to learn about the network environment it is currently attached using several different methods as described below.

1. Dynamic Host Configuration Protocol (DHCP)

Whenever a different network connection is connected on the nomadic router, it will broadcast a DHCP request to obtain configuration information for the current network. If no DHCP service is available on the network, it will switch to another method to learn about the network configuration.

2. Router Information Packets

Routers on the network will periodically broadcast router information packets which are used to build routing tables and allow routers to adapt to changes in the network. The nomadic router **10** will listen on the network for these router information packets. When one is received, it will extract out the configuration information from these packets.

3. Passive Listening

By placing the nomadic router's network connection in promiscuous mode, where it receives all packets not just ones destined for it, it is able to examine all packets on the network to discover how the network is configured. It is also able to determine the IP addresses used on the local area network and which machines are routers by the final destination address not being the next hop address.

Using this method, the nomadic router **10** is passively able to learn how the network is configured and will elect to use

an unused IP address. If that IP address does become used by another network device, it will switch over to another unused IP address.

4. Manual Configuration

The network configuration information can be manually configured in the nomadic router **10**. This information can be set using an embedded web server, Simple Network Management Protocol (SNMP) tools, an application running on one of the computers in the network, or other suitable means. When manual configuration is used to set the network information, the nomadic router **10** will still learn about the host information automatically and provide all the translation capabilities so the host computers do not have to be aware of the correct network information of the LAN to which they are currently connected.

Packet Translation

The nomadic router's packet translation function provides a mapping between location and service dependent configurations used by the host computer **12** and that used by the network **14** to which it is currently attached. For outbound traffic from the host computer **12** to the network **14**, the translation function changes the content of the packet such as the source address, checksum, and application specific parameters, causing all packets sent out to the network **14** to be directed back to the nomadic router **10** rather than to the host computer **12**.

The inbound traffic from the network **14** arriving at the nomadic router **10**, which is really for the host computer **12**, is passed through the translation function so the host computer **12** thinks that the replies were sent directly to it. The host computer **12** will be completely unaware of all the translation being performed by the nomadic router **10**.

The translation function works as illustrated in FIGS. **9***a* and **9***b*. In these figures, the operations performed in the OSI/ISO model application, transport, network, link and physical layers are illustrated in rows opposite the layer designations. The operations performed by the host computer **12**, nomadic router **10** and network **14** are illustrated in columns below the device designations.

The host computer **12** will generate network packets using the current configuration stored in the host computer **12** using the standard protocol stack as shown in step **1**. This configuration information is either manually configured in the host computer **12** or obtained using DHCP.

As shown in step **2**, when the host computer **12** addresses the link level destination address, the address automatically obtained using the Proxy ARP packet interception routine described earlier, this will cause the host computer **12** to send the packet to the network address of its standard router or home gateway device, but using the link level address of the nomadic router **10**.

In step **3**, the packet is transmitted across the standard physical connection between the host computer **12** and nomadic router **10**. As shown in step **4**, the nomadic router **10** will receive the packet at the link level either due to the Proxy ARP function which reconfigured the host computer's MAC address, or the nomadic router **10** will have the link level in promiscuous mode which will cause it to receive the packet even if destined to a different MAC address.

Once the packet is passed to the network layer, shown in step **5**, the nomadic router translation function will modify the content of the packet to change the source address to that of the nomadic router's address instead of the host computer's address. It will also translate other location dependent information such as the name of the local Domain Name Service (DNS) server. When translating the DNS packet, it will change the source address to that of the nomadic router's address and the destination address to that of a local DNS server.

Once the network layer translation is complete, the packet can be translated at the application and transport layers. The application layer is translated next, as shown in step **6**, since the transport layer requires a pseudo network layer header which includes the source and destination addresses and the content from the application layer.

At the application layer translation, any addresses which describe the source address of the host computer, such as with FTP, are translated to be that of the nomadic router's address. Any application layer destination addresses, such as a local proxy server, are translated to match that of the server running on the current network.

Once this application translation is complete, the transport layer, as shown in step **7**, can complete the checksum and any port number manipulation. The port number is manipulated if more than one host computer **12** is attached to the nomadic router **10**. Each host computer **12** when it sends out a request using a specific port is translated to match an available inbound port on the nomadic router **10**.

The port number assigned for use with each host computer **12** is stored in a table in the nomadic router **10** and is utilized with the reply packet described later. Finally the packet is sent out over the network **14** in step **8**.

When a reply packet comes in from the network **14**, as shown in step **9**, the nomadic router **10** will receive the packet. In step **10**, the nomadic router **10** will perform the reverse network layer translation to set the destination address to that of the host computer **12** rather than the nomadic router's address, and any source address to that replaced by the nomadic router **10** in step **5**.

Once this network translation is complete, the packet is translated at the application layer, as shown in step **11**, to change the destination address to that of the host computer **12** and the source address to the original destination address stored from step **6**. In step **12**, any port manipulation performed in step **7** is changed to the original setting and a new checksum is computed. Finally, as shown in step **13**, the packet is sent to the host computer **12** which then processes the packet normally.

Options of the Nomadic Router

There are numerous options and applications of the nomadic router. These applications include, but are not limited to, Nomadic E-mail, Remote Network File Synchronization, Nomadic Database Synchronization, Instant Network Nomadic Routing, Nomadic Intranets, and Trade Show Data Exchange. Each of these are described in more detail below.

Nomadic E-mail

Nomadic E-mail provides a synchronized yet distributed way for updates, reconciliation, and replicas to propagate through the internet. At various locations in the internet are nomadic router's equipped with nomadic E-mail support which provides the necessary synchronization, etc. Each nomadic router enabled for nomadic E-mail can utilize special protocols such as IMAP which provide support for mobile users without the host device having to support it (such as the case now with the POP3 protocol standard in most internet E-mail clients).

Remote Network File Synchronizer

The Remote Network File Synchronization option of the nomadic router provides copies of user files stored/cached at various locations (e.g., hotel, office, home) on other nomadic routers equipped for remote network file synchronization. Copies of updated files are automatically synchronized and distributed among all peer locations. Local updates can be made while the host is disconnected from the nomadic router and from the network.

Nomadic Database Synchronizer

The Nomadic Database Synchronizer houses the user's (synchronized) master databases (e.g., contacts, addresses, phone numbers). The nomadic router of the database synchronizer does not even need to be used on the network since it will interface directly with various host devices such as laptops, desktops, personal digital assistants, handheld personal computers, pagers, etc. via various standard ports.

Instant Network Nomadic Router

The objective of the Instant Network nomadic router is to enable rapid deployment of a communication network in any environment with little or no fixed infrastructure. The host and communication devices do not have to directly support the rapid deployment functionality.

The instant network nomadic router distributedly and intelligently establishes a wireless (or wired) communication link between the host device and the desired communication system while performing configuration, security, multihop routing, and network level data transmission over various communication devices. The nomadic router performs all the necessary network creation and processing automatically to remove configuration and system support from the host system or user. The instant network nomadic router utilizes proprietary and existing/emerging wireless communication systems, and multihop routing protocols.

By way of motivation, many communication infrastructures are varied and fragmented, and this problem is likely to be exacerbated as more technologies are introduced. For example, high performance LANs, wireless services, cellular telephony, satellite, ubiquitous paging networks, all provide varying degrees of coverage, cost and bandwidth/delay characteristics.

Sometimes there will be no connectivity at all because of lack of service, partial and intermittent connectivity as devices are plugged and unplugged from a system, damage to communication infrastructures deliberately or by accident, lossy communication as a system moves through various service areas or difficult domains, and times when multiple network devices (communication substrates) can be used at the same time. The instant network nomadic router will dynamically adapt the communication internetwork, dynamically creating one if necessary, to provide survivable communication in a mobile chaotic environment without the need for centralized control or fixed infrastructures.

The rapidly deployable nomadic router is a device associated with each user host device (e.g., PDA or laptop computer). It transparently provides the following capabilities for host computer systems using various wireless communication devices for physical and link layer access.

1. Dynamic wireless network creation
2. Initialization into existing wireless networks
3. Automatic configuration
4. Network and subnetwork level data transmission
5. Multihop routing functionality

The nomadic router can detect a device being used either by polling the interface, providing an interrupt signal, or through specialized signaling. This in turn activates the nomadic router to configure the device (if necessary) and establish a communication link to an appropriate corresponding interface and wireless subnetwork. The nomadic router operates at a level between the host device generating data and the physical communication transmission device as illustrated in FIG. **1**.

Nomadic Intranet

The Nomadic Intranet provides all network, server type, services for users who wish to dynamically create an adhoc network. This is similar to the instant network nomadic router except the nomadic intranet is a single device with multiple ports into which laptop/devices can be plugged. The instant network nomadic router is distributed to (one per) each host device. The nomadic intranet not only provides adhoc networking but can also provide services such as temporary file storage, protocol conversion, act as a print server, and provide other services described as part of the Basic nomadic router.

Trade Show Nomadic Router

The Trade Show nomadic router not only provides the basic nomadic router functionality for an exhibitor's computer that is brought to the show, but also provides lead capture and/or information distribution. Lead capture can be provided for by interfacing with a badge reader to read the attendee's information. This information is then captured by the nomadic router and made available in the exhibitor's lead database.

The nomadic router can also provide a mechanism for distributing information to the attendee's personalized web page or sent via e-mail directly across the internet. The exhibitor's computer is able to control the information flow with the nomadic router by running software, such as a web browser, which talks with the service/control software stored in the nomadic router. The standard web browser can control display and capture of lead information, collection of qualification information, and selection of information to be distributed back to the attendee.

Fixed Nomadic Router

The Fixed nomadic router provides the same basic functionality and architecture as the portable nomadic router but is stored in one location. The fixed nomadic router acts as a surrogate or "Home Agent" for the user when he/she is away on travel. When the user wishes to register or utilize their host device elsewhere in the network, the portable nomadic router will register with the fixed nomadic router where it is temporarily attached to the network so information can be forwarded to the user's new location. The fixed nomadic router can also be used to house the master copy of the user's E-mail for the nomadic E-mail service, or files for the nomadic file synchronizer.

Mobile Virtual Private Network

The nomadic router provides the mapping between the location based IP address used in the internet today and the permanent user based address housed in the host CPU. This mapping is done without support or knowledge of such mapping by the host CPU or user. The Internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU but rather are internal to the nomadic router.

By implementing this protocol as part of the translation function in the nomadic router, the nomadic router can encapsulate packets from the host computer and transmit them back to the fixed nomadic router which are sent out (un-encapsulated) on the native (home) network. Replies from the home network are received by the fixed nomadic router and are encapsulated and sent back to the nomadic router. When packets are transmitted between the nomadic router and fixed nomadic router, the packets are encrypted and sent using the Internet Tunneling Protocol.

Since the nomadic router provides location independence and the fixed nomadic router forwards all packets from a corresponding host to the host computer via the nomadic router, any changes in the location, failure of a network link, or attachment point of the mobile host computer does not

cause any open session to be lost. This session loss prevention is possible since the fixed nomadic router pretends to be the mobile host computer, and the nomadic router pretends to be the home network. The fixed nomadic router and nomadic router translation functions hide the link and network loss from the transport and application session.

Various modifications will become possible for those skilled in the art after receiving the teachings of the present disclosure without departing from the scope thereof.

Industrial Applicability

The present invention is broadly applicable to the field of electronic data communications using computers and other devices.

What is claimed is:

1. A method for allowing network communications over a foreign network for a user device configured to communicate with a home network, the method comprising:

connecting the user device to the foreign network;

intercepting packets transmitted from the user device which would otherwise be dropped by devices on the foreign network to determine without requiring prior knowledge of network settings of the user device;

using the determined network settings of the user device to determine whether to intercept subsequently transmitted packets; and

automatically modifying packets transmitted from the user device based on the network settings of the user device and network settings of the foreign network.

2. The method of claim **1** wherein intercepting packets comprises:

intercepting an Address Resolution Protocol (ARP) packet transmitted from the user device to a network address on the home network; and

replying to the ARP packet using the network address of the home device and a hardware address of a configuration translator such that subsequent packets generated by the user device are sent to the configuration translator.

3. The method of claim **1** wherein intercepting packets comprises:

operating in a promiscuous mode to intercept all packets without regard to a packet destination address; and

determining the network settings of the user device based on a source address and destination addresses of the packets.

4. The method of claim **1** wherein intercepting packets comprises:

intercepting a Dynamic Host Control Protocol (DHCP) packet transmitted from the user device; and

replying to the DHCP packet to provide configuration settings based on the foreign network configuration.

5. The method of claim **1** wherein modifying packets transmitted from the user device comprises:

replacing a source address with a router address where the router address is automatically determined based on the network settings of the foreign network.

6. The method of claim **5** wherein replacing the source address comprises replacing a source address within a packet header.

7. The method of claim **5** wherein replacing the source address comprises replacing a source address within a packet header and a source address within packet contents.

8. The method of claim **5** further comprising:

receiving data from the foreign network with the router address as a destination address; and

replacing the destination address with a network address of the user device.

* * * * *

US006130892C1

(12) EX PARTE REEXAMINATION CERTIFICATE (7203rd)

United States Patent
Short et al.

(10) **Number: US 6,130,892 C1**
(45) **Certificate Issued: Dec. 1, 2009**

(54) **NOMADIC TRANSLATOR OR ROUTER**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Leonard Kleinrock**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

Reexamination Request:
No. 90/007,423, Feb. 15, 2005

Reexamination Certificate for:
Patent No.: **6,130,892**
Issued: **Oct. 10, 2000**
Appl. No.: **09/041,534**
Filed: **Mar. 12, 1998**

Related U.S. Application Data

(63) Continuation-in-part of application No. 08/816,174, filed on Mar. 12, 1997, now abandoned.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(52) **U.S. Cl.** **370/401**; 370/338; 370/466

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,166,931	A	11/1992	Riddle
5,251,207	A	10/1993	Abensour et al.
5,325,362	A	6/1994	Aziz
5,410,543	A	4/1995	Seitz et al.
5,425,029	A	6/1995	Hluchyj et al.
5,442,633	A	8/1995	Perkins et al.
5,490,139	A	2/1996	Baker et al.
5,517,618	A	5/1996	Wada et al.
5,539,736	A	7/1996	Johnson
5,557,748	A	9/1996	Norris
5,572,528	A	11/1996	Shuen
5,608,786	A	3/1997	Gordon
5,623,600	A	4/1997	Ji et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 986 230	A2	3/2000
JP	5344122	A2	12/1993
JP	5-344122		12/1993

(Continued)

OTHER PUBLICATIONS

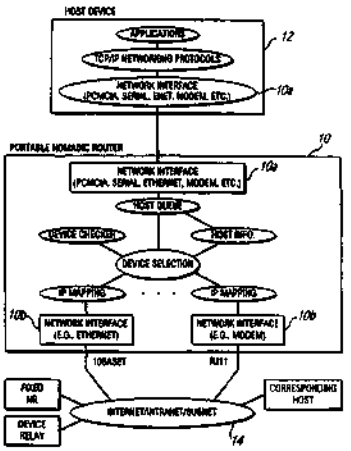
Network Working Group Request For Comments: 826;13 Ethernet Address Resolution Protocol (Nov. 1982).

(Continued)

Primary Examiner—Joseph R Pokrzywa

(57) **ABSTRACT**

A nomadic router or translator enables a laptop computer or other portable terminal which is configured to be connected to a home network to be connected to any location on the internet or other digital data communication system. The router automatically and transparently re-configures the terminal to its new location and processes outgoing and incoming data. The router includes a processor which appears as the home network to the terminal, and appears as the terminal to the communication system. The terminal has a permanent address, the router has a router or translator address, and the terminal transmits outgoing data to the system including the permanent address as a source address. The processor translates the outgoing data by replacing the permanent address with the router address as the source address. The terminal receives incoming data from the system including the router address as a destination address, and the processor translates the incoming data by replacing the router address with the permanent address as the destination address. Alternatively, the terminal can be directly connected to a point on a local network, and the router connected to another point on the network. The router can be employed to implement numerous applications including nomadic e-mail, network file synchronizer, database synchronizer, instant network, nomadic internet and trade show router and can also be utilized as a fixed nomadic router.



U.S. PATENT DOCUMENTS

5,633,868	A	5/1997	Baldwin et al.
5,636,216	A	6/1997	Fox et al.
5,651,002	A	7/1997	Van Seters et al.
5,708,780	A	1/1998	Levergood et al.
5,757,924	A	5/1998	Friedman et al.
5,761,683	A	6/1998	Logan et al.
5,781,550	A	7/1998	Templin et al.
5,802,320	A	9/1998	Baehr et al.
5,812,531	A	9/1998	Cheung et al.
5,812,776	A	9/1998	Gifford
5,822,526	A	10/1998	Waskiewicz
5,893,077	A	4/1999	Griffin
5,910,954	A	6/1999	Bronstein et al.
5,960,409	A	9/1999	Wexler
5,963,915	A	10/1999	Kirsch
5,987,430	A	11/1999	Van Horne et al.
5,987,498	A	11/1999	Athing et al.
5,991,292	A	11/1999	Focsaneanu et al.
5,991,828	A	11/1999	Horie et al.
6,014,698	A	1/2000	Griffiths
6,055,243	A	4/2000	Vincent et al.
6,061,356	A	5/2000	Terry
6,061,668	A	5/2000	Sharrow
6,088,725	A	7/2000	Kondo et al.
6,098,172	A	8/2000	Coss et al.
6,119,162	A	9/2000	Li et al.
6,128,601	A	10/2000	Van Horne et al.
6,128,739	A	10/2000	Fleming, III
6,130,892	A	10/2000	Short et al.
6,134,680	A	10/2000	Yeomans
6,141,690	A	10/2000	Weiman
6,205,481	B1	3/2001	Heddaya et al.
6,226,677	B1	5/2001	Slemmer
6,233,604	B1	5/2001	Van Horne et al.
6,243,379	B1	6/2001	Veerina et al.
6,249,527	B1	6/2001	Verthein et al.
6,286,039	B1	9/2001	Van Horne et al.
6,317,790	B1	11/2001	Bowker et al.
6,377,990	B1	4/2002	Slemmer et al.
6,385,653	B1	5/2002	Sitaraman et al.
6,393,468	B1	5/2002	McGee
6,412,073	B1	6/2002	Rangan
6,427,170	B1	7/2002	Sitaraman et al.
6,434,627	B1	8/2002	Millet et al.
6,460,084	B1	10/2002	Van Horne et al.
6,463,051	B1	10/2002	Ford
6,466,986	B1	10/2002	Sawyer et al.
6,496,850	B1	12/2002	Bowman-Amuah
6,535,493	B1	3/2003	Lee et al.
6,546,425	B1	4/2003	Hanson et al.
6,591,306	B1	7/2003	Redlich
6,636,894	B1	10/2003	Short et al.
6,640,251	B1	10/2003	Wiget et al.
6,671,379	B2	12/2003	Nemirovski
6,671,739	B1	12/2003	Reed
6,675,208	B1	1/2004	Rai et al.
6,779,118	B1	8/2004	Ikudome et al.
6,822,954	B2	11/2004	McConnell et al.
6,857,009	B1	2/2005	Ferreria et al.
6,868,399	B1	3/2005	Short et al.
7,051,087	B1	5/2006	Bahl et al.
7,088,727	B1	8/2006	Short et al.
7,139,268	B1	11/2006	Bhagwat et al.
7,313,631	B1	12/2007	Sesmun et al.
2002/0097674	A1	7/2002	Balabhadrapatreun

FOREIGN PATENT DOCUMENTS

JP	7066809	3/1995
JP	8065306 A2	3/1996
JP	8-242231	9/1996
WO	WO 95/27942	10/1995
WO	WO 97/11429	3/1997
WO	WO 99/039481	8/1999
WO	WO 99/57866	11/1999

OTHER PUBLICATIONS

Network Working Group Request For Comments: 894—Standards For Transmission of IP Datagrams Over Ethernet Networks (Apr. 1984).

Network Working Group Request For Comments: 925—Multi–LAN Address Resolution (Oct. 1984).

Network Working Group Request For Comments: 1009—Requirements For Internet Gateways (Jun. 1987).

Network Working Group Request For Comments: 1027—Using ARP to Implement Transparent Subnet Gateways (Oct. 1987).

Network Working Group Request For Comments: 1034—Domain Names—Concepts and Facilities (Nov. 1987).

Network Working Group Request For Comments: 153—Dynamic Host Confirmation Protocol (Oct. 1993).

Network Working Group Request For Comments: 1919—Classical Versus Transparent IP Proxies (Mar. 1996).

Network Working Group Request For Comments: 1945—Hypertext Transfer Protocol—HTTP;1.0 (May 1996).

L. Kleinrock, "Nomadic Computing" (Keynote address) *Int'l Conf. on Mobile Computing and Networking*, 1995, Berkeley, California, ACM.

M. Baker et al., Supporting Mobility in MosquitoNet, Proceedings of the 1996 Usenix Technical Conference, San Diego, CA, Jan. 1996.

Comer, "Internetworking With TCP/IP vol. 1, Chapter 10, Principles, Protocols, and Architecture", 3rd ed., Prentice Hall 1995.

Joel E. Short: "Auto–Porting and Rapid Prototyping with Application to Wireless and Nomadic Network Algorithms, A dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Computer Science", University of California, Los Angeles; Published Oct. 26, 1996; pp. xv, 118–124; Copyright Jan. 16, 1997.

Case No. 04CV1485 BTM (POR): *IP3 Networks, Inc.* v *Nomadix, Inc.*—Jul. 23, 2004 Complaint for: (1) Declaratory Judgment of Patent Non–Infringement and Invalidity of U.S. Patent No. 6,636,894; (2) Declaratory Judgment of Patent Non–Infringement of U.S. Patent No. 6,130,893; (3) Trade Libel; (4) Libel Under Cal. Civ. Code § 45; (5) Unfair Competition Under Cal. Bus.& Prof. Code § 17200, Et Seq.; and (6) Intentional Interference with Prospective Economic Advantage.

Case No. 04CV1485 BTM (POR): *IP3 Networks, Inc.* v *Nomadix, Inc.*—Sep. 20, 2004 Amended Complaint for: (1) Declaratory Judgment of Patent Non–Infringement and Invalidity of U.S. Patent No. 6,636,894; (2) Declaratory Judgment of Patent Non–Infringement of U.S. Patent No. 6,130,893; (3) Trade Libel; (4) Libel Under Cal. Civ. Code § 45; (5) Unfair Competition Under Cal. Bus.& Prof. Code § 17200, Et Seq.; and (6) Intentional Interference with Prospective Economic Advantage—Demand for Jury Trial.

Case No. 04CV1485 BTM (POR): *IP3 Networks, Inc.* v *Nomadix, Inc.*—Oct. 21, 2004 Answer and Counterclaims of Nomadix, Inc. to the Amended Complaint.

Case No. 04CV1485 BTM (POR): *IP3 Networks, Inc.* v *Nomadix, Inc.*—Plaintiff/Counter–Defendant IP3 Networks Inc.'s Reply to Defendant Nomadix, Inc.'s Counterclaim.

Perkins C.E et al.: "DHCP for mobile networking with TCP/IP" Proceedings IEEE International Symposium on Computers and Communications, Jun. 27, 1995, pp. 255–261, XP002132695.

Perkins C.E. Ed—Institute of Electrical and Electronics Engineers: "Mobile–AP, AD–HOC Networking, and Nomadicity" Proceedings of the 20th. Annual International Computer Software and Applications Conference (COMPSAC). Seoul, Aug. 21–23, 1996, Proceedings of the Annual International Computer Software and Applications Conference (COMPSAC), Los Alamitos, IEEE Comp, vol. Conf. 20, Aug. 21, 1996, pp. 472–576, XP 00684381, ISBN 0–8186–7579–9.

The Patent Office of the People's Republic of China Notification of First Office Action (PCT Application) and its translation for Chinese patent application 98 8 05023.4.

Google Groups: View Thread, Aug. 2, 2004, IP3 002505–06; Newsgroups: microsoft,public.win95.networking.

Google Groups: View Thread, Aug. 2, 2004, IP3 002507–10; Newsgroups: comp.os.os2.networking.tcp–ip.

Google Groups: network settings DHCP mobile, Aug. 3, 2004 IP3 002511–15; Newsgroups: comp.sys.mac.comm.

Google Groups: netswitcher; Aug. 2, 2004; IP3 002516; Newsgroups: comp.os.ms–windows.networking.win95.

Product Information—Netswitcher, the ultimate windows network setup utility; Aug. 2, 2004; IP 3 002517; Netswitcher™, Developed and Marketed by J.W. Hance, 1950–18 E. Greyhound Pass, Suite 305, Carmel, Indiana 46033 USA.

Google Groups: network laptop settings, Jul. 30, 2004; IP3 002767–68; Laptop on Dual Networks; Newsgroups: comp.os.ms–windows.nt.admin.networking.

Google Groups: network configuration laptop packets; Aug. 2, 2004 IP3 002765–66; Newsgroups: comp.protocols.tcp–ip.

Google Groups: "home network" laptop; Aug. 3, 2004; IP3 002769–70; Newsgroups: comp.sys.sun.admin. Newsgroups: comp.sys.sun.admin.

Google Groups: redirect "login page" Jul. 28, 2004; IP 3 002873–74; Newsgroups: microsoft.public.inetserver.iis.activeserverpages.

Yutaka Sato, "Details of Functions of Multi–purposeProxy Server DeleGate–Access/Route Control and Protocol Conversion", Interface vol. 21, No. 9, p. 130–146.

ATCOM/Info and Microsoft Plan Large–Scale Deployment of IPORT for Mid–1998, ATCOM–IPORT Press Release Mar. 4, 1998.

Hotel Online Special Report, Internet Access for the Road Warrior Easier Than Ever, IPORT™ Version 2.0 Released, ATCOM–IPORT Press Release Jul. 20, 1998.

Internet Access: ATCOM/Info Releases IPORT Central Office Solution. IPORT–CO Makes Plug & Play High–Speed Internet Access Possible too Multiple Properties from a Single Server–Product Announcement, ATCOM–IPORT Press Release Oct. 26, 1998.

Yutaka Sato, "Details of Functions of Multi–purpose Proxy Server DeleGate–Access/Route Control and Protocol Conversion", Interface vol. 21, No. 9, p. 130–146, Sep. 1995.

Nomadic Computing—An Opportunity, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: ACM SIGCOMM, Computer Communications Review, Publication Date: Jan. 1995, vol. 25, Issue: 1.

Nomadicity in the NII, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: Cross–Industry Working Team Papers & Reports, Publication Date: Jun. 1995.

Nomadic Computing, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: Information Network and Data Communications, IFIP/ICCC International Conference on Information Network and Data Communication, Publication Date: Jun. 1996, Location Trondheim, Norway.

Nomadicity: Anytime, Anywhere in a Disconnected World, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: Mobile Network and Applications, Special Issue on Mobile Computing and System Services, Publication Date: Dec. 1996, vol. 1, Issue: 4.

Review of Roaming Implementations, Aboba, B., Published as a RFC by ISOC, Sep. 1, 1997 UTC IP.com Document ID: IPCOM000002752D.

Network Layer Mobility: an architechture and survey Bhagwat, P. Perkins, C. Tripathi, S., Personal Communications, IEEE, Publication Date: Jun. 1996, vol. 3, Issue 3.

Classical versus Transparent IP Proxies (RFC1919), published as an RFC by ISOC on Mar. 1, 1996, M. Chatel.

Mobile IP–based multicast as a service for mobile hosts, Chikarmane, V., Dept. of Comput. Sci., Saskatchewan Univ., Saskatoon, Sask., Publication Date; Jun. 5–6, 1995.

A Virtual Home Agent Based Route Optimization for Mobile IP, Qiang Gao, Wireless Communications and Networking Conferences, 2000. WCNC. 2000 IEEE, Publication Date: Sep. 23–28, 2000, vol. 2.

Requirements for Policy–Based Management of Nomadic Computing Infrastructures, S. Heilbronner. Requirements for Policy–Based Management of Nomadic Computing Infrastructures. Proc. of the Sixth Workshop of the HP Openview University Association (HPOVUA'99), Bologna, Italy, Jun. 1999.

Automatically Configure a System to Route Internet Traffic to a Proxy, D. Liu, Originally disclosed by IBM on Apr. 1, 1999 UTC, RD v42 n420 04–99 article 42099.

Interactive Billing for Broadband and Multimedia Services Loeb, S., Community Networking, 1995. Publication Date: Jun. 20–22, 1995, Princeton, NJ.

AAA Protocols; Authentication, Authorization, and Accounting for the Internet, Metz, C. Internet Computing, IEEE, vol. 3, No. 6, pp. 75–79, Nov./Dec. 1999.

A Survey of Active Network Research, Tennenhouse, D.L. Smith, J.M. Sincoskie, W.D. Wetherall, D.J. Minden, G.J. Communications Magazine, IEEE, Publication Date: Jan. 1997, vol. 35, Issue: 1.

An Efficient Multicast Delivery Scheme to Support Mobile IP, Chu–Sing Yang, Database and Expert Systems Applications, 1999. Publication Date: Sep. 1–3, 1999.

A Mobile Networking System Based on Internet Protocol, Perkins, C.E., Bhagwat, P., Personal Communications, IEEE, Publication Date: 1st Qtr 1994, vol. 1, Issue: 1.

Nomadix, Inc. v *Second Rule LLC,* Civil Action No. 07–1946 DDP (VBKx), Expert Report of Peter Alexander, Ph.D. Regarding Invalidity of U.S. Patent Nos. 6,130,892; 6,636,894; 6,868,399; 7,088,727; 6,857,009.

TCP/IP Illustrated, The Protocols, vol. 1, W. Richard Stevens, pp. 53–62 and 231–235. 1994. ("Stevens").

"System Administration: IP Masquerading Code Follow–Up," Linux Journal archive, vol. 1997, Issue 43es, (Nov. 1997)ISSN:1075–3583, Chris Kostick ("Kostick97").
Building a Linux Firewall, Christ Kostick, Linux Journal 24, Apr. 1, 1996.
Linux as a Proxy Server, Linux Journal archive, vol. 1997, Issue 44 (Dec. 1997) Article 3, ISSN: 1075–3583, Peter Elton. ("Elton97") See http://portal.acm.org/citation.cfm?id=327077.327080.
IP Masquerading with Linux, Chris Kostick, Linux Journal Issue 27, Jul. 1996 ("Kostick96") See http://portal.acm.org/citation.cfm?id=328288.328289.
RFC 1009 Braden et al. "Requirements for Internet Gateways," Jun. 1987.
RFC 1027 "Using ARP to Implement Transparent Subnet Gateways," Carl–Mitchell et al, Oct. 1987.
RFC 1919, M. Chatel, Classical Versus Transparent IP Proxies, Mar. 1996.
Single–User Network Access Security TACAS+ http://www.cisco.com/warp/public/614/7.html IP3 002876–002884.
Building Internet Firewalls, D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, Inc., 103 Morris Street, Suite A. Sebastopol, CA 95472, IP3 002885–002944.
Internet Protocol, Darpa Internet Program, Protocol Specification, Sept. 1981, prepared for Defense Advanced Research Projects Agency, IP3 002945–002990.
Networking Working Group, Radius Accounting, Request for Comments: 21 39, Obsoletes: 2059; Category: Informational, C. Rigney, Livingston, Apr. 1997; IP 3 002991–003013.
U.S. Appl. No. 08/816,174, filed Mar. 12, 2997.
L Kleinrock, "Nomadic Computing" (Keystone address) *Int'l Conf. on Mobile Computing and Networking,* 1995, Berkeley, California, ACM.
M. Baker et al., Supporting Mobility in MosquitoNet, Proceedings of the 1996 Usenix Technical Conference, San Diego, CA, Jan. 1996.
Comer, "Internetworking With TCP/IP vol. 1, Chapter 10, Principles, Protocols, and Architecture," 3rd ed., Prentice Hall 1995.

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

NO AMENDMENTS HAVE BEEN MADE TO THE PATENT

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1–8** is confirmed.

* * * * *

US007088727B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 7,088,727 B1**
(45) **Date of Patent: Aug. 8, 2006**

(54) **SYSTEM AND METHOD FOR ESTABLISHING NETWORK CONNECTION WITH UNKNOWN NETWORK AND/OR USER DEVICE**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Leonard Kleinrock**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 927 days.

(21) Appl. No.: **09/684,937**

(22) Filed: **Oct. 6, 2000**

Related U.S. Application Data

(63) Continuation of application No. 09/041,534, filed on Mar. 12, 1998, now Pat. No. 6,130,892, which is a continuation-in-part of application No. 08/816,174, filed on Mar. 12, 1997, now abandoned.

(51) **Int. Cl.**
H04J 3/16 (2006.01)
H04L 12/56 (2006.01)

(52) **U.S. Cl.** **370/401**; 370/338; 370/466
(58) **Field of Classification Search** 370/401, 370/338, 389, 466, 392, 229, 252, 390, 393, 370/395, 397, 400, 402, 404, 406, 409, 465, 370/467, 254, 255, 408; 709/238, 220, 228, 709/221, 242, 230, 245, 225, 222, 223, 219, 709/226, 229
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592 A 10/1992 Perkins
5,309,437 A 5/1994 Perlman
5,325,362 A 6/1994 Aziz
5,371,852 A 12/1994 Attanasio et al.
5,412,654 A 5/1995 Perkins

(Continued)

FOREIGN PATENT DOCUMENTS

JP	5-344122	12/1993
JP	5344122 A2	12/1993
JP	7066809	3/1995
JP	8065306 A2	3/1996
WO	WO 97/11429	3/1997

OTHER PUBLICATIONS

Network Working Group, The IP Network Address Translator (NAT) (May 1994) www.ftp.isi.edu/in-notes/rfc1631.txt.
Official Communication mailed Nov. 22, 2005 for EP Patent Appl. No. EP 98 909 121.0.
U.S. Appl. No. 6,130,892, filed Feb. 15, 2005 Request for Reexamination.

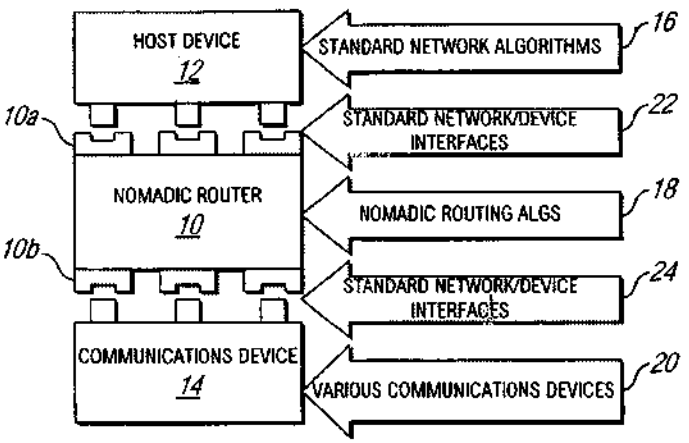
(Continued)

Primary Examiner—Ajit Patel
(74) *Attorney, Agent, or Firm*—Brooks Kushman P.C.

(57) **ABSTRACT**

A system and method for connecting a user device to a network where the user device settings, the network settings, or both are unknown include intercepting packets transmitted by the user device and modifying the packets to be compatible with the network. The system and method are particularly suited for use by mobile computers, such as laptop computers, which are connected to various foreign networks. Depending upon the particular application, a device may be carried with the mobile computer, or attached as a node on the network. The device automatically determines the network settings of the user device and/or the network and modifies packets appropriately so that the user device can communicate over the network without having to reconfigure the user device with appropriate settings for each network it may encounter. Communication settings such as network address, gateway, proxy address, etc. are automatically determined using various techniques.

20 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

5,425,029	A		6/1995	Hluchyj et al.	
5,442,633	A		8/1995	Perkins et al.	
5,490,139	A		2/1996	Baker et al.	
5,517,618	A		5/1996	Wada et al.	
5,539,736	A		7/1996	Johnson	
5,557,748	A		9/1996	Norris	
5,572,528	A		11/1996	Shuen	
5,586,269	A		12/1996	Kubo	
5,608,786	A		3/1997	Gordon	
5,636,216	A		6/1997	Fox et al.	
5,651,002	A		7/1997	Van Seters et al.	
5,708,655	A		1/1998	Toth et al.	
5,708,780	A		1/1998	Levergood et al.	
5,751,971	A		5/1998	Dobbins et al.	
5,781,550	A		7/1998	Templin et al.	
5,781,552	A		7/1998	Hashimoto	
5,790,541	A		8/1998	Patrick et al.	
5,793,763	A		8/1998	Mayes	
5,798,706	A		8/1998	Kraemer et al.	
5,802,320	A		9/1998	Baehr et al.	
5,812,531	A		9/1998	Cheung et al.	
5,812,776	A		9/1998	Gifford	
5,841,769	A		11/1998	Okanoue et al.	
5,854,901	A		12/1998	Cole et al.	
5,862,345	A		1/1999	Okanoue et al.	
5,909,549	A		6/1999	Compliment	
5,910,954	A	*	6/1999	Bronstein et al.	370/401
5,915,119	A		6/1999	Cone	
5,918,016	A		6/1999	Brewer et al.	
5,920,699	A		7/1999	Bare	
5,960,409	A		9/1999	Wexler	
5,963,915	A		10/1999	Kirsch	
5,991,828	A		11/1999	Horie et al.	
6,006,272	A		12/1999	Aravamudan et al.	
6,012,088	A		1/2000	Li	
6,014,698	A		1/2000	Griffiths	
6,055,243	A	*	4/2000	Vincent et al.	370/466
6,061,356	A	*	5/2000	Terry	370/401
6,098,172	A		8/2000	Coss et al.	
6,119,162	A		9/2000	Li et al.	
6,226,677	B1		5/2001	Slemmer	
6,249,527	B1	*	6/2001	Verthein et al.	370/466
6,377,990	B1	*	4/2002	Slemmer et al.	709/225
6,410,543	B1		6/2002	Strobel et al.	
6,463,051	B1	*	10/2002	Ford	370/352
6,640,251	B1	*	10/2003	Wiget et al.	709/238
2002/0097674	A1	*	7/2002	Balabhadraptreuni et al.	

OTHER PUBLICATIONS

Copy of patent application for Ser. No. 08/816,174, filed Mar. 12, 1997.

Single–User Network Access Security TACACS+ http://www.cisco.com/warp/public/614/7.html IP3 002876–002884.

Networking Working Group Request For Comments: 826 –Ethernet Address Resolution Protocol (Nov. 1982).

Network Working Group Request For Comments: 894 –Standards For Transmission of IP Datagrams Over Ethernet Networks (Apr. 1984).

Network Working Group Request For Comments: 925 –Multi–LAN Address Resolution (Oct. 1984).

Network Working Group Request For Comments: 1009 –Requirements For Internet Gateways (Jun. 1987).

Network Working Group Request For Comments: 1027 –Using ARP to Implement Transparent Subnet Gateways (Oct. 1987).

Networking Working Group Request For Comments: 1034 –Domain Names –Concepts and Facilities (Nov. 1987).

Network Working Group Request For Comments: 1531 –Dynamic Host Confirmation Protocol (Oct. 1993).

Network Working Group Request For Comments: 1919 –Classical Versus Transparent IP Proxies (Mar. 1996).

Network Working Group Request For Comments: 1945 –Hypertext Transfer Protocol –HTTP/1.0 (May 1996).

L. Kleinrock, "Nomadic Computing" (Keynote address) *Int'l Conf. on Mobile Computing and Networking,* 1995, Barkeley, California, ACM.

M. Baker et al., Supporting Mobility in MosquitoNet, Proceedings of the 1996 USENIX Technical Conference, San Diego, CA, Jan. 1996.

Comer, "Internetworking With TCP/IP vol. 1, Chapter 10, Principles, Protocols, and Architecture", 3rd ed., Prentice Hall 1995.

Joel E. Short: "Auto–Porting and Rapid Prototyping with Application to Wireless and Nomadic Network Algorithms, A dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Computer Science", University of California, Los Angeles; Published Oct. 26, 1996; pp. xv, 118–124; Copyright Jan. 16, 1997.

Case No. 04CV11485 BTM (POR): IP3 Networks, Inc. v Nomadix, Inc. –Jul. 23, 2004 Complaint for: (1) Declaratory Judgement of Patent Non–Infringement and Invalidity of U.S. Appl. No. 6,636,894; (2) Declaratory Judgement of Patent Non–Infridgement of U.S. Appl. No. 6,130,893; (3) Trade Libel; (4) Libel Under Cal. Civ. Code § 45; (5) Unfair Competition Under Cal. Bus.& Prof. Code § 17200, Et Seq.; and (6) Intentional Interference with Prospective Economic Advantage –Demand for Jury Trial.

Case No. 04CV1485 BTM (POR): IP3 Neworks, Inc. v Nomadix, Inc. –Oct. 21, 2004 Answer and Counterclaims of Nomadix, Inc. to the Amended Complaint.

Case No. 04CV1485 BTM (POR): IP3 Networks, Inc. v Nomadix, Inc. –Plaintiff/Counter–Defendant IP3 Networks Inc.'s Reply to Defendant Nomadix, Inc.'s Counterclaim.

Perkins C. E. et al.: "DHCP for Mobile networking with TCP/IP" Proceedings IEEE International Symposium on Computers and Communications, Jun. 27, 1995, pp. 255–261, XP002132695.

Perkins C.E. ED –Institute of Electrical and Electronics Engineers: "Mobile–AP, AD–HOC Networking, and Nomadicity" Proceedings of the 20th . Annual International Computer Software and Applications Conference (COMPSAC) . Seoul, Aug. 21–23, 1996, Proceedings of the Annual International Computer Software and Applications Conference (COMPSAC), Los Alamitos, IEEE Comp. vol. CONF. 20, Aug. 21, 1996, pp. 472–476, XP 000684381. ISBN 0–8186–7579–9.

The Patent Office of the People's Republic of China Notification of First Office Action (PCT Application) and its translation for Chinese patent application 98 8 05023.4.

Google Groups: View Thread, Aug. 2, 2004, IP3 002505–06; Newsgroups: microsoft, public.win95.networking.

Google Groups: View Thread, Aug. 2, 2004, IP3 002507–10; Newsgroups: comp.os.os2.networking.tcp–ip.

Google Groups: network settings DHCP mobile, Aug. 3, 2004 IP3 002511–15; Newsgroups: comp.sys.mac.comm.

EXHIBIT 3

Google Groups: netswitcher; Aug. 2, 2004; IP3 002516; Newsgroup: comp.os.ms–windows.networking.win95; .

Product Information –Netswitcher, the ultimate windows network setup utility; Aug. 2, 2004; IP 3 002517; Netswitcher™, Developed and Marketed by: J.W. Hance, 1950–18 E. Greyhound Pass, Suite 305, Carmel, Indiana 46033 USA.

Google Groups: network laptop settings, Jul. 30, 2004; IP3 002767–68; Laptop on Dual Networks; Newsgroups: comp.os.ms–windows.nt.admin.networking.

Google Groups: network configuration laptop packets; Aug. 2, 2004 IP3 002765–66; Newsgroups: comp.protocols.tcp–ip.

Google Groups: "home network" laptop; Aug. 3, 2004; IP3 002769–70; Newsgroups: comp.sys.sun.admin. Newsgroups: comp.sys.sun.admin.

Google Groups: redirect "login page" Jul. 28, 2004; IP 3 002873–74; Newsgroup: microsoft.public,inetserver.iis.activeserverpages.

* cited by examiner

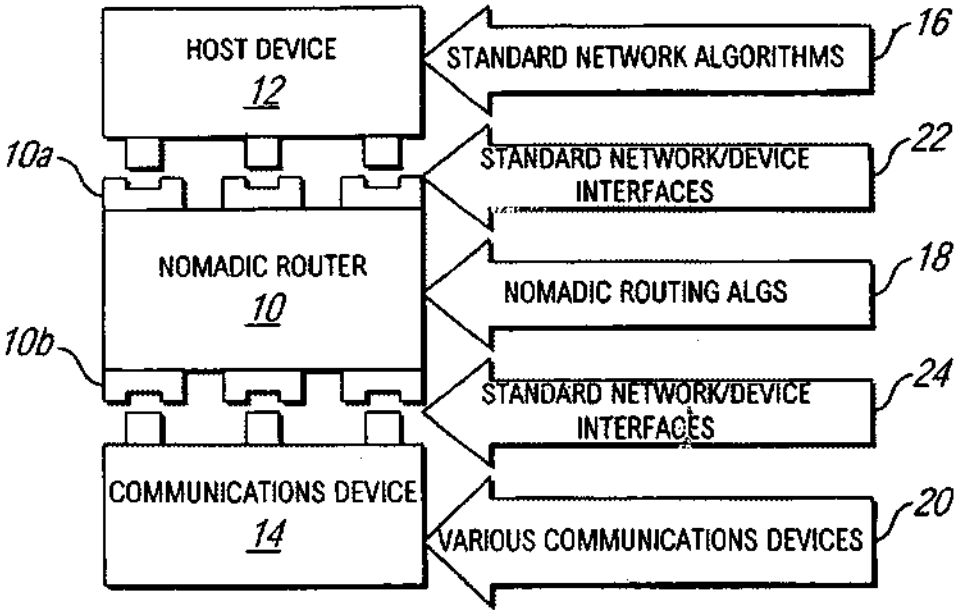

HOST DEVICE
12
10a
NOMADIC ROUTER
10
10b
COMMUNICATIONS DEVICE
14
STANDARD NETWORK ALGORITHMS
16
STANDARD NETWORK/DEVICE INTERFACES
22
NOMADIC ROUTING ALGS
18
STANDARD NETWORK/DEVICE INTERFACES
24
VARIOUS COMMUNICATIONS DEVICES
20

FIG. 1

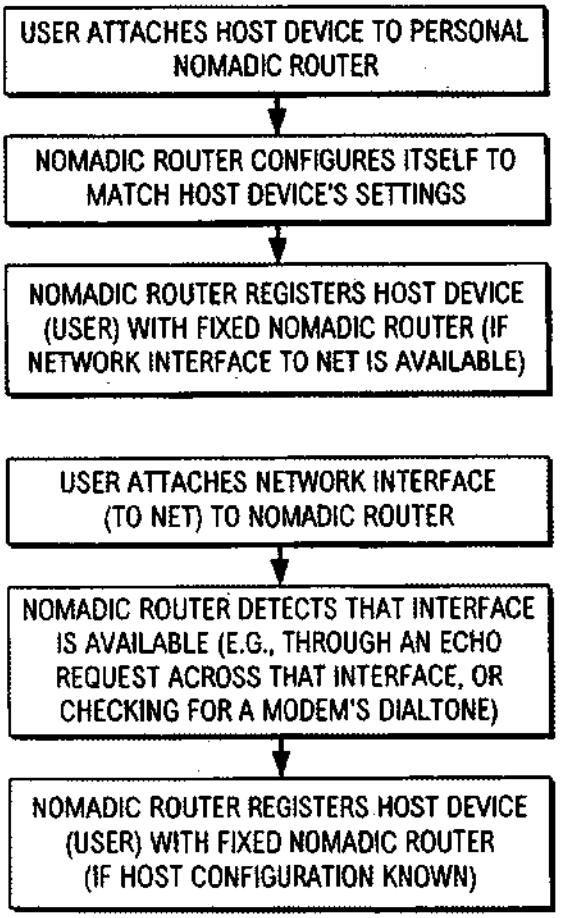

USER ATTACHES HOST DEVICE TO PERSONAL NOMADIC ROUTER
NOMADIC ROUTER CONFIGURES ITSELF TO MATCH HOST DEVICE'S SETTINGS
NOMADIC ROUTER REGISTERS HOST DEVICE (USER) WITH FIXED NOMADIC ROUTER (IF NETWORK INTERFACE TO NET IS AVAILABLE)
USER ATTACHES NETWORK INTERFACE (TO NET) TO NOMADIC ROUTER
NOMADIC ROUTER DETECTS THAT INTERFACE IS AVAILABLE (E.G., THROUGH AN ECHO REQUEST ACROSS THAT INTERFACE, OR CHECKING FOR A MODEM'S DIALTONE)
NOMADIC ROUTER REGISTERS HOST DEVICE (USER) WITH FIXED NOMADIC ROUTER (IF HOST CONFIGURATION KNOWN)

FIG. 3

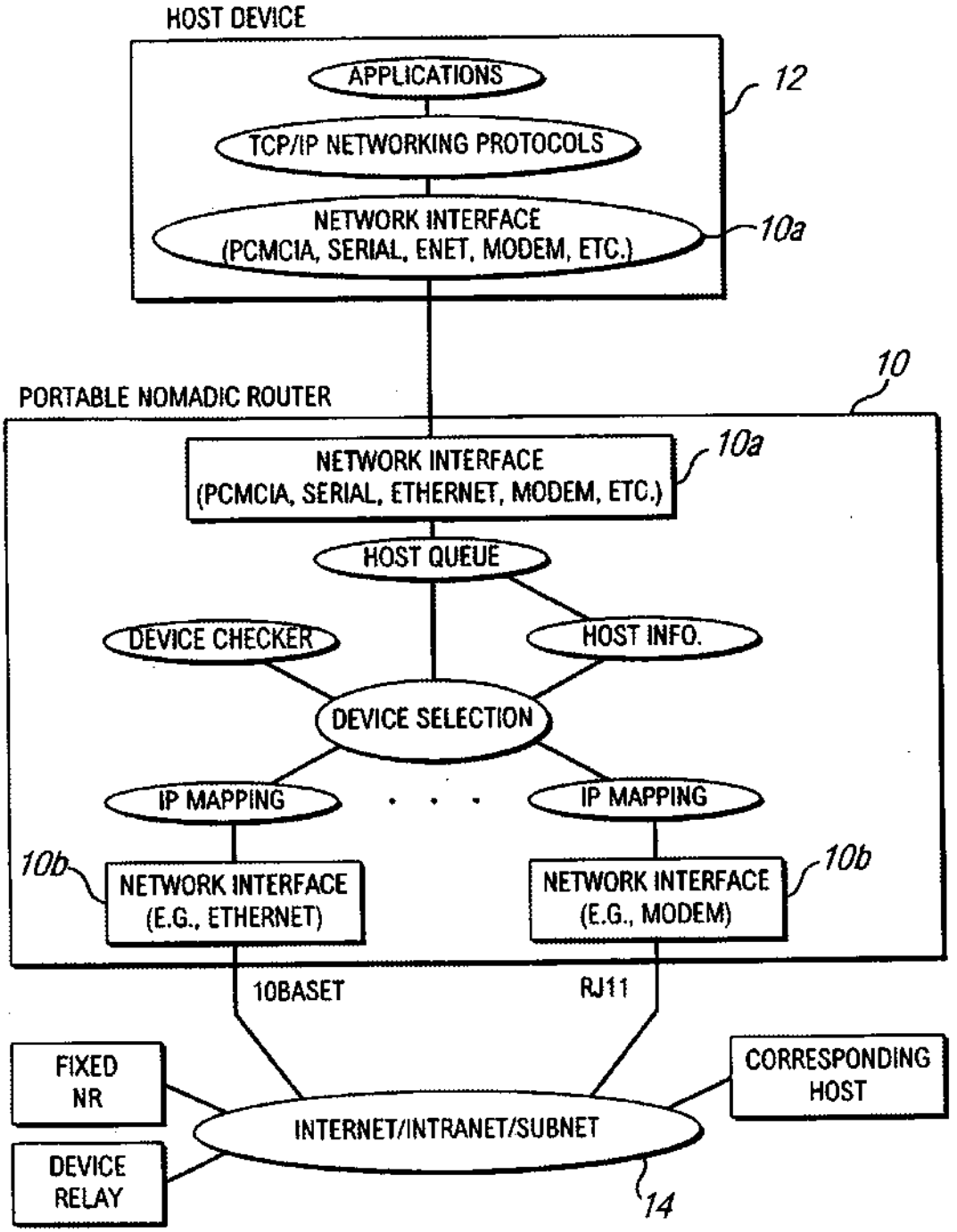

HOST DEVICE
APPLICATIONS
TCP/IP NETWORKING PROTOCOLS
NETWORK INTERFACE
(PCMCIA, SERIAL, ENET, MODEM, ETC.)
12
10a
10
PORTABLE NOMADIC ROUTER
NETWORK INTERFACE
(PCMCIA, SERIAL, ETHERNET, MODEM, ETC.)
10a
HOST QUEUE
DEVICE CHECKER
HOST INFO.
DEVICE SELECTION
IP MAPPING
IP MAPPING
10b
NETWORK INTERFACE
(E.G., ETHERNET)
NETWORK INTERFACE
(E.G., MODEM)
10b
10BASET
RJ11
FIXED
NR
DEVICE
RELAY
INTERNET/INTRANET/SUBNET
CORRESPONDING
HOST
14

FIG. 2

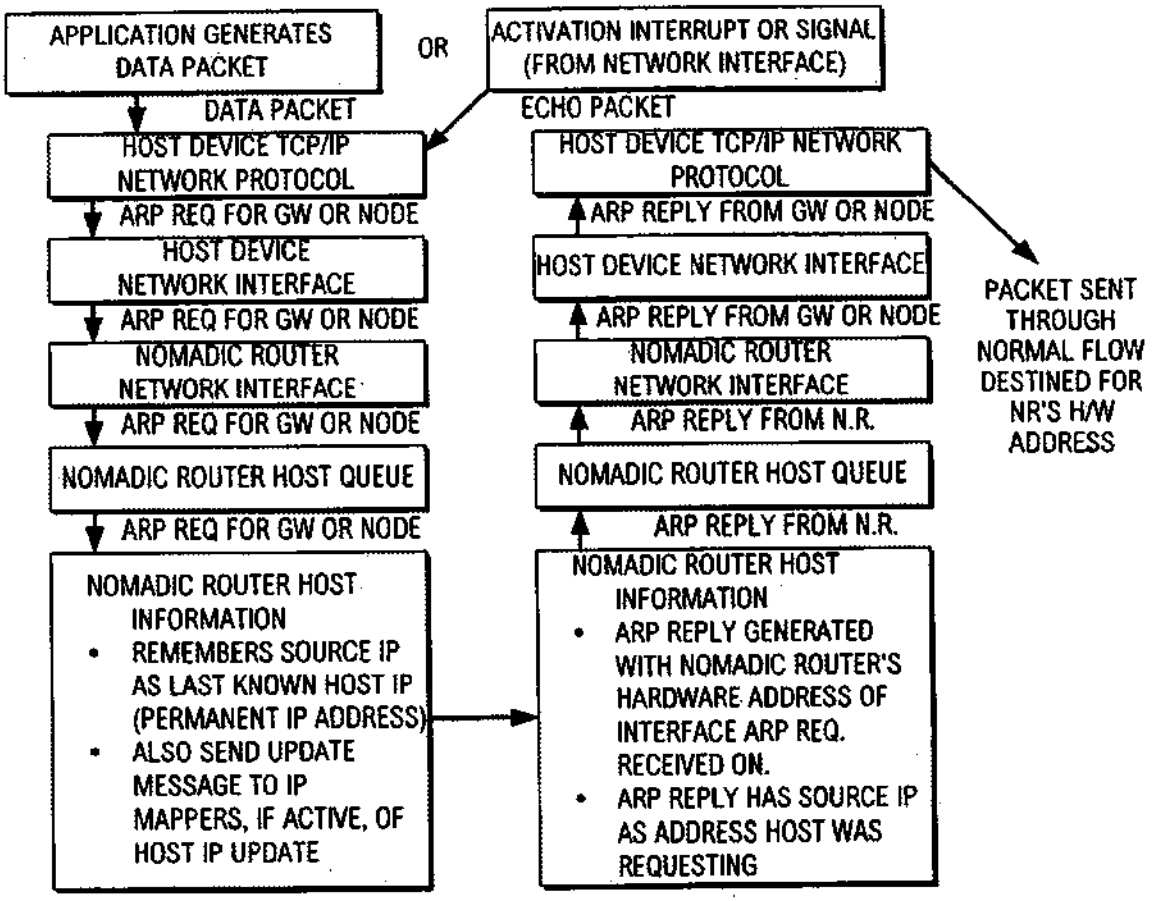

APPLICATION GENERATES DATA PACKET
OR
ACTIVATION INTERRUPT OR SIGNAL (FROM NETWORK INTERFACE)
DATA PACKET
ECHO PACKET
HOST DEVICE TCP/IP NETWORK PROTOCOL
HOST DEVICE TCP/IP NETWORK PROTOCOL
ARP REQ FOR GW OR NODE
ARP REPLY FROM GW OR NODE
HOST DEVICE NETWORK INTERFACE
HOST DEVICE NETWORK INTERFACE
ARP REQ FOR GW OR NODE
ARP REPLY FROM GW OR NODE
NOMADIC ROUTER NETWORK INTERFACE
NOMADIC ROUTER NETWORK INTERFACE
ARP REQ FOR GW OR NODE
ARP REPLY FROM N.R.
NOMADIC ROUTER HOST QUEUE
NOMADIC ROUTER HOST QUEUE
ARP REQ FOR GW OR NODE
ARP REPLY FROM N.R.
NOMADIC ROUTER HOST INFORMATION
• REMEMBERS SOURCE IP AS LAST KNOWN HOST IP (PERMANENT IP ADDRESS)
• ALSO SEND UPDATE MESSAGE TO IP MAPPERS, IF ACTIVE, OF HOST IP UPDATE
NOMADIC ROUTER HOST INFORMATION
• ARP REPLY GENERATED WITH NOMADIC ROUTER'S HARDWARE ADDRESS OF INTERFACE ARP REQ. RECEIVED ON.
• ARP REPLY HAS SOURCE IP AS ADDRESS HOST WAS REQUESTING
PACKET SENT THROUGH NORMAL FLOW DESTINED FOR NR'S H/W ADDRESS

FIG. 4

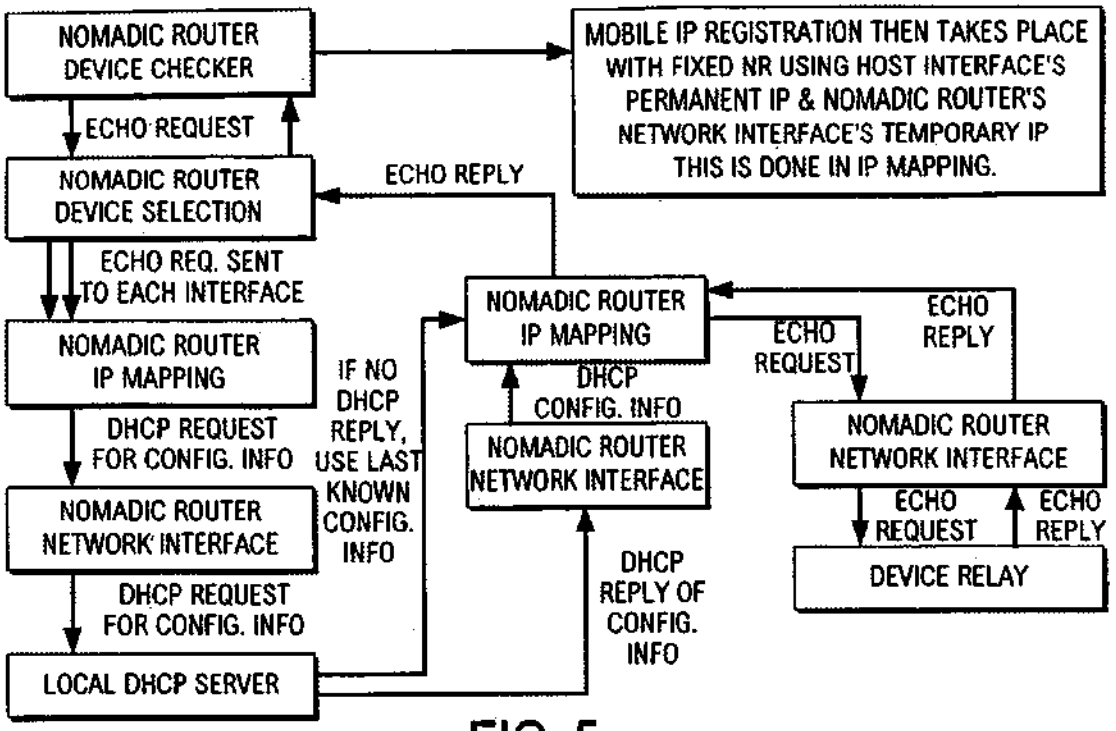

NOMADIC ROUTER DEVICE CHECKER
MOBILE IP REGISTRATION THEN TAKES PLACE WITH FIXED NR USING HOST INTERFACE'S PERMANENT IP & NOMADIC ROUTER'S NETWORK INTERFACE'S TEMPORARY IP THIS IS DONE IN IP MAPPING.
ECHO REQUEST
ECHO REPLY
NOMADIC ROUTER DEVICE SELECTION
ECHO REQ. SENT TO EACH INTERFACE
NOMADIC ROUTER IP MAPPING
NOMADIC ROUTER IP MAPPING
ECHO REQUEST
ECHO REPLY
DHCP CONFIG. INFO
DHCP REQUEST FOR CONFIG. INFO
IF NO DHCP REPLY, USE LAST KNOWN CONFIG. INFO
NOMADIC ROUTER NETWORK INTERFACE
NOMADIC ROUTER NETWORK INTERFACE
ECHO REQUEST
ECHO REPLY
DHCP REQUEST FOR CONFIG. INFO
DHCP REPLY OF CONFIG. INFO
DEVICE RELAY
LOCAL DHCP SERVER

FIG. 5

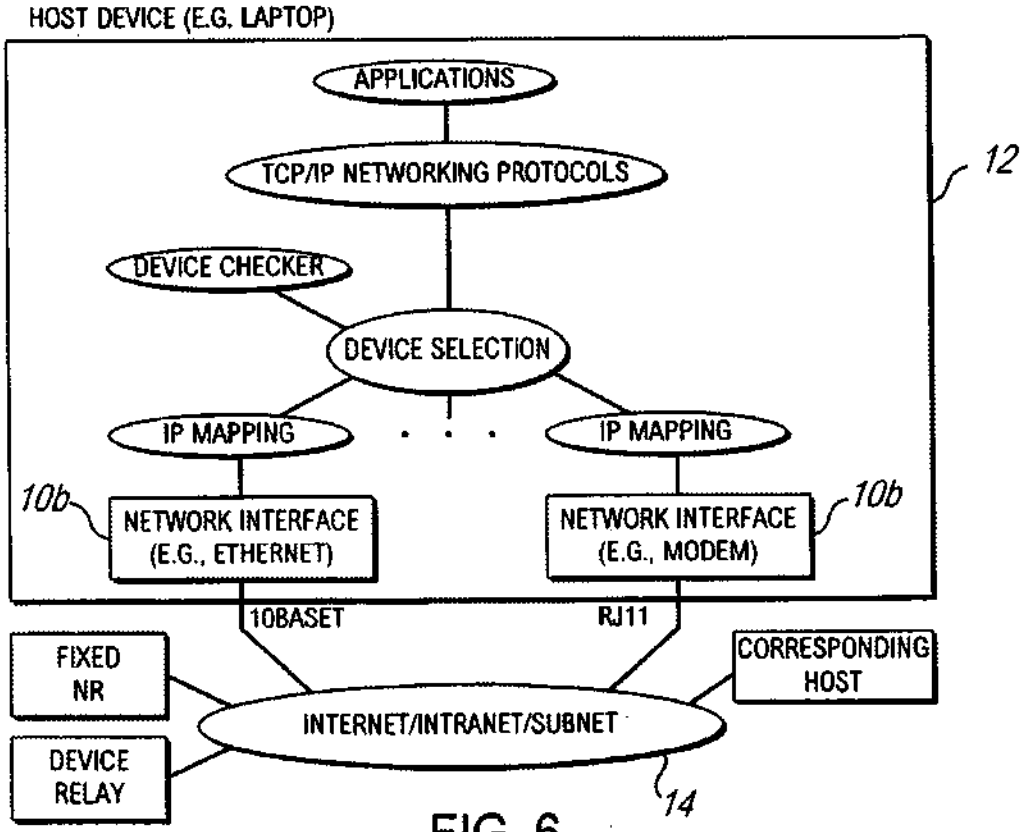

HOST DEVICE (E.G. LAPTOP)
APPLICATIONS
TCP/IP NETWORKING PROTOCOLS
12
DEVICE CHECKER
DEVICE SELECTION
IP MAPPING
IP MAPPING
10b
NETWORK INTERFACE (E.G., ETHERNET)
NETWORK INTERFACE (E.G., MODEM)
10b
10BASET
RJ11
FIXED NR
CORRESPONDING HOST
INTERNET/INTRANET/SUBNET
DEVICE RELAY
14

FIG. 6

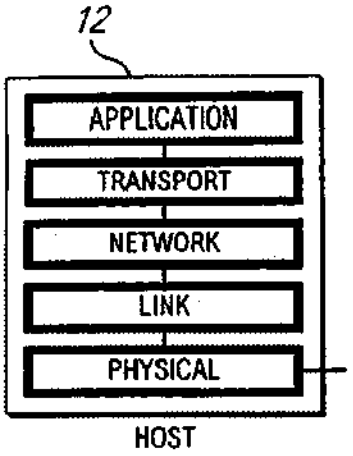


FIG. 7A

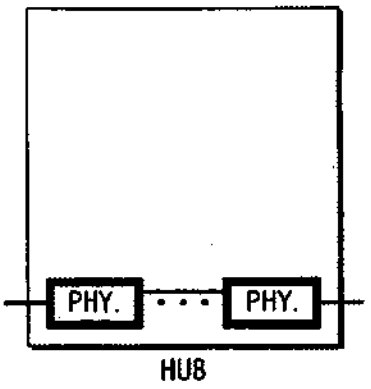


FIG. 7B

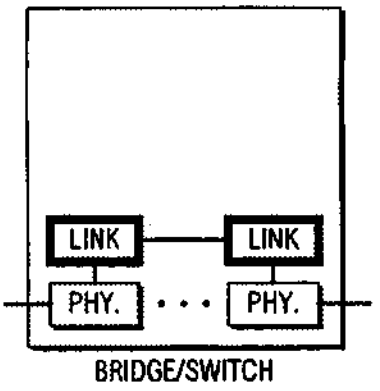


FIG. 7C

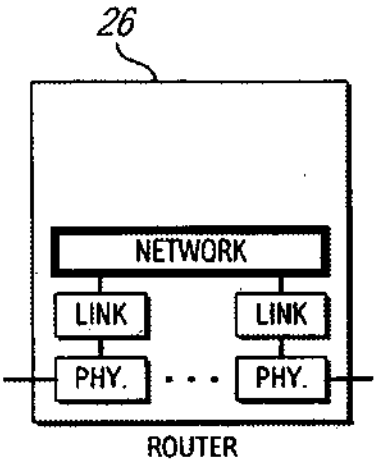


FIG. 7D

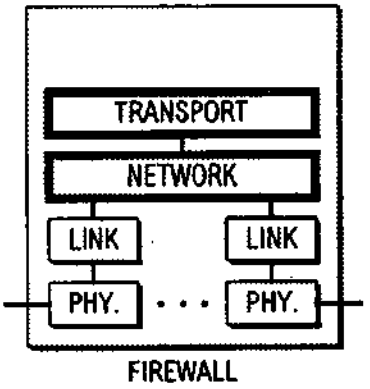


FIG. 7E

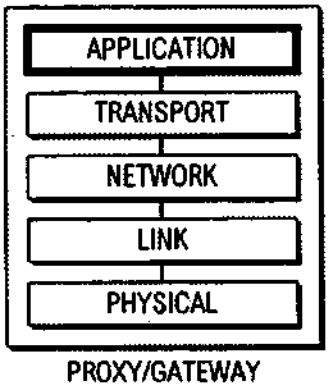


FIG. 7F

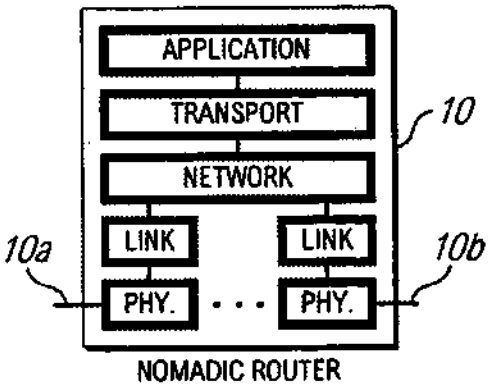


FIG. 7G

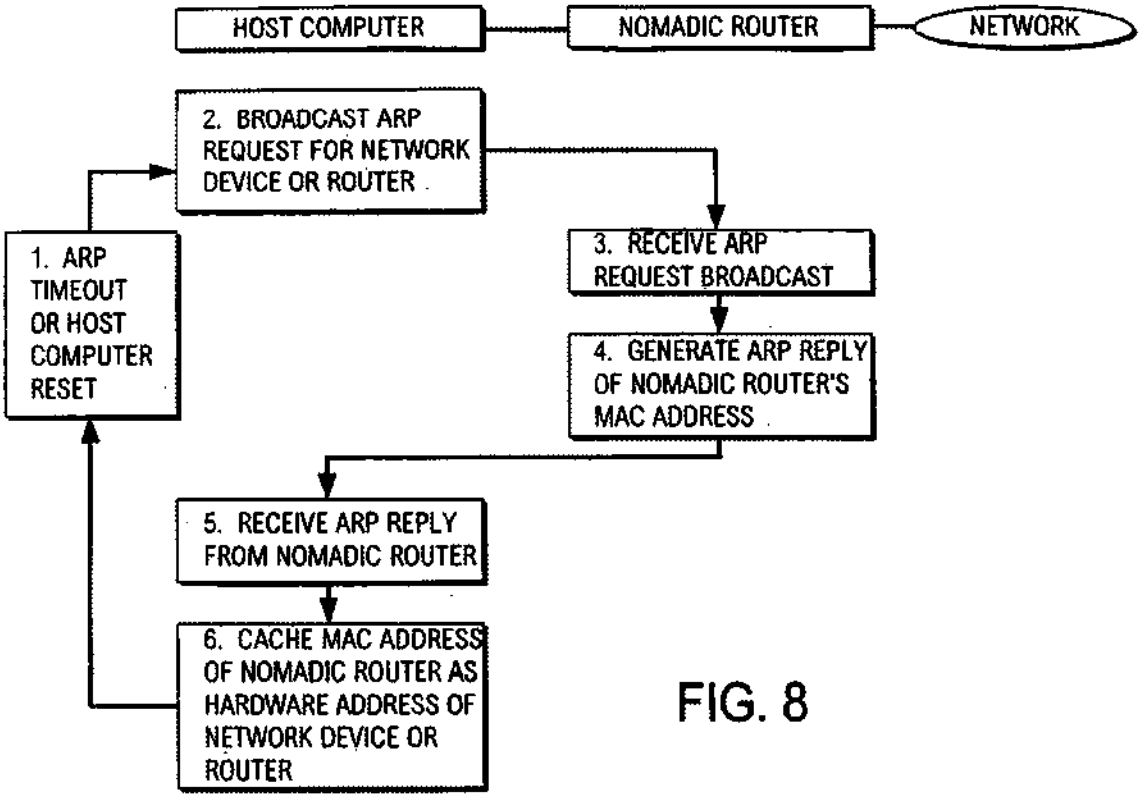

HOST COMPUTER
NOMADIC ROUTER
NETWORK
2. BROADCAST ARP REQUEST FOR NETWORK DEVICE OR ROUTER
1. ARP TIMEOUT OR HOST COMPUTER RESET
3. RECEIVE ARP REQUEST BROADCAST
4. GENERATE ARP REPLY OF NOMADIC ROUTER'S MAC ADDRESS
5. RECEIVE ARP REPLY FROM NOMADIC ROUTER
6. CACHE MAC ADDRESS OF NOMADIC ROUTER AS HARDWARE ADDRESS OF NETWORK DEVICE OR ROUTER

FIG. 8

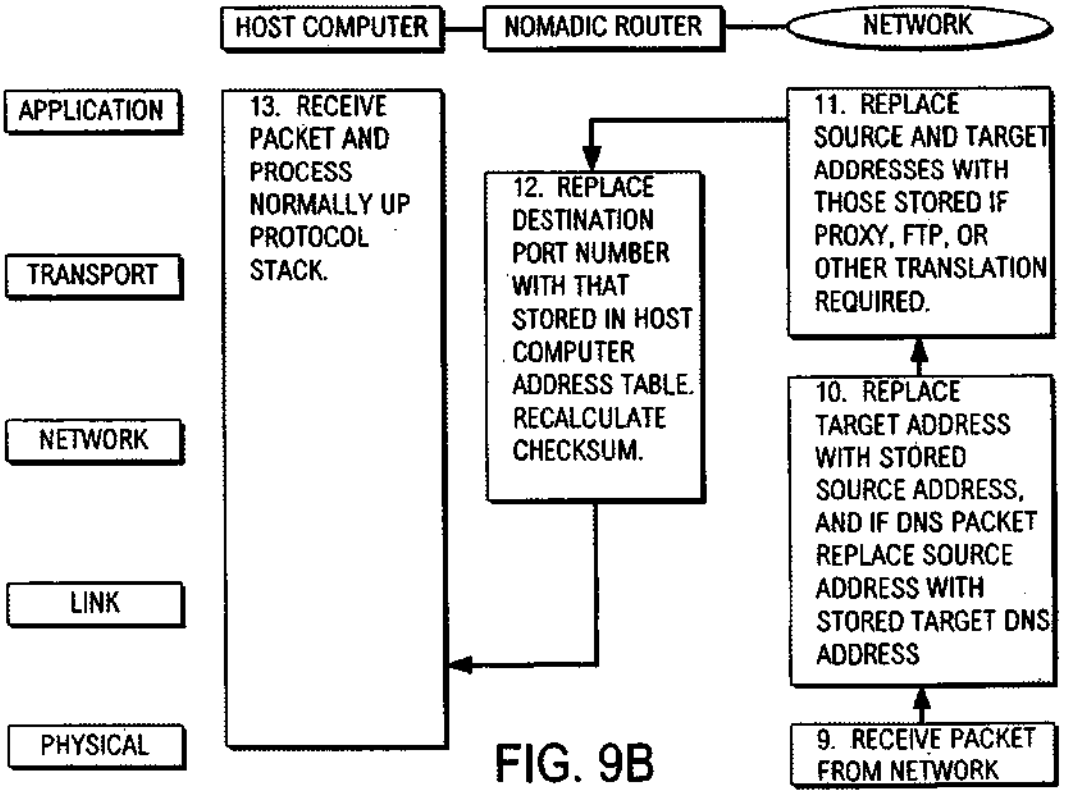

HOST COMPUTER
NOMADIC ROUTER
NETWORK
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
13. RECEIVE PACKET AND PROCESS NORMALLY UP PROTOCOL STACK.
12. REPLACE DESTINATION PORT NUMBER WITH THAT STORED IN HOST COMPUTER ADDRESS TABLE. RECALCULATE CHECKSUM.
11. REPLACE SOURCE AND TARGET ADDRESSES WITH THOSE STORED IF PROXY, FTP, OR OTHER TRANSLATION REQUIRED.
10. REPLACE TARGET ADDRESS WITH STORED SOURCE ADDRESS, AND IF DNS PACKET REPLACE SOURCE ADDRESS WITH STORED TARGET DNS ADDRESS
9. RECEIVE PACKET FROM NETWORK

FIG. 9B

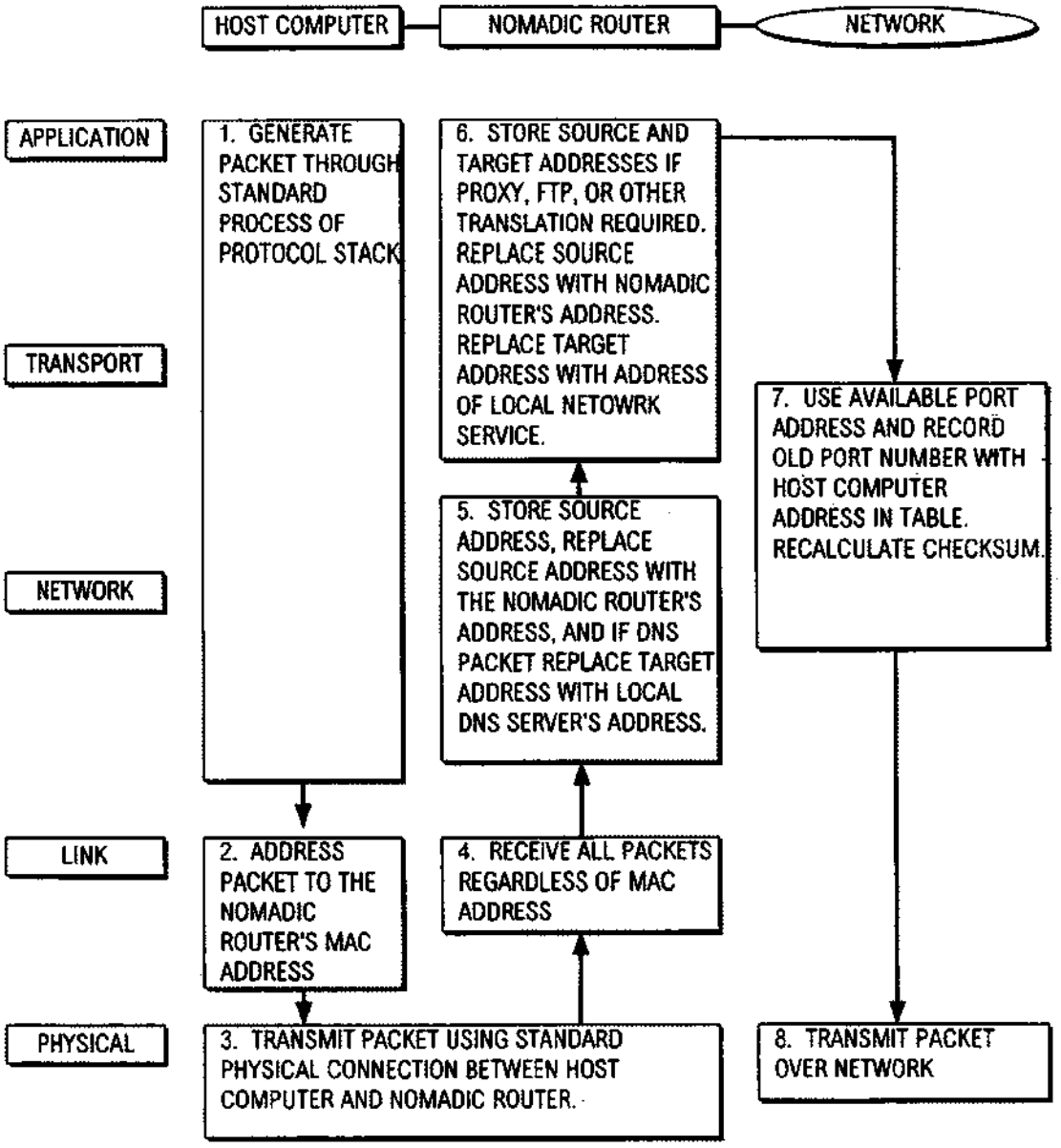

HOST COMPUTER
NOMADIC ROUTER
NETWORK
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
1. GENERATE PACKET THROUGH STANDARD PROCESS OF PROTOCOL STACK
2. ADDRESS PACKET TO THE NOMADIC ROUTER'S MAC ADDRESS
3. TRANSMIT PACKET USING STANDARD PHYSICAL CONNECTION BETWEEN HOST COMPUTER AND NOMADIC ROUTER.
4. RECEIVE ALL PACKETS REGARDLESS OF MAC ADDRESS
5. STORE SOURCE ADDRESS, REPLACE SOURCE ADDRESS WITH THE NOMADIC ROUTER'S ADDRESS, AND IF DNS PACKET REPLACE TARGET ADDRESS WITH LOCAL DNS SERVER'S ADDRESS.
6. STORE SOURCE AND TARGET ADDRESSES IF PROXY, FTP, OR OTHER TRANSLATION REQUIRED. REPLACE SOURCE ADDRESS WITH NOMADIC ROUTER'S ADDRESS. REPLACE TARGET ADDRESS WITH ADDRESS OF LOCAL NETOWRK SERVICE.
7. USE AVAILABLE PORT ADDRESS AND RECORD OLD PORT NUMBER WITH HOST COMPUTER ADDRESS IN TABLE. RECALCULATE CHECKSUM.
8. TRANSMIT PACKET OVER NETWORK

FIG. 9A

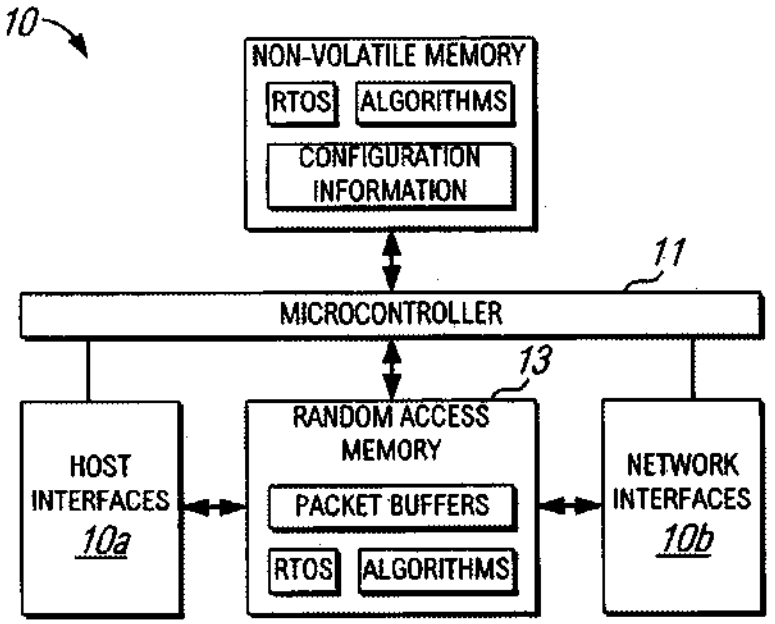

10
NON-VOLATILE MEMORY
RTOS
ALGORITHMS
CONFIGURATION INFORMATION
11
MICROCONTROLLER
13
RANDOM ACCESS MEMORY
PACKET BUFFERS
RTOS
ALGORITHMS
HOST INTERFACES
10a
NETWORK INTERFACES
10b

FIG. 10

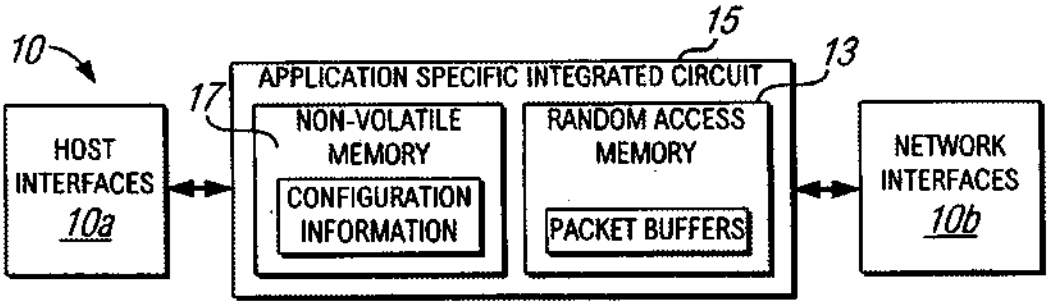

10
15
13
17
APPLICATION SPECIFIC INTEGRATED CIRCUIT
NON-VOLATILE MEMORY
CONFIGURATION INFORMATION
RANDOM ACCESS MEMORY
PACKET BUFFERS
HOST INTERFACES
10a
NETWORK INTERFACES
10b

FIG. 11

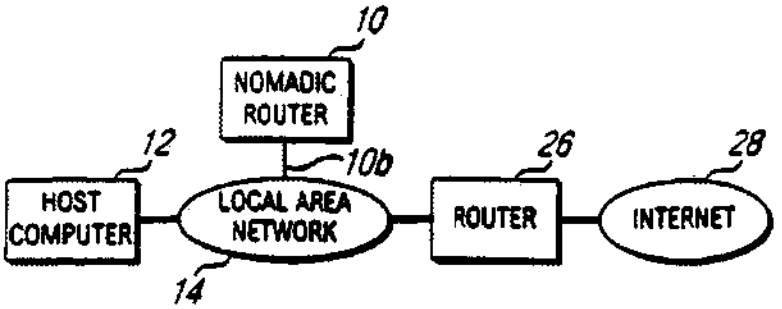


FIG. 12A

FIG. 12B

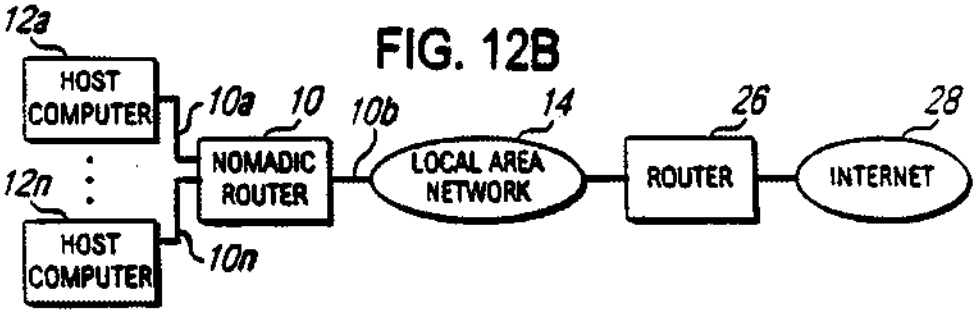


FIG. 12C

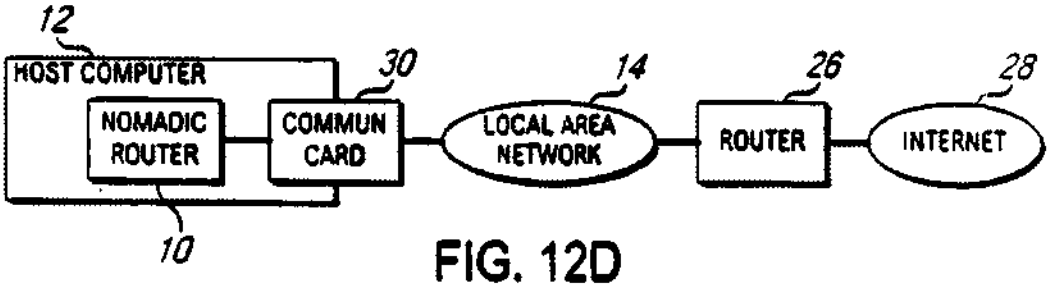


FIG. 12D

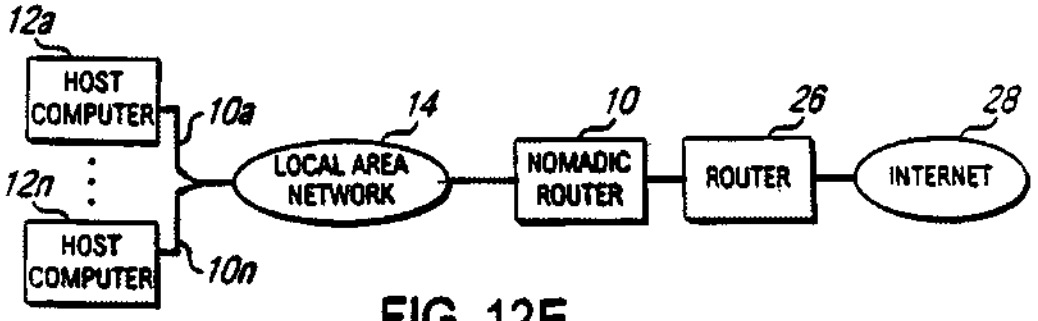


FIG. 12E

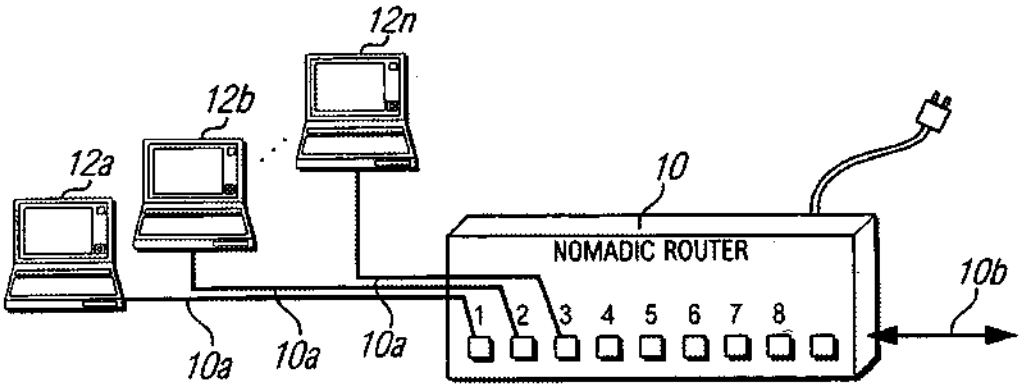


FIG. 13

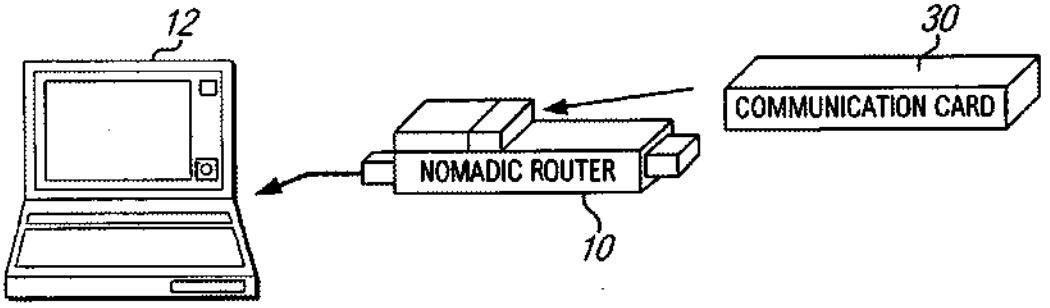


FIG. 14

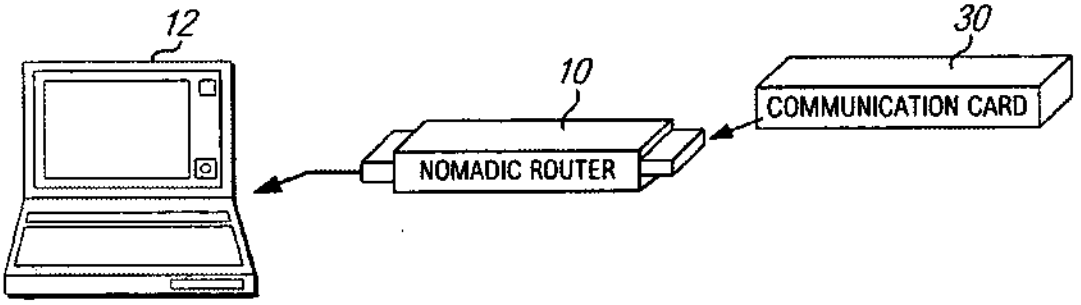


FIG. 15

SYSTEM AND METHOD FOR ESTABLISHING NETWORK CONNECTION WITH UNKNOWN NETWORK AND/OR USER DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. application Ser. No. 09/041,534, filed on Mar. 12, 1998, now U.S. Pat. No. 6,130,892, which is a continuation-in-part of U.S. application Ser. No. 08/816,174, filed on Mar. 12, 1997, now abandoned.

U.S. government may have rights in this invention as provided for by the terms of Contract No. DAAH01-97-C—R179 awarded by DARPA.

TECHNICAL FIELD

The present invention is generally related to the art of network communications.

BACKGROUND ART

User digital communication addresses such as internet or IP addresses are conventionally associated with a fixed physical location, similar to a user's business telephone line. However, portable communication devices such as laptop computers are becoming increasingly popular, and it is common for a user to access the internet from locations as diverse as hotel rooms and airplanes.

Digital communication networks are set up to route communications addressed to a communication or network address to an associated destination computer at an established physical location. Thus, if a laptop computer is moved to a remote location, communications to and from the laptop computer may not reach the new physical location.

For a computer (host) to communicate across a network (e.g., the internet), software protocols (e.g., Transport Control Protocol/Internet Protocol (TCP/IP)) must be loaded into the host. A host computer sends information (i.e., packets of data) to another destination computer via devices on the network (routers) which receive the packets and send the packets to the network or segment of the destination host. The destination host will route replies back using a similar process. Each host computer and router must therefore be configured to send the packets of data to an appropriate router to reach the intended destination. However, a router will receive the packets only if the host computers specifically send (address) the packets to that router at the link layer of the communication protocol. If a host is configured incorrectly (bad address or address of a router not on the local network), then the host computer and router will be unable to communicate, i.e., the router will not listen to the host or will "drop" packets.

With the advent of mobile computers (laptops) and the desire to plug them into various networks to gain access to the resources on the network and internet, a mobile computer must be reconfigured for each network. Traditionally this new configuration can be done either (i) manually in software on the mobile computer (usually causing the mobile computer to be restarted to load the new configuration), or (ii) with a new set of protocols which must be utilized on the mobile computer to obtain the configuration information from a device on the network to which the computer is being connected. When new services (protocols) are created to add functionality to the host computers, these new protocols may need to be updated in the host computers or routers, depending upon the type of new functionality being added.

DISCLOSURE OF INVENTION

In accordance with the present invention, a "Nomadic" router or translator enables a laptop computer or other terminal which is configured to be connected to a local home network to be connected to any location on the internet or other digital data communication system. The nomadic router automatically and transparently reconfigures packets sent to/from the terminal for its new location by processing outgoing and incoming data.

The nomadic router includes a processor which appears as the home network to the terminal, and appears as the terminal to the communication system. The terminal has a terminal address, the nomadic router has a router address, and the terminal transmits outgoing data to the system including the terminal address as a source address. Whether or not the message is addressed to the nomadic router at the link layer, the processor intercepts the message and translates the outgoing data by replacing the permanent address with the router address as the source address. Incoming data intended for the terminal from the system includes the translator address as a destination address, and the processor translates the incoming data by replacing the translator address with the permanent address as the destination address.

The terminal can be directly connected to a point on a local network, and the nomadic router connected to another point on the network. The nomadic router can be employed to implement numerous applications including nomadic e-mail, network file synchronization, database synchronization, instant networking, a nomadic internet, mobile virtual private networking, and trade show routing, and can also be utilized as a fixed nomadic router in hotels, or multi-dwelling units, or multiple tenant units, for example.

The nomadic router can be implemented as software and/or hardware. The nomadic router establishes location and device transparency for a digital communication terminal such as a laptop computer. The terminal can be connected to any of a variety of networks and locations which can employ a variety of communication interface devices.

The nomadic router automatically converts the actual location address to a unique communication address for the user such as an internet address, such that the terminal performs communications originating from the communication address regardless of the physical location of the terminal.

The nomadic router includes software and services which can be packaged in a personal portable device to support a rich set of computing and communications capabilities and services to accommodate the mobility of nomads (users) in a transparent, integrated, and convenient form. This is accomplished by providing device transparency and location transparency to the user.

There is a vast array of communication device alternatives such as Ethernet, Wireless LAN, and dialup modem among which the user switches when in the office, moving around the office, or on the road (such as at a hotel, airport, or home). The device transparency in the nomadic router provides seamless switching among those devices (easily, transparently, intelligently, and without session loss). The location transparency support in the nomadic router prevents users from having to reconfigure (e.g., IP and gateway address) their network device (laptop) each time they move to a new network or subnetwork.

The present nomadic router provides a separation of location and identity by providing a permanent IP address to the network device (host). The nomadic router provides independence between the location, communication device, and the host operating system. There are no new standards which need to be adopted by the networking community. All specialized processing is stored internally to the nomadic router with standard interfaces to the host device and various communication devices.

The nomadic router supports the migration to Network Computers by providing identity and security services for the user. The nomadic router also supports multiple parallel communication paths across the communications network for soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates.

A portable router for enabling a data communication terminal to be location and device transparent according to the present invention, comprises: a first module for storing a digital communication address of a user; a second module for detecting a data communication network location to which the terminal is connected; a third module for detecting communication devices that are connected to the terminal; a fourth module for establishing data communication between the terminal and the network such that the communication address of the location from the second module is automatically converted to the communication address of the user from the first module; and a fifth module for automatically selecting a communication device which was detected by the third module for use by the fourth module.

The present nomadic router utilizes a unique process embodied in a self-contained apparatus which manipulates the packets of data being sent between the host computers and routers. This process provides an intelligent active universal translation of the content of the packets being transmitted between the host computer and nomadic router. The translation allows the host computer to communicate with the nomadic router, which intercepts packets from the host, even when the host computer is not configured to communicate with the nomadic router.

This is achieved by the nomadic router pretending to be the router for which the host is configured, and by the nomadic router pretending to be the host with which the router expects to communicate. Therefore, the nomadic router supports the mobility of computers in that it enables these computers to plug into the network at different locations (location independence) without having to install, configure, or utilize any net protocols on the mobile computer.

The mobile computer continues to operate without being aware of the change in location or configuration of the new network, and the nomadic router translates the data allowing the host to think that it is communicating with its home router. By putting this process in a self-contained apparatus, the deployment of new protocols can be performed independently of the host computer and its operating system (host independent).

All specialized processing and translation is stored internally in the nomadic router with standard interfaces to the host device and various communication devices. Thus, no new standards need be adopted. By removing the complexity of supporting different network environments out of the mobile computer and into this self-contained apparatus, the nomadic router allows the host computer to maintain a very minimal set of software protocols and functionality (e.g., the minimum functionality typically installed in network computers) to communicate across the network.

The nomadic router translation ability also enables the use of alternate communication paths (device independence) without the host computer being aware of any new communication device that utilizes an alternate communication path. The translation of the packets is done not just at the physical, link, or network layer of the protocol stack but at the transport and application layers as well. This allows the network card, protocol stack, and application running on the host computer to be independent of the network environment and configuration.

As an example of the communication device independence, the translation allows soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates. In addition, the nomadic router translation ability provides a flexible process for deploying enhanced nomadic and mobile computing software and services such as filtering of packets and determining which packets should be allowed to be transmitted between the mobile computer and the nomadic router or local area network (Internal Firewall).

The router apparatus can be: (i) carried with the mobile user (e.g., using an external box); (ii) attached to the mobile computer (e.g., PCMCIA card); (iii) installed inside the mobile computer (e.g., a chip in the laptop); (iv) or installed into the remote network infrastructure to provide network access for any mobile computer (e.g., a box which plugs into the remote or foreign local area network translating packets being sent between the host and its router, or a chip which is installed in routers on the remote network). The nomadic router can also be provided in the form of software which is loaded into and run in the mobile computer or another computer or router on a network.

These and other features and advantages of the present invention will be apparent to those skilled in the art from the following detailed description, taken together with the accompanying drawings, in which like reference numerals refer to like parts.

BRIEF DESCRIPTION OF DRAWINGS

FIG. **1** is a diagram illustrating one implementation of a nomadic router positioned between the host computing device and various communication devices using standard interfaces;

FIG. **2** is a diagram illustrating a basic nomadic router architecture, which is referred to as the hardware implementation architecture;

FIG. **3** is a flowchart illustrating a configuration overview of the basic steps performed when a host device is attached to the present nomadic router and when a network interface is attached to the router;

FIG. **4** is a flowchart illustrating automatic adaptation to the host device when the first data packet from the host is sent to a home network router or when an activation interrupt or signal is received;

FIG. **5** is a flowchart illustrating a process initializing and checking the various communication device interfaces for initialization, activation, etc.;

FIG. **6** is a diagram illustrating a basic nomadic router architecture when implemented as software in the host device;

FIGS. **7**A to **7**G are diagrams illustrating protocol stack implementations for various network devices, with the translation function performed for all layers of the protocol stack in the nomadic router;

FIG. **8** is a flowchart illustrating a proxy ARP packet interception and host reconfiguration process;

FIGS. **9**A and **9**B provide a flowchart illustrating a translation process which takes place in the host computer and nomadic router at various levels in the protocol stack;

FIG. **10** is a diagram illustrating the architecture of the nomadic router implemented as a hardware device including a microcontroller and a non-volatile memory for storing algorithms implementing the translation function;

FIG. **11** is a diagram illustrating the architecture of the nomadic router apparatus implemented as an Application Specific Integrated Circuit (ASIC) chip;

FIGS. **12**A to **12**E are diagrams illustrating host and network interface modes in which the nomadic router is able to operate;

FIG. **13** is a simplified perspective view illustrating the nomadic router as implemented in a self-contained box which connects onto a local area network via a network interface port and has multiple ports to connect to host computers;

FIG. **14** is a simplified perspective view illustrating the nomadic router apparatus as implemented on a PCMCIA Type III card where the nomadic router plugs into the host computer's type II slot and the communication card device, of Type II, plugs directly into the nomadic router so both may be powered and stored in the portable host computer; and

FIG. **15** is a simplified perspective view illustrating the nomadic router as implemented on a PCMCIA Type II cared where the nomadic router plugs into the host computer via a type II interface slot and where the communication card device, Type II, plugs into the nomadic router type II card.

BEST MODE FOR CARRYING OUT THE INVENTION

FIG. **1** illustrates a "nomadic" translator or router **10** embodying the present invention as being connected between a host device or computer **12** and a communications device **14**. Host device **12** is a laptop computer or other fixed or mobile digital data communication terminal which is sufficiently portable or mobile that it can be carried from one location to another. A laptop computer, for example, can be used in any convenient location such as an airplane, customer's office, home, etc.

Communications device **14** can be part of any type of communication system to which host computer **12** can be connected. Such communication systems include, but are not limited to, local networks, wide area networks, dial-up and direct internet communications, etc. In a typical application, the communications device will connect the host computer to a local network which itself is connected to the internet. Thus, host device **12** is able to communicate with an unlimited number of networks and nodes which are themselves interconnected with routers, switches, bridges, etc. in any known manner.

Router **10** includes a terminal interface **10***a* which normally is used to connect router **10** to host device **12**, and a system interface **10***b* which connects router **10** to communications device **14**. Router **10** generally includes a processor consisting of hardware and/or software which implements the required functionality. Router **10** is further configured to operate in an alternate mode in which host device **12** is connected directly to a network, and router **10** is also connected to a point in the network via system interface **10***b*. In this case, terminal interface **10***a* is unused.

Although device **10** is described herein as being a router, it will be understood that router **10** is not a conventional router in that it includes the capability for providing interconnectability between networks. Instead, router **10** is essentially a translator which enables host device **12** to be automatically and transparently connected to any communications device **14**, and process incoming and outgoing data for device **12**.

Host device **12** may be provided with a permanent internet address which conveniently need not be changed in accordance with the present invention. Device **12** is initially configured to communicate with a particular gateway or other home device at its base location. The gateway has a link layer address which device **12** attempts to locate when it is connected to any communication system. Without the functionality of the present nomadic router **10**, host device **12** would not be able to operate at a remote location because it would not find its gateway.

It will be understood that the term "home" does not relate to a residence, but is the network, gateway or other communication device or system to which the terminal is normally connected and which corresponds to the home internet or IP address.

FIG. **1** further illustrates a top protocol layer **16** representing host computer device **12** which generates and consumes data that is transferred through communications device **14**. Interface **16** is below the IP layer, and above the link layer in the typical OSI/ISO model. In the middle is a layer **18**, which represents router **10**, whose function is to adaptively configure and utilize the underlying communications device and provide router support. A lower layer **20** is a physical communication which carries out the communication (potentially wire-lined internet based, ad-hoc or wireless) as made available and determined for use by the nomadic router or user. Between router layer **18** and layers **16** and **20** are interfaces **22** and **24** which router **10** identifies and configures dynamically.

The present invention operates with host computers, routers, and other network devices through well-defined standard interfaces such as specified by the IETF (Internet Engineering Task Force) and IEEE standardization committees. These standards specify the packet format, content, and physical communication characteristics. As shown in FIG. **7**A, host computers have to be configured at various layers of the protocol stack depending on the communication capabilities and configurations of the current network.

Hubs, as shown in FIG. **7**B, provide a well defined interface to connect host computers and network devices by transmitting packets across multiple physical connections. Hubs do not provide any manipulation or translation of the content of the packets being transmitted.

Bridges or switches, as shown in FIG. **7**C, provide an intelligent filtering mechanism by which packets are transmitted across multiple physical connections based upon the physical connection the device is connected to, according to the link layer addressing (Media Access Control Address). Bridges and switches do not manipulate the content of the packet and do not provide any higher layer protocol functionality.

Routers, as shown in FIG. **7**D, accept packets based upon the destination address at the network layer in the packet. However, the host computer must explicitly address the packet to the router at the link layer. The router will then retransmit the packet across the correct physical connection based upon how it is configured. No modification or translation of the packet is performed at any higher layer of the protocol stack than the network layer.

Firewalls, as shown in FIG. **7**E, filter packets at the network and transport layers to allow only certain packets to

be retransmitted on the other physical connection. Firewalls do not manipulate the content of the packet, only forward it on to the next hop in the network if it passes the transport (port) or network (IP address) filter.

Proxies and gateways, as shown in FIG. **7**F, only receive packets explicitly addressed to them by host computers. They only manipulate packets at the application level. The present nomadic router **10**, as shown in FIG. **7***g*, manipulates the content of the packets at the link, network, transport, and application layers of the protocol stack to provide a translation between the host computer configuration and the configuration of the remote or foreign network to which the host computer is currently attached.

Unlike all other devices shown in FIGS. **7**A to **7**F, router **10** will automatically intercept and translate packets without the other devices being aware of router **10** or being configured to use it, i.e., without packets being addressed to router **10**. The translation algorithms in router **10** which provide this location independence are provided completely internal to router **10**. Thus, no new standards need to be developed, accepted, or implemented in host computers **12** or routers **26** to deploy new network services when using the nomadic router.

Whenever a new or different communication device (which includes the link and physical layers) is utilized in a host computer **12**, the host computer's network layer must be aware of this new communication device. Since router **10** has its own network interface to the communication device, alternate communication devices can be utilized in router **10** which the host computer **12** can utilize but does not have to be configured to use.

Today we communicate with individuals in terms of the location of their communications instruments (for instance, their computer's IP address or their fax machine's phone number). To support mobility and changing communication environments and devices, it is necessary to create an environment where people communicate with other people, and not specifically with the devices they use. To transparently support mobility and adaptivity in a wireless, potentially ad-hoc, communication internetwork, a common virtual network must be provided by an intelligent device or agent which supports the various computing hosts and communication devices.

The present nomadic router **10** provides the mapping between the location based IP address used in the internet today and the permanent user based address housed in the host CPU in the device **12**. This is illustrated in FIG. **2** as "IP Mapping." This mapping is done without support or knowledge of such mapping by the host CPU or user.

The internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU but rather are internal to the nomadic router. The host configuration information, such as IP number, is discovered or determined as illustrated in FIG. **4** and stored in nomadic router **10** as illustrated in FIG. **2** as "Host Info." This configuration process is overviewed in FIG. **3**.

As illustrated in FIG. **2**, nomadic router **10** can provide off-load communication processing for the host CPU by being physically separate from host device **12**. The adaptation, selection, and transportation of information across the network is performed by nomadic router **10**. This allows the host terminal or device **12** to utilize the network without having to directly support the network protocols. By having the nomadic router be responsible for adapting to the current network substrate, the host CPU can maintain a higher performance because the routing, adaptation, packetization, etc. algorithms, or packet processing, are performed by router **10**.

The nomadic router can also queue, transmit, and receive data independent of whether the host device **12** is available or even attached. CPU **11** built into nomadic router **10** may provide all necessary computing routines to be a fully functional network co-processor independent of the host CPU. This will allow increased battery life for the user because the nomadic router does not have numerous user I/O devices as does the host device **12**.

The instant network nomadic router provides the ability to provide ubiquitous and reliable support in a location independent fashion. This removes any burden on the user for device reconfiguration (e.g., IP address configuration, gateway or next hop router address, netmask, link level parameters, and security permissions) or data transmission.

The problem with existing protocol stacks is that communicating devices have to be reconfigured every time the communication environment changes. TCP/IP requires a new network node and gateway number. Appletalk will automatically choose an unused node number and discover the network number, but all open communications are lost and services have to be restarted to begin using the new information.

This occurs, for example, when a PowerBook is plugged into a network, put to sleep, and then powered up in a different network. All network services are restarted upon wakeup, and network applications get confused if they are not restarted. The nomadic router solves this problem by providing temporary as well as permanent network and node numbers similar to that provided by Mobile IP. However, the nomadic router will also work with other protocol stacks (e.g., AppleTalk).

Mobile IP provides location independence at the network level and not at the link level. All link level parameters, which are device specific, will be automatically configured as illustrated in FIG. **5** when a new communications (network interface) device is attached to the nomadic router. The nomadic router completely eliminates the need for manual configuration by adaptively supporting device independence.

Another innovative feature of the nomadic router is the support for simultaneous use of multiple communication substrates. This is illustrated in FIG. **2** as "Device Selection." Users should be able to utilize two or more communication substrates, either to increase throughput or to provide soft-handoff capability. This functionality is not supported in today's typical protocol stacks (e.g., TCP/IP or AppleTalk). For example, via the "network" control panel, the user can select between communications substrates such as EtherTalk, LocalTalk, Wireless, ARA, etc., but cannot remotely login across EtherTalk while trying to print via LocalTalk. Routers are typically able to bridge together various communication substrates, but merging the LocalTalk and EtherTalk networks together is often not desirable for many reasons, including performance and security.

A problem with existing routers is that they require manual configuration and exist external to the node. To overcome this, the nomadic router can support automatic configuration and full router functionality internally. This allows a mobile or nomadic node to adapt to various communication and network devices dynamically, such as when the user plugs in a PCMCIA card or attaches a communications device to the serial port.

Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use, is shown in FIG. **2** and FIG. **5** as part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface. There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Another feature of the nomadic router is the support for alternate or simultaneous use of various communication substrates. This is performed as part of step **5** in FIG. **6** when the source address is that of the communication substrate on which the nomadic router is going to send the packet. Host computers will now indirectly be able to utilize two or more communication substrates, either to increase throughput or to provide soft-handoff capability.

This functionality is not supported in typical protocol stacks (e.g. TCP/IP or AppleTalk). Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use is part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface.

The nomadic router can run completely in software without any special hardware as shown in FIG. **6**, or without a CPU separate from the main host, or packaged in the form of a hardware device as shown in FIG. **2**. The nomadic router can also be provided as a digital storage medium which stores the software program that implements the functionality of the router's translation processing. Examples of digital storage media include optical media (e.g. CD-ROM), magnetic media (e.g. floppy disks), non-volatile or read-only memories, or any combination thereof. The program is loaded into and run on mobile terminal **12**, or alternatively into any other computer or router which is connected to a network.

One potential implementation of the nomadic router device uses Embedded PC Technology. As an example, the rugged PC/104 standard modules have a form-factor of 3.550" by 3.775" and typically 0.6" per module and weigh approximately 7 oz. per module. The PC/104 module's utilization of a self-stacking bus with minimum component count and power consumption (typically 1–2 Watts per module) eliminates the need for a backplane or card cage.

The nomadic router can run on a 16 bit bus with an 80486 processor, for example. The standard network access devices can support burst rates up to 10 Mbps with typical user data throughput around 1–2 Mbps. The user bandwidth is less depending on the available wireless communication device. For example, Proxim's 2 Mbps wireless LAN typically covers 500 yards with user data throughput around 500 Kbps. As illustrated in FIG. **1**, nomadic router **10** typically includes 3 modules; a processor **10**, host device or terminal interface **10***a*, and communication device or system interface **10***b*.

Another potential hardware implementation is with the CARDIO S-MOS System technology. This CPU board is basically the same size as a PCMCIA credit card adapter. It is 3.55×3.775×0.6 inches. The power requirements are +5V DC +/−10% with an operating temperature of 0 to 70° C., a storage temperature of −40 to 85° C., and relative humidity of 10% to 85% non-condensing.

The CARDIO is the most compact PC/104 compatible system available which meets the one-stack mechanical and electrical PC/104 Rev. 2.2 specifications. Power fail indicator, battery backup, and automatic switchover are also possible.

The nomadic router can also be implemented on a small portable device such as a PCMCIA card or partially on a PCMCIA card. In the case of a full implementation on a PCMCIA card, the host CPU and power supply are used to execute the Nomadic Routing and other protocols, algorithms, operating system, and application services. A hybrid implementation with some components as part of a PCMCIA card and others as part of other hardware implementation can also be used.

By performing packet translation in a self-contained apparatus, processing done on the packets in the nomadic router does not affect the host computer. All specific translation of the packets to match the network's configuration and available services is done internally to the nomadic router. The nomadic router can queue, transmit, and receive data independent of whether the host computer is available or even attached. The algorithms and microcontroller built into the nomadic router provides all necessary computing routines to be a fully functional network co-processor independent of the host computer.

By allowing the nomadic router to process packets independently of the host computer, the host computer can be powered down or asleep while processing is taking place, providing an increase in battery life for the mobile host computer.

The nomadic router can be configured with various components in several different ways. In FIG. **10**, the nomadic router contains a processor or microcontroller **11** to translate the packets stored in packet buffers in random access memory. The translation functions are stored in non-volatile memory **13** with the Real Time Operating System (RTOS) and configuration information relative to the types of translation that need to be performed.

Upon startup (boot) of the nomadic router, the RTOS and translation algorithms are loaded from non-volatile memory into RAM where they are executed. There may be zero, one, or more host interfaces in which host computers are connected. There are one or more network interfaces. If no host interface is available, the nomadic router receives packets via the host computer from the network interface.

In FIG. **11**, nomadic router **10** is implemented as an Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA) **15**. These chips embed the algorithms for packet translation. The chip can include storage for non-volatile memory **17** which stores the configuration information such as when manually configured for the current network. The chip **15** can also include random access memory to buffer packets for translation in the nomadic router before being sent off to the host or network interface.

As described above, the nomadic router can be packaged in several different hardware configurations. The nomadic router can be embedded in the host computer, or a network device, such as a switch or router. It can also be implemented as a PCMCIA card which plugs into the host computer, or as a self-contained external box.

Each nomadic router can have from one to many interfaces. If router **10** is put into the network infrastructure, it does not have to be carried around with the mobile user. As

shown in FIG. **12***a*, nomadic router **10** is attached to a Local Area Network (LAN) of the network infrastructure (which constitutes the communications device **14**) through system interface **10***b*. LAN **14** is connected through a conventional router **26** to the internet **28**. In this case, host computer interface **10***a* of nomadic router **10** is not needed since packets from host computer **12** are received through LAN **14**.

To provide a secure interface between host computer **12** and network **14** to prevent host computers from being able to watch (sniff) packets on network **14**, nomadic router **10** can have one interface to host computer **12** (terminal interface **10***a*) and a second interface (**10***b*) to network **14** as shown in FIG. **12**B. Nomadic router **10** can provide filtering of packets received and retransmitted between the various interfaces thus providing a firewall type of security device which operates internally on the network. To support multiple host computers **12***a* . . . **12***n* with a single nomadic router **10**, nomadic router **10** may have multiple host interfaces $\mathbf{10}a_1 \ldots \mathbf{10}a_n$ as shown in FIGS. **12**C and **20** in FIG. **13**, and a network or system interface **10***b*.

If the nomadic router is carried around by the mobile user, it can take the form of a PCMCIA card. In FIG. **12**D, nomadic router **10** is implemented as a PCMCIA card. The processing and translation capability is stored inside the card and the interface to host computer **12** is through a PCMCIA BUS interface or communication card **30**. The nomadic router may also be used as an interface between a local area network **14** and a router **26** as illustrated in FIG. **12**E. Local area network **14** may be a mobile or portable network with router **26** being fixed at a particular location with a physical connection to the internet. Such an arrangement may be used for a customer demonstration or trade show, for example, where the local area network **14** is established among computers previously configured to communicate with each other but not with the foreign network having router **26**.

As shown in FIG. **14**, the PCMCIA card can fit in a type III slot where there is a connector on nomadic router **10** which accepts communication card **30** (a type II PCMCIA card). In this mode, the nomadic router does not require internal communication device specific components. Nomadic router **10** can also take the form of a type II PCMCIA card. In this form, the communication device or card **30** plugs into the opposite end of nomadic router card **10** as illustrated in FIG. **15**.

The nomadic router initialization and self configuration process provides the means by which the nomadic router is able to learn about the host computer and network so it knows what translation is necessary. Depending on the particular application, the nomadic router may have to learn the configuration of the host computer, the remote/foreign network, or both. For example, when utilized as a fixed nomadic router in a hotel or multiple dwelling unit, the nomadic router will have already learned (or been manually configured for) the remote/foreign network. The nomadic router need only determine the settings of mobile hosts which are subsequently connected to the network. Similarly, when the nomadic router is implemented as a PCMCIA card which travels with the mobile host, the nomadic router need only learn the settings of the foreign/remote network (since the host settings were previously learned or manually configured). In some applications, the nomadic router learns both the network and host configurations as previously described.

Nomadic router **10** is able to learn the host computer **12** configuration by looking at the content of the packets sent from host computer **12**. Rather than host computer **12** sending packets directly to router **26** or other network device (which is what it is initially configured to do), nomadic router **10** is able to redirect all outbound packets from the host computer **12** to itself. This redirection can be accomplished in several ways as described below.

Whenever a host computer **12** has an IP packet to send to router **26** or other network device, host computer **12** uses the Address Resolution Protocol (ARP) to obtain the link layer Media Access Control address (MAC address). As illustrated in FIG. **8**, when host computer **12** broadcasts an ARP request for the MAC address of a destination node, nomadic router **10** intercepts this ARP request broadcast and responds with its own MAC address (rather than that of the destination node).

When host computer **12** receives the ARP reply from nomadic router **10** (which contains the MAC address of nomadic router **10**), host computer **12** will cache this MAC address and send all packets destined for the configured router or network device to the MAC address of nomadic router **10**. Host computer **12** will think that the MAC address is that of its originally configured IP network device. However, nomadic router **10** is only pretending (proxying) to be the device (its home gateway) that host computer **12** expects to find. Since the MAC address is cached in host computer **12** for a short period of time, host computer **12** will not send out a new ARP request to obtain the MAC address again unless a timeout period occurs or the cache is cleared, such as when computer **12** is restarted.

When a conventional network device receives or hears a packet with a MAC address which does not match its own, it will ignore or drop the packet. Since it is possible to rapidly switch from one network environment to another using a portable computer, nomadic router **10** must be able to intercept packets even when the MAC address is not that of the nomadic router's home gateway or device. This is accomplished by placing the nomadic router's network connection is promiscuous mode. In this mode, the network connection on the nomadic router accepts all packets being transmitted on the communication link, not just ones being broadcast or addressed specifically to it.

Nomadic router **10** may also provide other network services to host computer **12**. For example, host computer **12** may be able to utilize the DHCP service to obtain configuration information rather than being manually configured. However, a host computer utilizing the DHCP service requires that a DHCP server be installed on the network segment to which it is currently attached. If the host computer **12** is configured to use this service but a DHCP server is not available on the remote/foreign network, nomadic router **10** will intercept the DHCP requests and respond with configuration information for host computer **12** to use.

The nomadic router is able to learn about the network environment it is currently attached using several different methods as described below.

When the nomadic router is connected to a different network, it will broadcast a DHCP request to obtain configuration information for that network. If no DHCP service is available on the network, the nomadic router will use another method to learn about the network configuration. For example, routers on the network will periodically broadcast router information packets which are used to build routing tables and allow routers to adapt to changes in the network. Nomadic router **10** will listen on the network for these router information packets. When a router information packet is received, the nomadic router will extract the

configuration information from each packet and store the information for use in translating packets from the mobile host.

By placing the nomadic router's network connection in promiscuous mode, the nomadic router receives all packets (not just ones addressed to the nomadic router). The nomadic router examines all packets received on the network interface to discover the network configuration. The nomadic router is also able to determine the IP addresses used on the current network and which machines are routers (by the final destination address not being the next hop address). Using this method, nomadic router **10** is passively able to learn how the network is configured and will elect to use an unused IP address. If that IP address does become used by another network device, the nomadic router will switch over to another unused IP address.

The network configuration information can also be manually configured in the nomadic router **10** as described above. This information can be set using an embedded web server, Simple Network Management Protocol (SNMP) tools, an application running on one of the computers in the network, or other suitable means. When manual configuration is used to set the network configuration, nomadic router **10** will still automatically learn the host information and provide all the translation capabilities so the host computers do not have to be aware of the correct network information of the LAN to which they are currently connected.

After learning the network and/or host computer configuration(s), the nomadic router has the necessary information to translate packets transmitted/received by the host computer. The nomadic router's packet translation function provides a mapping between location and service dependent configurations used by host computer **12** and that used by network **14** to which it is currently attached. For outbound traffic from host computer **12** to network **14**, the translation function changes the content of the packet such as the source address, checksum, and application specific parameters, causing all packets sent out to network **14** to be directed back to nomadic router **10** rather than to host computer **12**.

Inbound traffic from network **14** arriving at nomadic router **10** (which is really for host computer **12**), is passed through the translation function so host computer **12** thinks that the replies were sent directly to it. Host computer **12** will be completely unaware of all the translation being performed by nomadic router **10**.

The translation functions works as illustrated in FIGS. **9***a* and **9***b*. In these figures, the operations performed in the OSI/ISO model application, transport, network, link, and physical layers are illustrated in rows opposite the layer designations. The operations performed by host computer **12**, nomadic router **10** and network **14** are illustrated in columns below the device designations. Host computer **12** will generate network packets using the current configuration stored in host computer **12** using the standard protocol stack as shown in step **1**. This configuration information is either manually configured in host computer **12** or obtained using DHCP (from the network or the nomadic router).

As shown in step **2**, when host computer **12** attaches the link level destination address (automatically obtained using the Proxy ARP packet interception routine described earlier), host computer **12** will send the packet to the network address of its standard router or home gateway device using the link level address of the nomadic router **10**.

In step **3**, the packet is transmitted across the standard physical connection between host computer **12** and nomadic router **10**. As shown in step **4**, nomadic router **10** will receive the packet at the link level either because the Proxy ARP function reconfigured the host computer's MAC address, or because nomadic router **10** has the network link level in promiscuous mode which causes it to receive the packet even if addressed to a different MAC address.

Once the packet is passed to the network layer, shown in step **5**, the nomadic router translation function will modify the content of the packet to change the source address to match that of the nomadic router's address instead of the host computer's address. It will also translate other location dependent information such as the name of the local Domain Name Service (DNS) server. When translating the DNS packet, it will change the source address to that of the nomadic router's address and the destination address to that of a local DNS server.

Once the network layer translation is complete, the packet can be translated at the application and transport layers. The application layer is translated next, as shown in step **6**, because the transport layer requires a pseudo-network layer header which includes the source and destination addresses and the content from the application layer. At the application layer translation, any addresses which describe the source address of the host computer, such as with FTP, are translated to be that of the nomadic router's address. Any application layer destination addresses, such as a local proxy server, are translated to match that of the server running on the current network.

Once this application layer translation is complete, the transport layer, as shown in step **7**, can complete the checksum and any port number manipulation. The port number is manipulated if more than one host computer **12** is attached to nomadic router **10**. Each request sent by any one of the host computers **12** include a specific port that is translated to match an available inbound port on the nomadic router **10**.

The port number assigned for use with each host computer **12** is stored in a table in nomadic router **10** and is utilized with the reply packet to route the reply to the corresponding host computer as describer later. Finally, the outgoing packet is transmitted over network **14** in step **8**.

When a reply packet is transmitted over network **14**, as shown in step **9**, nomadic router **10** will receive the packet. In step **10**, nomadic router **10** will perform the reverse network layer translation to set the destination address to that of host computer **12** rather than the nomadic router's address, and any source address to the source address replaced by nomadic router **10** in step **5**.

Once network translation is complete, the packet is translated at the application layer, as shown in step **11**, to change the destination address to that of host computer **12** and the source address to the original destination address stored from step **6**. In step **12**, any port manipulation performed in step **7** is changed to the original setting and a new checksum is computed. Finally, as shown in step **13**, the packet is sent to host computer **12** which then processes the packet normally.

There are numerous options and applications of the nomadic router. These applications include, but are not limited to, Nomadic E-mail, Remote Network File Synchronization, Nomadic Database Synchronization, Instant Network Nomadic Routing, Nomadic Intranets, and Trade Show Data Exchange. Each of these are described in more detail below.

The Nomadic E-mail application provides a synchronized yet distributed means for updates, reconciliation, and replicas to propagate through the internet. Nomadic routers are

located on various networks of the internet and are equipped with nomadic E-mail support to provide synchronization, etc. Each nomadic router enabled for nomadic E-mail can utilize protocols such as IMAP to provide support for mobile users without the host device having to support it (similar to the POP3 protocol standard in internet E-mail clients).

The Remote Network File Synchronization option of the nomadic router provides copies of user files that are stored/cached at various locations (e.g., hotel, office, home) on other nomadic routers equipped for remote network file synchronization. Copies of updated files are automatically synchronized and distributed among all peer locations. Local updates can be made while the host is disconnected from the nomadic router and from the network.

The Nomadic Database Synchronizer houses the user's (synchronized) master databases (e.g., contacts, addresses, phone numbers). The nomadic router of the database synchronizer does not need to be used on the network because it will interface directly with various host devices such as laptops, desktops, personal digital assistants, handheld personal computers, pagers, etc. via various standard porets.

The objective of the Instant Network nomadic router is to enable rapid deployment of a communication network in any environment with little or no fixed infrastructure. The host and communication devices do not have to directly support the rapid deployment functionality.

The instant network nomadic router distributedly and intelligently establishes a wireless (or wired) communication link between the host device and the desired communication system while performing configuration, security, multihop routing, and network level data transmission over various communication devices. The nomadic router performs all the necessary network creation and processing automatically to remove configuration and system support from the host system or user. The instant network nomadic router utilizes proprietary and existing/emerging wireless communication systems, and multihop routing protocols.

Many communication infrastructures are varied and fragmented, which is likely to be exacerbated as more technologies are introduced. For example, high performance LANs, wireless services, cellular telephony, satellite, and ubiquitous paging networks, all provide varying degrees of coverage, cost, and bandwidth/delay characteristics.

Conditions may range from no connectivity at all because of lack of service, to partial and/or intermittent connectivity as devices are plugged and unplugged from a system. Likewise, damage communication infrastructures (deliberately or by accident), lossy communication as a system moves through various service areas or difficult domains, and times when multiple network devices (communication substrates) can be used at the same time complicate connectivity. The instant network nomadic router will dynamically adapt the communication internetwork (dynamically creating one if necessary) to provide survivable communication in a mobile chaotic environment without the need for centralized control or fixed infrastructures.

The rapidly deployable nomadic router is a device associated with each user host device (e.g., PDA or laptop computer). It transparently provides the following capabilities for host computer systems using various wireless communication devices for physical and link layer access: dynamic wireless network creation; initialization into existing wireless networks; automatic configuration; network and subnetwork level data transmission; and multihop routing functionality.

The nomadic router can detect another device by polling the interface, providing an interrupt signal, or through specialized signaling. This in turn activates the nomadic router to provide translation for the device (if necessary) and establish a communication link to an appropriate corresponding interface and wireless subnetwork. The nomadic router operates at a level between the host device generating data and the physical communication transmission device as illustrated in FIG. **1**.

The Nomadic Intranet application provides all network and server type services for users to dynamically create an adhoc network. This is similar to the instant network nomadic router except the nomadic intranet is a single device with multiple ports into which laptop/devices can be plugged. The instant network nomadic router is distributed to each host device. The nomadic intranet not only provides adhoc networking but can also provide services such as temporary file storage, protocol conversion, act as a print server, and provide other services described as part of the Basic nomadic router.

The Trade Show nomadic router applications not only provide the basic nomadic router functionality for an exhibitor's computer that is brought to the show, but also provides lead capture and/or information distribution. Lead capture can be provided by interfacing with a badge reader to read attendees' information. This information is then captured by the nomadic router and made available in the exhibitor's lead database.

The Nomadic Intranet application provides all network and server type services for users to dynamically create an adhoc network. This is similar to the instant network nomadic router except the nomadic intranet is a single device with multiple ports into which laptop/devices can be plugged. The instant network nomadic router is distributed to each host device. The nomadic intranet not only provides adhoc networking but can also provide services such as temporary file storage, protocol conversion, act as a print server, and provide other services described as part of the Basic nomadic router.

As briefly described above, the fixed nomadic router applications provide the same basic functionality and architecture as the portable nomadic router with the nomadic router stored in one location. The fixed nomadic router acts as a surrogate or "Home Agent" for the user when he/she is away on travel. When the user wishes to register or utilize their host device elsewhere in the network, the portable nomadic router will register with the fixed nomadic router where it is temporarily attached to the network so information can be forwarded to the user's new location. The fixed nomadic router can also be used to house the master copy of the user's E-mail for the nomadic E-mail service, or files for the nomadic file synchronizer.

The nomadic router provides the mapping between the location-based IP address used in the internet today and the permanent user-based address housed in the host CPU. This mapping is done without support or knowledge of such mapping by the host CPU or user. The Internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU, but rather are internal to the nomadic router.

By implementing this protocol as part of the translation function in the nomadic router, the nomadic router can encapsulate packets from the host computer and transmit them back to the fixed nomadic router which are sent out

(un-encapsulated) on the native (home) network. Replies from the home network are received by the fixed nomadic router and are encapsulated and sent back to the nomadic router. When packets are transmitted between the nomadic router and fixed nomadic router, the packets are encrypted and sent using the Internet Tunneling Protocol.

Since the (mobile) nomadic router provides location independence and the fixed nomadic router forwards all packets from a corresponding host to the host computer via the nomadic router, any changes in the location, failure of a network link, or attachment point of the mobile host computer does not cause any open session to be lost. This session loss prevention is possible since the fixed nomadic router pretends to be the mobile host computer, and the nomadic router pretends to be the home network. The fixed nomadic router and nomadic router translation functions hide the link and network loss from the transport and application session.

While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention.

What is claimed is:

1. A method for providing connectivity between a foreign device on a second local area network and a user device configured for a first local area network, the user device having a permanent address, the method comprising:

intercepting packets transmitted by the user device intended for the foreign device on the second local area network to automatically determine network settings of the user device, the packets transmitted by the user device having the permanent address of the user device as a source address;

modifying packets transmitted by the user device to make these packets compatible with the second local area network based on the network settings of the user device and on network settings of the second local area network such that the second local area network appears as the first local area network to the user device;

wherein modifying packets transmitted by the user device includes substituting the permanent address of these packets with a router address as the source address, wherein the router address is an address recognized by the foreign device;

intercepting packets transmitted by the foreign device intended for the user device, the packets transmitted by the foreign device having the router address as a destination address;

modifying packets transmitted by the foreign device to make these packets compatible with the first local area network based on the network settings of the user device and on the network settings of the second local area network such that the first local area network appears as the second local area network to the foreign device;

wherein modifying packets transmitted by the foreign device includes substituting the router address of these packets with the permanent address as the destination address.

2. The method of claim **1** wherein the step of intercepting packets transmitted by the user device comprises receiving and processing packets transmitted by the user device which would otherwise be dropped by devices on the second local area network due to incompatible network settings.

3. The method of claim **1** further comprising:

automatically determining the network settings of the second local area network based on packets transmitted over the second local area network.

4. The method of claim **1** further comprising:

automatically determining the network settings of the second local area network by transmitting a Dynamic Host Control Protocol (DHCP) packet over the second local area network.

5. The method of claim **1** wherein the step of intercepting packets transmitted by the user device comprises:

intercepting an Address Resolution Protocol (ARP) message transmitted by the user device having a network address of a device on the first local area network; and

replying to the ARP message with a Media Access Control (MAC) address of a device on the second local area network.

6. The method of claim **1** wherein the step of intercepting packets transmitted by the user device comprises operating in a promiscuous mode to receive and process all packets transmitted by the user device.

7. The method of claim **1** wherein the router address is automatically determined based on the network settings of the second local area network.

8. The method of claim **7** wherein the step of substituting the permanent address of a packet transmitted by the user device comprises replacing a source address within a packet header.

9. The method of claim **7** wherein the step of substituting the permanent address of a packet transmitted by the user device comprises replacing a source address within contents of the packet.

10. The method of claim **1** wherein the step of intercepting packets transmitted by the user device comprises:

intercepting a Dynamic Host Control Protocol (DHCP) packet transmitted by the user device;

determining whether a DHCP server is available on the second local area network; and

replying to the DHCP packet to provide configuration settings based on network settings of the second local area network.

11. A method for providing access to a network utilizing private IP addresses for a user device having an incompatible private IP address, the method comprising:

intercepting data transmitted by the user device containing the incompatible private IP address;

modifying the data using a private IP address compatible with the network private IP addresses; and

transmitting the modified data on the network.

12. The method of claim **11** further comprising connecting a translator to the network to perform the steps of intercepting the data transmitted by the user device, modifying the data, and transmitting the data.

13. The method of claim **12** wherein the step of connecting comprises connecting the translator between the user device and the network.

14. The method of claim **12** wherein the user device and translator are directly connected to the network.

15. The method of claim **11** wherein the step of intercepting packets comprises receiving and processing packets which would otherwise be dropped by devices on the second local area network due to incompatible network settings.

16. The method of claim **11** wherein the step of intercepting packets comprises operating in a promiscuous mode to receive and process all packets transmitted by the user device.

17. The method of claim 11 wherein the step of intercepting packets comprises:

intercepting an Address Resolution Protocol (ARP) message transmitted by the user device; and

replying to the ARP message with a hardware address of a device on the network so future messages transmitted by the user device are directed to the device on the network.

18. A method for providing access to a network utilizing DHCP for a user device configured with a static IP address, the method comprising:

intercepting packets transmitted by the user device to determine the static IP address;

transmitting a DHCP request on the network to determine at least one available network IP address;

modifying the packets transmitted by the user device based on an available IP address; and

transmitting the modified packets on the network to provide network access to the user device.

19. A method for providing connectivity to a first network for a user device, the user device having a permanent address, the method comprising:

automatically determining network settings of the first network based on addresses contained in messages transmitted over the first network;

intercepting user device messages transmitted over the first network without regard to message destination addresses, the user device messages having the permanent address of the user device as a source address; and

modifying incorrectly configured messages transmitted by the user device based on the network settings of the foreign network, wherein modifying incorrectly configured messages transmitted by the user device includes substituting the permanent address of these messages with a router address as the source address, wherein the router address is an address recognized by the foreign network.

20. The method of claim 19 wherein the user device is configured to communicate over a home network having network settings incompatible with the foreign network, the method further comprising:

automatically determining network settings of the user device by intercepting an Address Resolution Protocol (ARP) message transmitted by the user device having a destination address of a device on the home network and replying to the ARP message by associating a Media Access Control (MAC) address of a device on the first network with the destination address of the device on the home network.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,088,727 B1
APPLICATION NO. : 09/684937
DATED : August 8, 2006
INVENTOR(S) : Joel E. Short et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 20, Line 7, Claim 19:
Delete "foreign" and insert therefor -- first --.

Column 20, Line 12, Claim 19:
Delete "foreign" and insert therefor -- first --.

Column 20, Line 15, Claim 20:
Delete "foreign" and insert therefor -- first --.

Signed and Sealed this

Twelfth Day of December, 2006

JON W. DUDAS
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,088,727 B1
APPLICATION NO. : 09/684937
DATED : August 8, 2006
INVENTOR(S) : Joel E. Short et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page:

Item (63) Delete "continuation" and insert therefor --continuation-in-part--.

Column 1, Line 8:
Delete "continuation" and insert therefor--continuation-in-part--.

Signed and Sealed this

Twenty-second Day of May, 2007

JON W. DUDAS
Director of the United States Patent and Trademark Office

US007554995B2

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 7,554,995 B2**
(45) **Date of Patent: Jun. 30, 2009**

(54) **SYSTEM AND METHOD FOR ESTABLISHING NETWORK CONNECTION WITH UNKNOWN NETWORK AND/OR USER DEVICE**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Leonard Kleinrock**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Newbury Park, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 631 days.

(21) Appl. No.: **11/097,925**

(22) Filed: **Apr. 1, 2005**

(65) **Prior Publication Data**

US 2005/0188092 A1 Aug. 25, 2005

Related U.S. Application Data

(63) Continuation of application No. 09/684,937, filed on Oct. 6, 2000, now Pat. No. 7,088,727, which is a continuation-in-part of application No. 09/041,534, filed on Mar. 12, 1998, now Pat. No. 6,130,892, which is a continuation-in-part of application No. 08/816,174, filed on Mar. 12, 1997, now abandoned.

(51) **Int. Cl.**
H04L 12/28 (2006.01)
H04L 12/56 (2006.01)

(52) **U.S. Cl.** **370/401**; 370/338

(58) **Field of Classification Search** 370/338, 370/401, 465, 466, 467, 389, 392
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592 A 10/1992 Perkins
5,166,931 A 11/1992 Riddle

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 986 230 A2 3/2000

(Continued)

OTHER PUBLICATIONS

Nomadix, Inc. V. Second Rule LLC—CV 07 1946 First Amended Answer, Affirmative Defenses and Counterclaims of Second Rule LLC, Jul. 16, 2007.

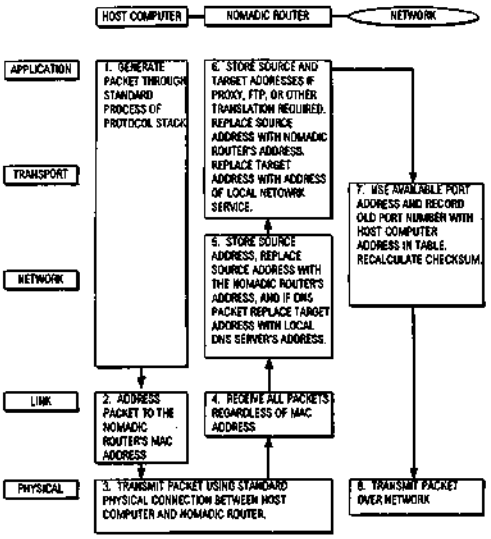
(Continued)

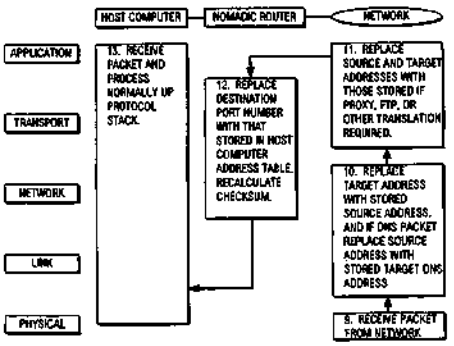
Primary Examiner—Ajit G Patel
(74) *Attorney, Agent, or Firm*—Brooks Kushman P.C.

(57) **ABSTRACT**

A system and method for connecting a user device to a network where the user device settings, the network settings, or both are unknown include intercepting packets transmitted by the user device and modifying the packets to be compatible with the network. The system and method are particularly suited for use by mobile computers, such as laptop computers, which are connected to various foreign networks. Depending upon the particular application, a device may be carried with the mobile computer, or attached as a node on the network. The device automatically determines the network settings of the user device and/or the network and modifies packets appropriately so that the user device can communicate over the network without having to reconfigure the user device with appropriate settings for each network it may encounter. Communication settings such as network address, gateway, proxy address, etc. are automatically determined using various techniques.

55 Claims, 10 Drawing Sheets





U.S. PATENT DOCUMENTS

5,251,207	A	10/1993	Abensour et al.	
5,309,437	A	5/1994	Perlman	
5,325,362	A	6/1994	Aziz	
5,371,852	A	12/1994	Attanasio et al.	
5,410,543	A	4/1995	Seitz et al.	
5,412,654	A	5/1995	Perkins	
5,425,029	A	6/1995	Hluchyj et al.	
5,442,633	A	8/1995	Perkins et al.	
5,490,139	A	2/1996	Baker et al.	
5,517,618	A	5/1996	Wada et al.	
5,539,736	A	7/1996	Johnson	
5,557,748	A	9/1996	Norris	
5,572,528	A	11/1996	Shuen	
5,586,269	A	12/1996	Kubo	
5,608,786	A	3/1997	Gordon	
5,623,600	A	4/1997	Ji et al.	
5,633,868	A	5/1997	Baldwin et al.	
5,636,216	A	6/1997	Fox et al.	
5,651,002	A	7/1997	Van Seters et al.	
5,708,655	A	1/1998	Toth et al.	
5,708,780	A	1/1998	Levergood et al.	
5,751,971	A	5/1998	Dobbins et al.	
5,757,924	A	5/1998	Friedman et al.	
5,761,683	A	6/1998	Logan et al.	
5,781,550	A	7/1998	Templin et al.	
5,781,552	A	7/1998	Hashimoto	
5,790,541	A	8/1998	Patrick et al.	
5,793,763	A	8/1998	Mayes	
5,798,706	A	8/1998	Kraemer et al.	
5,802,320	A	9/1998	Baehr et al.	
5,812,531	A	9/1998	Cheung et al.	
5,812,776	A	9/1998	Gifford	
5,822,526	A	10/1998	Waskiewicz	
5,841,769	A	11/1998	Okanoue et al.	
5,854,901	A	12/1998	Cole et al.	
5,862,345	A	1/1999	Okanoue et al.	
5,893,077	A	4/1999	Griffin	
5,909,549	A	6/1999	Compliment	
5,910,954	A	6/1999	Bronstein et al.	
5,915,119	A	6/1999	Cone	
5,918,016	A	6/1999	Brewer et al.	
5,920,699	A	7/1999	Bare	
5,960,409	A	9/1999	Wexler	
5,963,915	A	10/1999	Kirsch	
5,987,430	A	11/1999	Van Horne et al.	
5,987,498	A	11/1999	Athing et al.	
5,991,292	A	11/1999	Focsaneanu et al.	
5,991,828	A	11/1999	Horie et al.	
6,006,272	A	12/1999	Aravamudan et al.	
6,012,088	A	1/2000	Li	
6,014,698	A	1/2000	Griffiths	
6,055,243	A	4/2000	Vincent et al.	
6,061,356	A	5/2000	Terry	
6,061,668	A	5/2000	Sharrow	
6,088,725	A	7/2000	Kondo et al.	
6,098,172	A	8/2000	Coss et al.	
6,119,162	A	9/2000	Li et al.	
6,128,601	A	10/2000	Van Horne et al.	
6,128,739	A	10/2000	Fleming, III	
6,130,892	A	10/2000	Short et al.	
6,134,680	A	10/2000	Yeomans	
6,141,690	A	10/2000	Weiman	
6,226,677	B1	5/2001	Slemmer	
6,233,604	B1	5/2001	Van Horne et al.	
6,243,379	B1	6/2001	Veerina et al.	
6,249,527	B1	6/2001	Verthein et al.	
6,286,039	B1	9/2001	Van Horne et al.	
6,317,790	B1	11/2001	Bowker et al.	
6,377,990	B1	4/2002	Slemmer et al.	
6,385,653	B1	5/2002	Sitaraman et al.	
6,393,468	B1	5/2002	McGee	
6,412,073	B1	6/2002	Rangan	
6,427,170	B1	7/2002	Sitaraman et al.	
6,434,627	B1	8/2002	Millet et al.	
6,460,084	B1	10/2002	Van Horne et al.	
6,463,051	B1	10/2002	Ford	
6,466,986	B1	10/2002	Sawyer et al.	
6,496,850	B1	12/2002	Bowman-Amuah	
6,535,493	B1	3/2003	Lee et al.	
6,546,425	B1	4/2003	Hanson et al.	
6,591,306	B1	7/2003	Redlich	
6,636,894	B1	10/2003	Short et al.	
6,640,251	B1	10/2003	Wiget et al.	
6,671,379	B2	12/2003	Nemirovski	
6,671,739	B1	12/2003	Reed	
6,675,208	B1	1/2004	Rai et al.	
6,822,954	B2	11/2004	McConnell et al.	
6,857,009	B1	2/2005	Ferreria et al.	
6,868,399	B1	3/2005	Short et al.	
7,051,087	B1	5/2006	Bahl et al.	
7,088,727	B1	8/2006	Short et al.	
7,151,758	B2 *	12/2006	Kumaki et al.	370/331
7,159,035	B2 *	1/2007	Garcia-Luna-Aceves et al.	709/241
7,313,631	B1	12/2007	Sesmun et al.	
2002/0021689	A1 *	2/2002	Robbins	370/352
2002/0097674	A1	7/2002	Balabhadrapatruni	
2007/0266125	A1 *	11/2007	Lu et al.	709/222

FOREIGN PATENT DOCUMENTS

JP	5-344122	12/1993
JP	5344122 A2	12/1993
JP	7066809	3/1995
JP	8065306 A2	3/1996
JP	8-242231	9/1996
WO	WO 95/27942	10/1995
WO	WO 97/11429	3/1997
WO	WO 1999/039481	8/1999
WO	WO 99/57866	11/1999

OTHER PUBLICATIONS

Nomadix, Inc. V. Second Rule LLC—CV 07 1946 Plaintiff's Reply to Defendant's First Amended Answer and Counterclaims and Demand for Jury Trial, Jul. 31, 2007.

ATCOM/INFO and Microsoft Plan Large-Scale Deployment of IPORT for Mid-1998, ATCOM-IPORT Press Release Mar. 4, 1998.

Hotel Online Special Report, Internet Access for the Road Warrior Easier Than Ever, IPORT™ Version 2.0 Released, ATCOM-IPORT Press Release Jul. 20, 1998.

Internet Access: ATCOM/INFO Releases IPORT Central Office Solution. IPORT-CO Makes Plug & Play High-Speed Internet Access Possible too Multiple Properties from a Single Server-Product Announcement, ATCOM-IPORT Press Release Oct. 26, 1998.

Yutaka Sato, "Details of Functions of Multi-purpose Proxy Server DeleGate-Access/Route Control and Protocol Conversion", Interface vol. 21, No. 9, p. 130-146, Sep. 1995.

Yutaka Sato, "Details of Functions of Multi-purposeProxy Server DeleGate-Access/Route Control and Protocol Conversion", Interface vol. 21, No. 9, p.130-146.

Office Action mailed Oct. 5, 2005, for U.S. Appl. No. 09/684,937.

Official Communication mailed Nov. 22, 2005 for EP Patent Application No. EP 98 909 121.0.

Request for Reexamination filed Feb. 15, 2005 for U.S. Patent No. 6,130,892.

Patent application for U.S. Appl. No. 08/816,174, filed Mar. 12, 1997.

Google Groups: View Thread, Aug. 2, 2004, IP3 002505-06; Newsgroups: microsoft,public.win95.networking.

Google Groups: View Thread, Aug 2, 2004, IP3 002507-10; Newsgroups: comp.os.os2.networking.tcp-ip.

Google Groups: network settings DHCP mobile, Aug. 3, 2004 IP3 002511-15; Newsgroups: comp.sys.mac.comm.

Google Groups: netswitcher; Aug. 2, 2004; IP3 002516; Newsgroups: comp.os.ms-windows.networking.win95.

Product Information—Netswitcher, the ultimate windows network setup utility; Aug. 2, 2004; IP 3 002517; Netswitcher™ Developed and Marketed by: J.W. Hance, 1950-18 E. Greyhound Pass, Suite 305, Carmel, Indiana 46033 USA.

Google Groups: network laptop settings, Jul. 30, 2004; IP3 002767-68; Laptop on Dual Networks; Newsgroups: comp.os.ms-windows.nt.admin.networking.

Google Groups: network configuration laptop packets; Aug. 2, 2004 IP3 002765-66; Newsgroups: comp.protocols.tcp-ip.

Google Groups: "home network" laptop; Aug. 3, 2004; IP3 002769-70; Newsgroups: comp.sys.sun.admin. Newsgroups: comp.sys.sun.admin.

Google Groups: redirect "login page" Jul. 28, 2004; IP 3 002873-74; Newsgroups: microsoft.public.inetserver.iis.activeserverpages.

Perkins C.E. et al.: "DHCP for mobile networking with TCP/IP" Proceedings IEEE International Symposium on Computers and Communications, Jun. 27, 1995, pp. 255-261, XP002132695.

Perkins C.E. ED—Institute of Electical and Electronics Engineers: "Mobile-AP, AD-HOC Networking, and Nomadicity" Proceedings of the 20th . Annual International Computer Software and Applications Conference (COMPSAC). Seoul, Aug. 21-23, 1996, Proceedings of the Annual International Computer Software and Applications Conference (COMPSAC) Los Alamitos, IEEE Comp, vol. CONF. 20, Aug. 21, 1996 , pp. 472-476, XP 000684381, ISBN 0-8186-7579-9.

Network Working Group Request for Comments: 826—Ethernet Address Resolution Protocol (Nov. 1982).

Network Working Group Request for Comments: 894—Standards For Transmission of IP Datagrams Over Ethernet Networks (Apr. 1984).

Network Working Group Request for Comments: 925—Multi-LAN Address Resolution (Oct. 1984).

Network Working Group Request for Comments: 1009—Requirment For Internet Gateways (Jun. 1987).

Network Working Group Request for Comments: 1027—Using ARP to Implement Transparent Subnet Gateways (Oct. 1987).

Network Working Group Request for Comments: 1034—Domain Names—Concepts and Facilities (Nov. 1987).

Network Working Group Request for Comments: 1531—Dynamic Host Confirmation Protocol (Oct. 1993).

Network Working Group Request for Comments: 1919—Classical Versus Transparent IP Proxies (Mar. 1996).

Network Working Group Request for Comments: 1945—Hypertext Transfer Protocol—HTTP/1.0 (May. 1996).

L. Kleinrock, "Nomadic Computing" (Keynote address) *Int'l Conf. on Mobile Computing and Networking*,1995, Berkeley, California, ACM.

M. Baker et al., Supporting Mobility in MosquitoNet, Proceedings of the 1996 USENIX Technical Conference, San Diego, CA, Jan. 1996.

Comer, "Internetworking With TCP/IP vol. 1, Chapter 10, Principles, Protocols and Architecture", 3rd ed., Prentice Hall 1995.

Joel E. Short: "Auto-Porting and Rapid Prototyping with Application to Wireless and Nomadic Network Algorithms, A dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Computer Science", University of California, Los Angeles; Published Oct. 26, 1996; pp. xv, 118-124, Copyright Jan. 16, 1997.

Case No. 04CV1485 BTM (POR): *IP3 Networks, Inc. v Nomadix, Inc.* —Jul. 23, 2004 Complaint for: (1) Declaratory Judgment of Patent Non-Infringement and Invalidity of U.S. Patent No. 6,636,894; (2) Declaratory Judgment of Patent Non-Infringement of U.S. Patent No. 6,130,893; (3) Trade Libel; (4) Libel Under Cal. Civ. Code§ 45; (5) Unfair Competition Under Cal. Bus.&Prof. Code§ 17200, Et Seq.; and (6) Intentional Interference with Prospective Economic Advantage.

Case No. 04CV1485 BTM (POR): *IP3 Networks, Inc.* —Sep. 20, 2004 Amended Complaint for: (1) Declaratory Judgment of Patent Non-Infringement and Invalidity of U.S. Patent No. 6,636,894; (2) Declaratory Judgment of Patent Non-Infringement of U.S. Patent No. 6,130,893; (3) Trade Libel; (4) Libel Under Cal. Civ. Code § 45; (5) Unfair Competition Under Cal. Bus.&Prof. Code § Et Seq.; and (6) Intentional Interference with Prospective Economic Advantage—Demand for Jury Trial.

Case No. 04CV1485 BTM (POR):*IP3 Networks, Inc. v Nomadixm Inc.*—Oct. 21, 2004 Answer and Counterclaims of Nomadix, Inc. to the Amended Complaint.

Egevang, The IP Network Address Translator, Network Working Group RFC, 1631, pp. 1-10, May 1994.

Internet Protocol, Darpa Internet Program, Protocol Specification, Sep. 1981, prepared for Defense Advanced Research Projects Agency, IP3 002945-002990.

Networking Working Group, Radius Accounting, Request for Comments: 21 39, Obsoletes: 2059; Category: Informational, C. Rigney, Livingston, Apr. 1997; IP 3 002991-003013.

Review of Roaming Implementations, Aboba, B., Published as a RFC by ISOC, Sep. 1, 1997 UTC IP.com Document ID: IPCOM000002752D.

Network Layer Mobility: an architecture and survey Bhagwat, P. Perkins, C. Tripathi, S., Personal Communications, IEEE, Publication Date: Jun. 1996, vol. 3, Issue 3.

Classical versus Transparent IP Proxies (RFC1919), published as an RFC by ISOC on Mar. 1, 1996, M. Chatel.

Mobile IP-based multicast as a service for mobile hosts, Chikarmane, V., Dept. of Comput. Sci., Saskatchewan Univ., Saskatoon, Sask.; Publication Date: Jun. 5-6, 1995.

Defendant's Initial Disclosure of Prior Art dated Jan. 18, 2008, Civil Action No. 07-1946 GPS(VBK), *Nomadix, Inc.* v. *Second Rule LLC*.

Defendant's Response to Plaintiff's Claim Chart, *Nomadix, Inc.* v. *Second Rule LLC*, Civil Action No. 07-1946 GPS (VBK) dated Feb. 19, 2008.

A Virtual Home Agent Based Route Optimization for Mobile IP, Qiang Gao, Wireless Communications and Networking Conferences, 2000. WCNC. 2000 IEEE, Publication Date: Sep. 23-28, 2000, vol. 2.

Requirements for Policy-Based Management of Nomadic Computing Infrastructures, S. Heilbronner. Requirements for Policy-Based Management of Nomadic Computing Infrastructures. Proc. of the Sixth Workshop of the HP Openview University Association (HPOVUA '99), Bologna, Italy, Jun. 1999.

Automatically Configure a System to Route Internet Traffic to a Proxy, D. Liu, Originally disclosed by IBM on Apr. 1, 1999 UTC, RD v42 n420 04-99 article 42099.

Interactive Billing for Broadband and Multimedia Services Loed, S., Community Networking, 1995. Publication Date: Jun. 20-22, 1995, Princeton, NJ.

AAA Protocols; Authentication, Authorization, and Accounting for the Internet, Metz, C. Internet Computing, IEEE, vol. 3, No. 6, pp. 75-79, Nov./Dec. 1999.

A Survey of Active Network Research, Tennenhouse, D.L. Smith, J.M. Sincoskie, W.D. Wetherall, D.J. Minden, G.J. Communications Magazine, IEEE, Publication Date: Jan. 1997, vol. 35, Issue: 1.

An Efficient Multicast Delivery Scheme to Support Mobile IP, Chu-Sing Yang, Database and Expert Systems Applications, 1999. Publication Date: Sep. 1-3, 1999.

A Mobile Networking System Based on Internet Protocol, Perkins, C.E., Bhagwat, P., Personal Communications, IEEE, Publication Date: 1st Qtr 1994, vol. 1, Issue: 1.

IP3 Networks, Inc. V. *Nomadix, Inc.*-Plaintiff/Counter- Defendant IP3 Networks Inc.'s Reply to Defendant Nomadix, Inc.'s Counterclaim, Case No. 04 CV 1485 DMA (POR); dated Nov. 15, 2004.

Nomadix, Inc. v. *Second Rule LLC*, Complaint for Patent Infringement of U.S. Patent No. 6,130,892, 7,088,727, 6,636,894, 6,857,009, and 6,868,399 dated Mar. 23, 2007.

The Patent Office of the People's Republic of China, Notification of First Office Action (PCT Application) and its English translation for Chinese Patent Application No. 98805023.4 dated Jan. 12, 2005.

Single-User Network Access Security TACAS+ http.www.cisco.com/warp/public/614.7.html IP3 002876-002884; dated: Aug. 10, 2005.

Building Internet Firewalls, D. Brent Chapman and Elizabeth D. Zwicky, O'Reily & Associates, Inc. 103 Morris Street, Suite A, Sebastophol, CA 95472, IP3 002885-002944; dated: Sep. 1995.

Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946GPS (VBK), Defendant's First Supplemental Response to Plaintiff's Claim Chart dated Apr. 18, 2008.

Nomadic Computing - An Opportunity, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: ACM SIGCOMM, Computer Communications Review, Publication Date: Jan. 1995, vol. 25, Issue: 1.
Nomadicity in the NII, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: Cross-Industry Working Team Papers & Reports, Publication Date: Jun. 1995.
Nomadic Computing, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: Information Network and Data Communication' IFIP/ICCC International Conference on Information Network and Data Communication Publication Date: Jun. 1996, Location Trondheim, Norway.
Nomadicity: Anytime, Anywhere in a Diconnected World, Kleinrock, Leonard, Computer Science Department, UCLA, Los Angeles, CA; This paper appears in: Mobile Network and Applications, Special Issue on Mobile Computing and System Services Publication Date: Dec. 1996, vol. 1, Issue: 4.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Plaintiff Nomadix Inc.'s Proposed Claim Construction Statement dated May 23, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 GPS (VBK), Second Rule LLC's Response to Nomadix, Inc. 's Proposed Claim Construction Statement dated Jun. 6, 2008.
"Internetworking with TCP/IP" (Comer, "Internetworking with TCP/IP" vol. 1, Chapter 10, Principles, Protocols, and Architecture, 3rd Ed., Prentice Hall 1995).
"Nomadic Computing" (Kleinrock, "Nomadic Computing" (Keynote address) *Intl Conf. on Mobile Computing and Networking*, 1995, Berkley, California, ACM).
"Supporting Mobility in MosquitoNet" (Baker et al., Supporting Mobility in MosquitoNet, Proceedings of the 1996 USENIX Technical Conference, San Diego, CA, Jan. 1996).
RFC 1631 (Egevang, IP Network Address Translator, Network Working Group, May 1994).
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Proposed Joint Claim Construction Statement dated Jul. 2, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Plaintiff's Opening Claim Construction Brief, Redacted Public Version, dated Aug. 4, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Declaration of Mark Lezama in Support of Nomadix, Inc. s Opening Claim Construction Brief, dated Aug. 4, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Defendant's Opening Claim Construction Brief, dated Aug. 4, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Declaration of Don P. Foster Re: Second Rule LLC's Opening Claim Construction Brief, dated Aug. 4, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Plaintiff Nomadix Inc. 's Reply Claim Construction Brief, dated Aug. 22, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Supplemental Declaration of Mark Lezama in Support of Nomadix, Inc. 's Reply Claim Construction Brief, dated Aug. 22, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Declaration of Douglas G. Muehlhauser in Support of Nomadix Inc.'s Claim Construction Briefs, dated Aug. 22, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Defendant's Reply to Plaintiff's Opening Claim Construction Brief, dated Aug. 22, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Declaration of Don P. Foster Re: Second Rule LLC's Reply to Plaintiff's Opening Claim Construction Brief, dated Aug. 22, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Memorandum of Law in Support of Motion of Second Rule, LLC for Partial Summary Judgement dated Sep. 5, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Defendant's Statement of Uncontroverted Facts and Conclusions of Law in Support of Defendant's Motion for Partial Summary Judgment, dated Sep. 5, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Declaration of Don P. Foster Re: Motion of Second Rule LLC for Partial Summary Judgment, dated Sep. 5, 2008.
Nomadix, Inc. v. *Second Rule LLC*, Civil Action No. 07-1946 DDP (VBKx), Declaration of Peter Alexander, Ph. D. in Support of Second Rule's Motion for Partial Summary Judgment, dated Sep. 4, 2008.

* cited by examiner

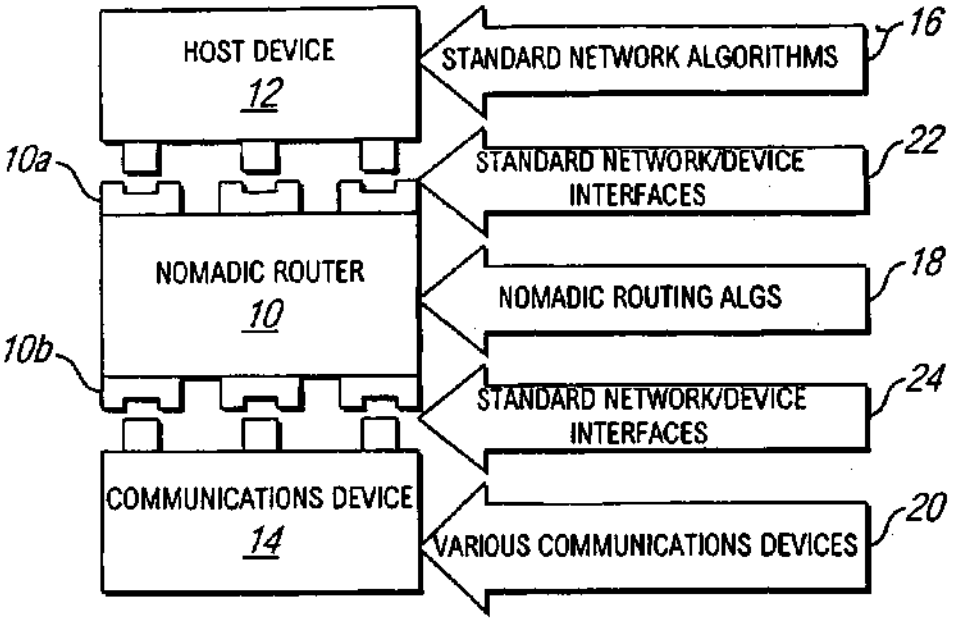

HOST DEVICE
12
10a
NOMADIC ROUTER
10
10b
COMMUNICATIONS DEVICE
14
STANDARD NETWORK ALGORITHMS
16
STANDARD NETWORK/DEVICE INTERFACES
22
NOMADIC ROUTING ALGS
18
STANDARD NETWORK/DEVICE INTERFACES
24
VARIOUS COMMUNICATIONS DEVICES
20

FIG. 1

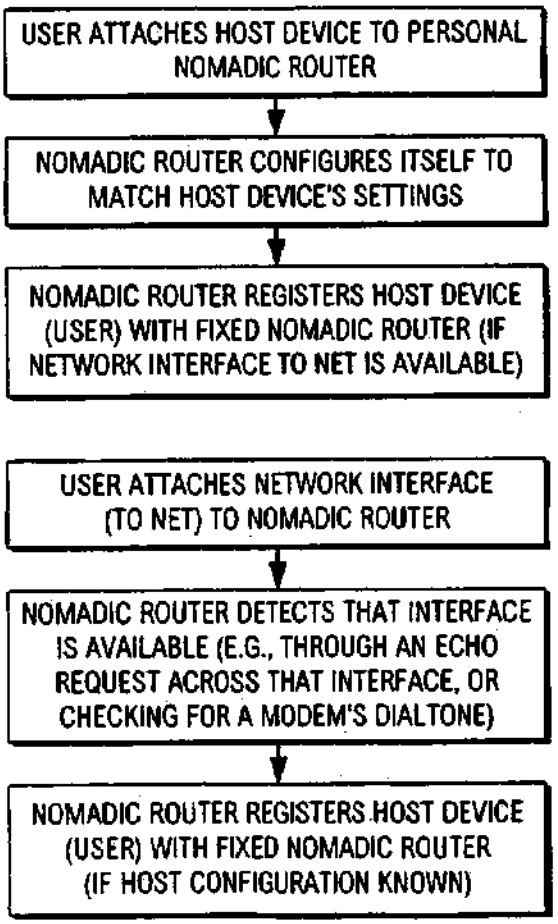

USER ATTACHES HOST DEVICE TO PERSONAL NOMADIC ROUTER
NOMADIC ROUTER CONFIGURES ITSELF TO MATCH HOST DEVICE'S SETTINGS
NOMADIC ROUTER REGISTERS HOST DEVICE (USER) WITH FIXED NOMADIC ROUTER (IF NETWORK INTERFACE TO NET IS AVAILABLE)
USER ATTACHES NETWORK INTERFACE (TO NET) TO NOMADIC ROUTER
NOMADIC ROUTER DETECTS THAT INTERFACE IS AVAILABLE (E.G., THROUGH AN ECHO REQUEST ACROSS THAT INTERFACE, OR CHECKING FOR A MODEM'S DIALTONE)
NOMADIC ROUTER REGISTERS HOST DEVICE (USER) WITH FIXED NOMADIC ROUTER (IF HOST CONFIGURATION KNOWN)

FIG. 3

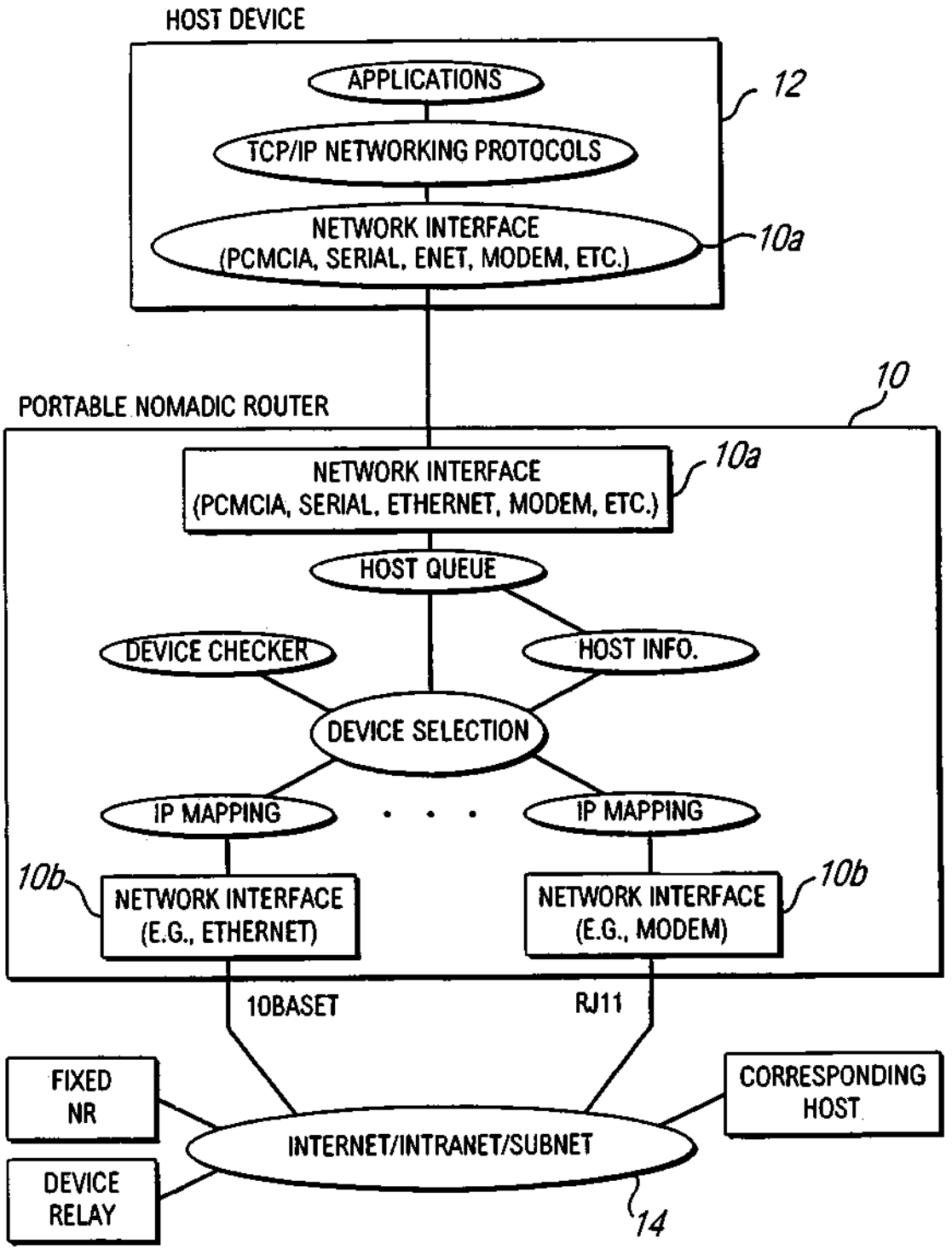

HOST DEVICE
APPLICATIONS
TCP/IP NETWORKING PROTOCOLS
NETWORK INTERFACE
(PCMCIA, SERIAL, ENET, MODEM, ETC.)
12
10a
10
PORTABLE NOMADIC ROUTER
NETWORK INTERFACE
(PCMCIA, SERIAL, ETHERNET, MODEM, ETC.)
10a
HOST QUEUE
DEVICE CHECKER
HOST INFO.
DEVICE SELECTION
IP MAPPING
IP MAPPING
10b
NETWORK INTERFACE
(E.G., ETHERNET)
NETWORK INTERFACE
(E.G., MODEM)
10b
10BASET
RJ11
FIXED
NR
DEVICE
RELAY
INTERNET/INTRANET/SUBNET
14
CORRESPONDING
HOST

FIG. 2

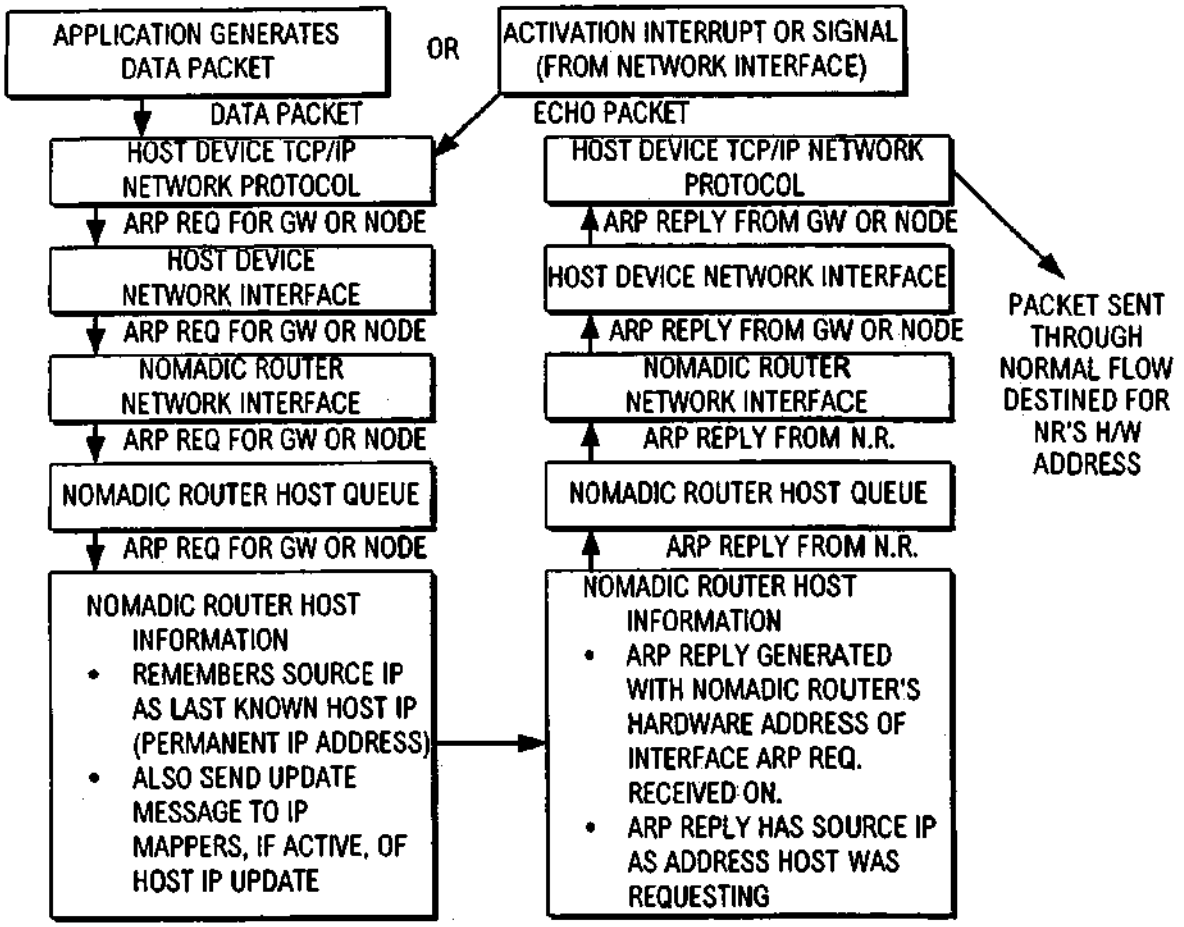

APPLICATION GENERATES DATA PACKET
OR
ACTIVATION INTERRUPT OR SIGNAL (FROM NETWORK INTERFACE)
DATA PACKET
ECHO PACKET
HOST DEVICE TCP/IP NETWORK PROTOCOL
ARP REQ FOR GW OR NODE
HOST DEVICE NETWORK INTERFACE
ARP REQ FOR GW OR NODE
NOMADIC ROUTER NETWORK INTERFACE
ARP REQ FOR GW OR NODE
NOMADIC ROUTER HOST QUEUE
ARP REQ FOR GW OR NODE
NOMADIC ROUTER HOST INFORMATION
• REMEMBERS SOURCE IP AS LAST KNOWN HOST IP (PERMANENT IP ADDRESS)
• ALSO SEND UPDATE MESSAGE TO IP MAPPERS, IF ACTIVE, OF HOST IP UPDATE
HOST DEVICE TCP/IP NETWORK PROTOCOL
ARP REPLY FROM GW OR NODE
HOST DEVICE NETWORK INTERFACE
ARP REPLY FROM GW OR NODE
NOMADIC ROUTER NETWORK INTERFACE
ARP REPLY FROM N.R.
NOMADIC ROUTER HOST QUEUE
ARP REPLY FROM N.R.
NOMADIC ROUTER HOST INFORMATION
• ARP REPLY GENERATED WITH NOMADIC ROUTER'S HARDWARE ADDRESS OF INTERFACE ARP REQ. RECEIVED ON.
• ARP REPLY HAS SOURCE IP AS ADDRESS HOST WAS REQUESTING
PACKET SENT THROUGH NORMAL FLOW DESTINED FOR NR'S H/W ADDRESS

FIG. 4

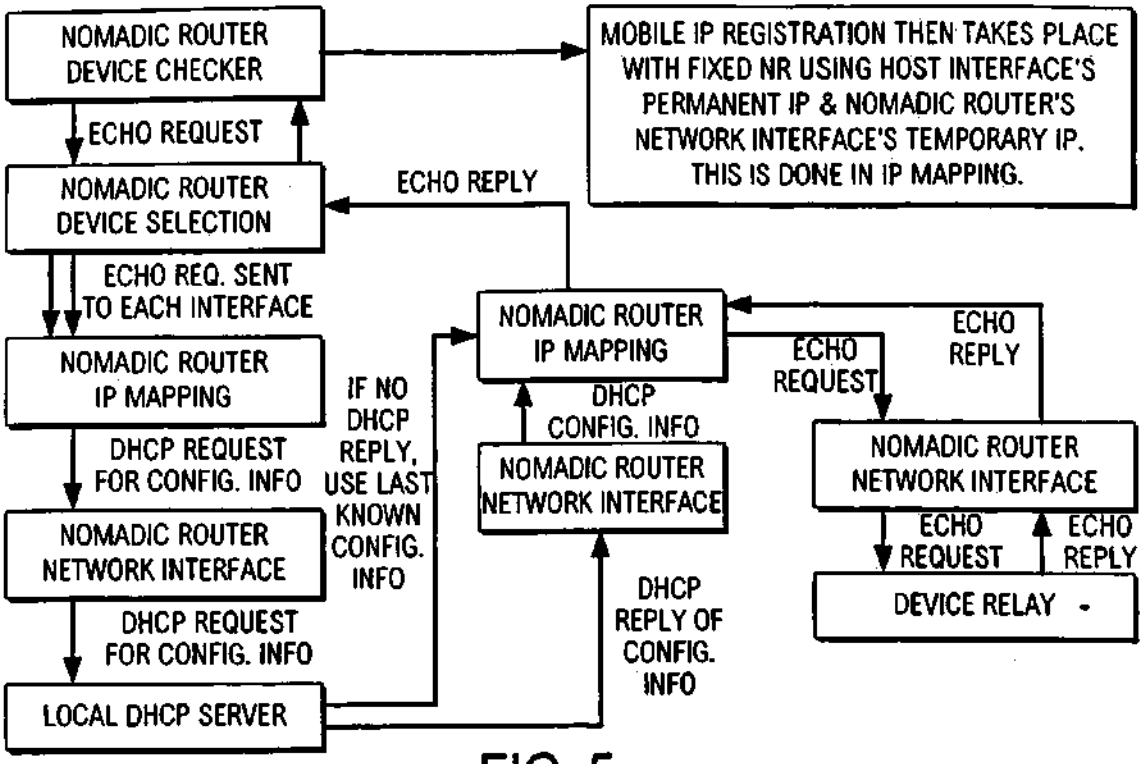

NOMADIC ROUTER DEVICE CHECKER
MOBILE IP REGISTRATION THEN TAKES PLACE WITH FIXED NR USING HOST INTERFACE'S PERMANENT IP & NOMADIC ROUTER'S NETWORK INTERFACE'S TEMPORARY IP. THIS IS DONE IN IP MAPPING.
ECHO REQUEST
NOMADIC ROUTER DEVICE SELECTION
ECHO REPLY
ECHO REQ. SENT TO EACH INTERFACE
NOMADIC ROUTER IP MAPPING
NOMADIC ROUTER IP MAPPING
ECHO REQUEST
ECHO REPLY
IF NO DHCP REPLY, USE LAST KNOWN CONFIG. INFO
DHCP CONFIG. INFO
DHCP REQUEST FOR CONFIG. INFO
NOMADIC ROUTER NETWORK INTERFACE
NOMADIC ROUTER NETWORK INTERFACE
ECHO REQUEST
ECHO REPLY
DHCP REPLY OF CONFIG. INFO
DHCP REQUEST FOR CONFIG. INFO
DEVICE RELAY
LOCAL DHCP SERVER

FIG. 5

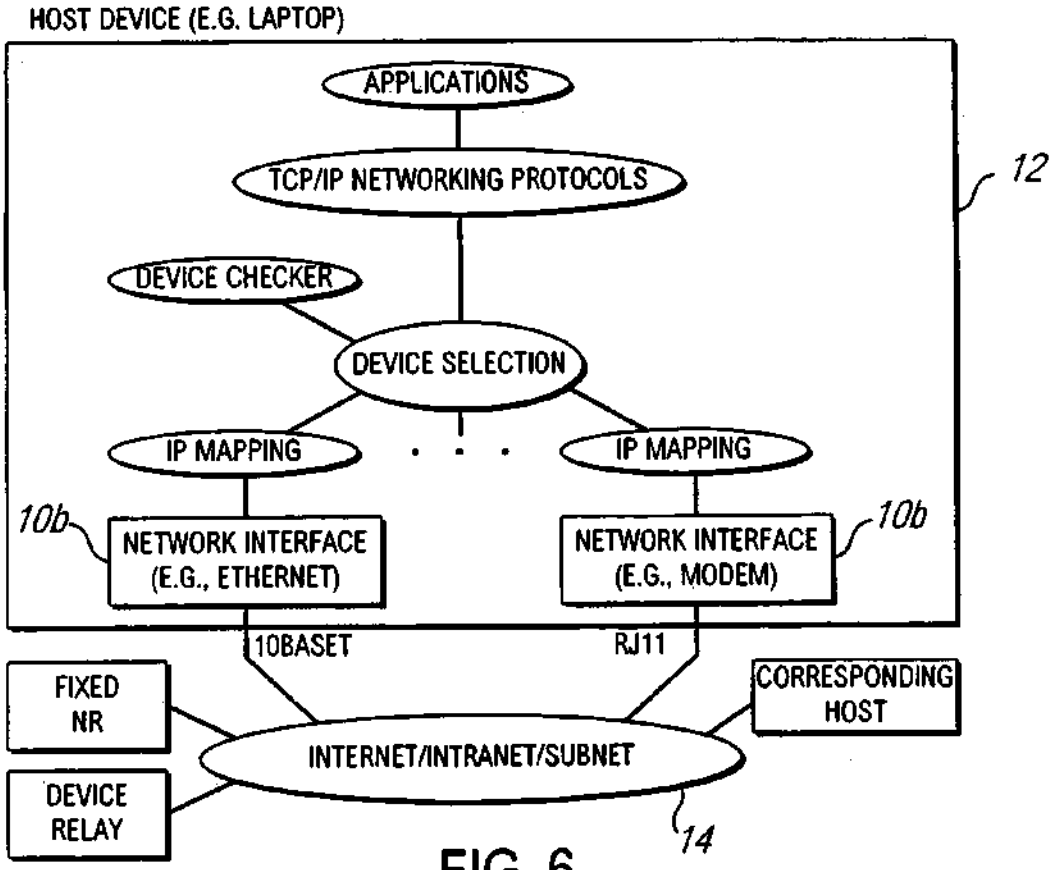

HOST DEVICE (E.G. LAPTOP)
APPLICATIONS
TCP/IP NETWORKING PROTOCOLS
12
DEVICE CHECKER
DEVICE SELECTION
IP MAPPING
IP MAPPING
10b
NETWORK INTERFACE (E.G., ETHERNET)
NETWORK INTERFACE (E.G., MODEM)
10b
10BASET
RJ11
FIXED NR
CORRESPONDING HOST
INTERNET/INTRANET/SUBNET
DEVICE RELAY
14

FIG. 6

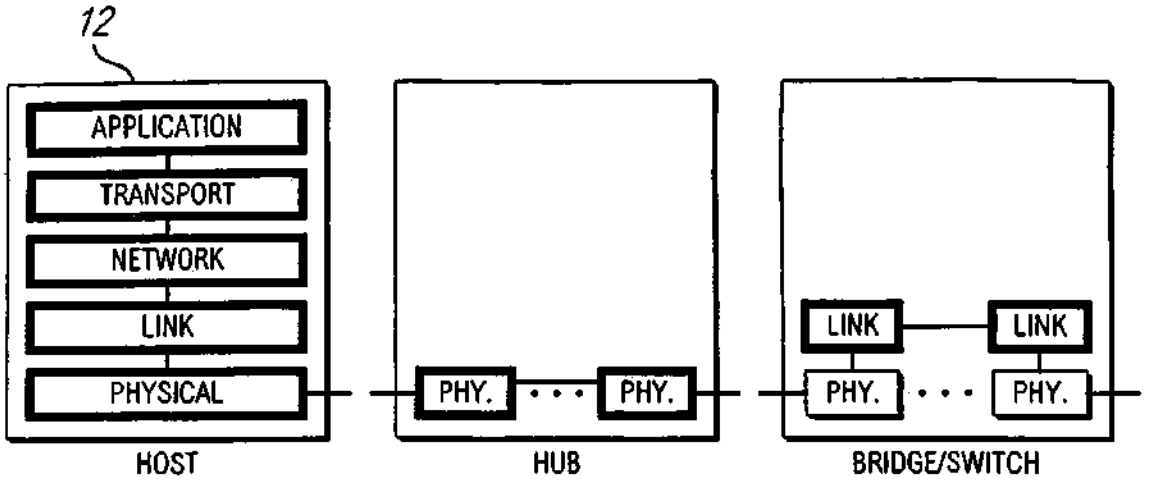


FIG. 7A FIG. 7B FIG. 7C

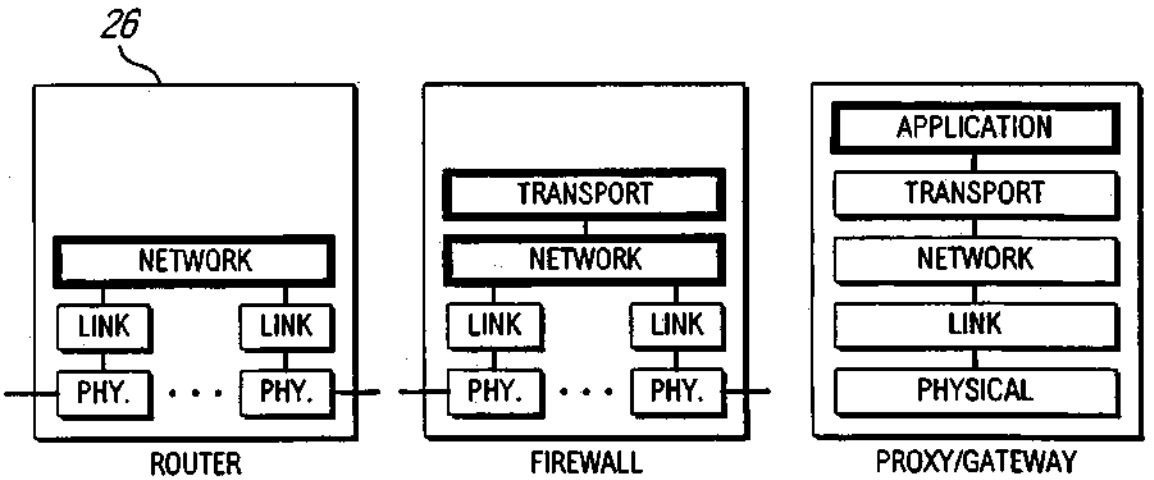


FIG. 7D FIG. 7E FIG. 7F

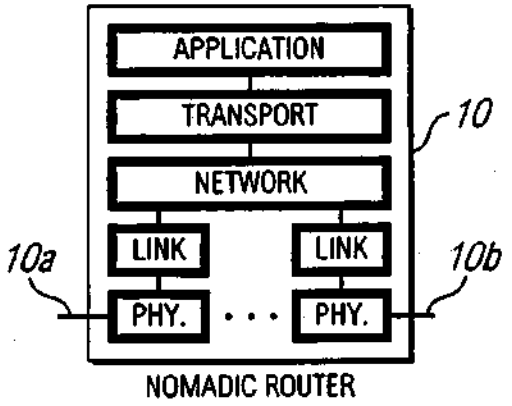


FIG. 7G

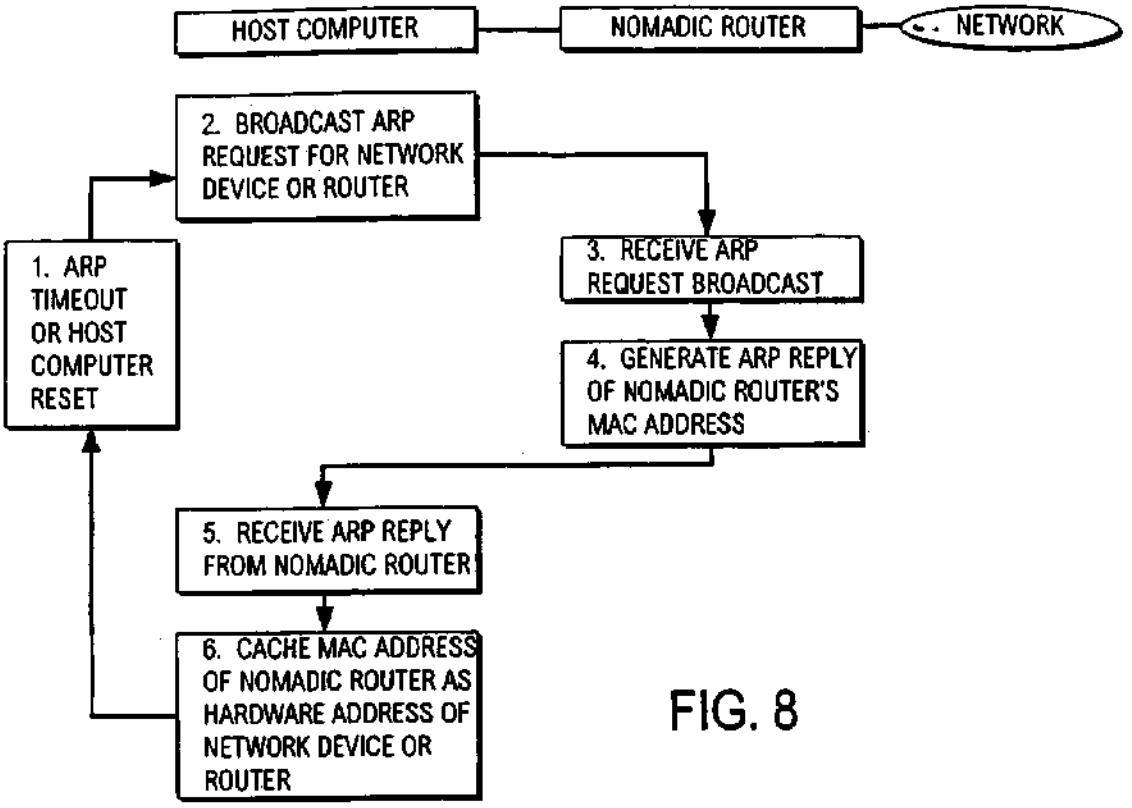

HOST COMPUTER
NOMADIC ROUTER
NETWORK
2. BROADCAST ARP REQUEST FOR NETWORK DEVICE OR ROUTER
1. ARP TIMEOUT OR HOST COMPUTER RESET
3. RECEIVE ARP REQUEST BROADCAST
4. GENERATE ARP REPLY OF NOMADIC ROUTER'S MAC ADDRESS
5. RECEIVE ARP REPLY FROM NOMADIC ROUTER
6. CACHE MAC ADDRESS OF NOMADIC ROUTER AS HARDWARE ADDRESS OF NETWORK DEVICE OR ROUTER

FIG. 8

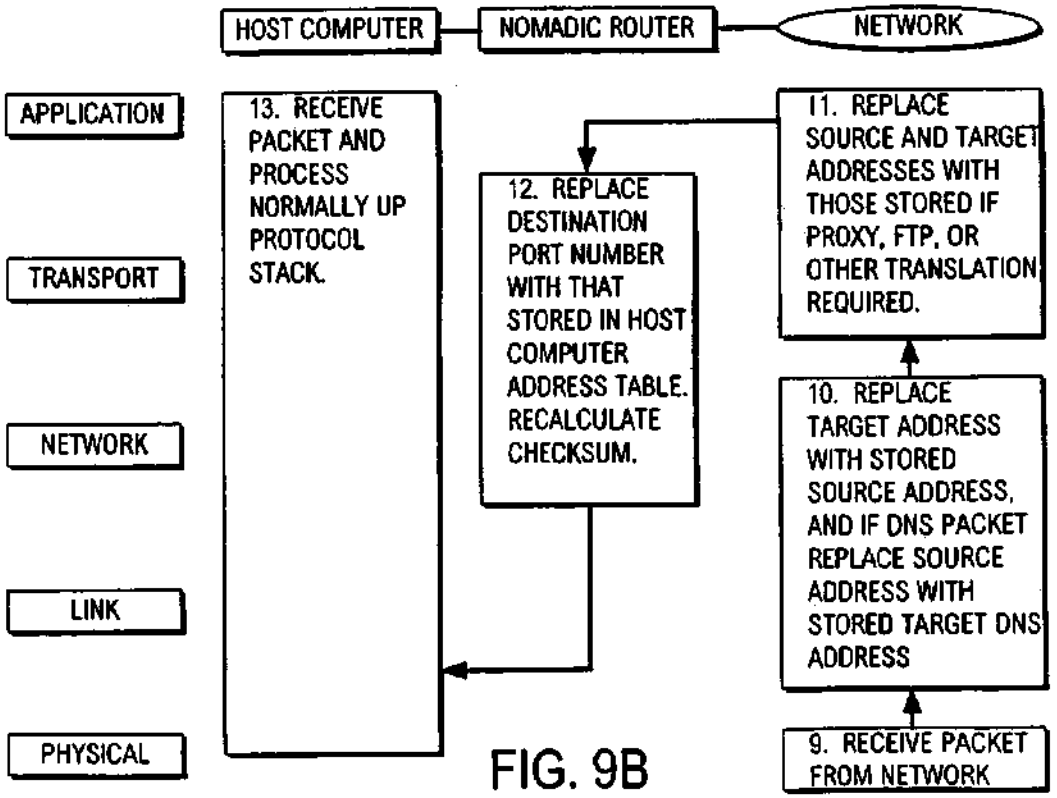

HOST COMPUTER
NOMADIC ROUTER
NETWORK
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
13. RECEIVE PACKET AND PROCESS NORMALLY UP PROTOCOL STACK.
12. REPLACE DESTINATION PORT NUMBER WITH THAT STORED IN HOST COMPUTER ADDRESS TABLE. RECALCULATE CHECKSUM.
11. REPLACE SOURCE AND TARGET ADDRESSES WITH THOSE STORED IF PROXY, FTP, OR OTHER TRANSLATION REQUIRED.
10. REPLACE TARGET ADDRESS WITH STORED SOURCE ADDRESS, AND IF DNS PACKET REPLACE SOURCE ADDRESS WITH STORED TARGET DNS ADDRESS
9. RECEIVE PACKET FROM NETWORK

FIG. 9B

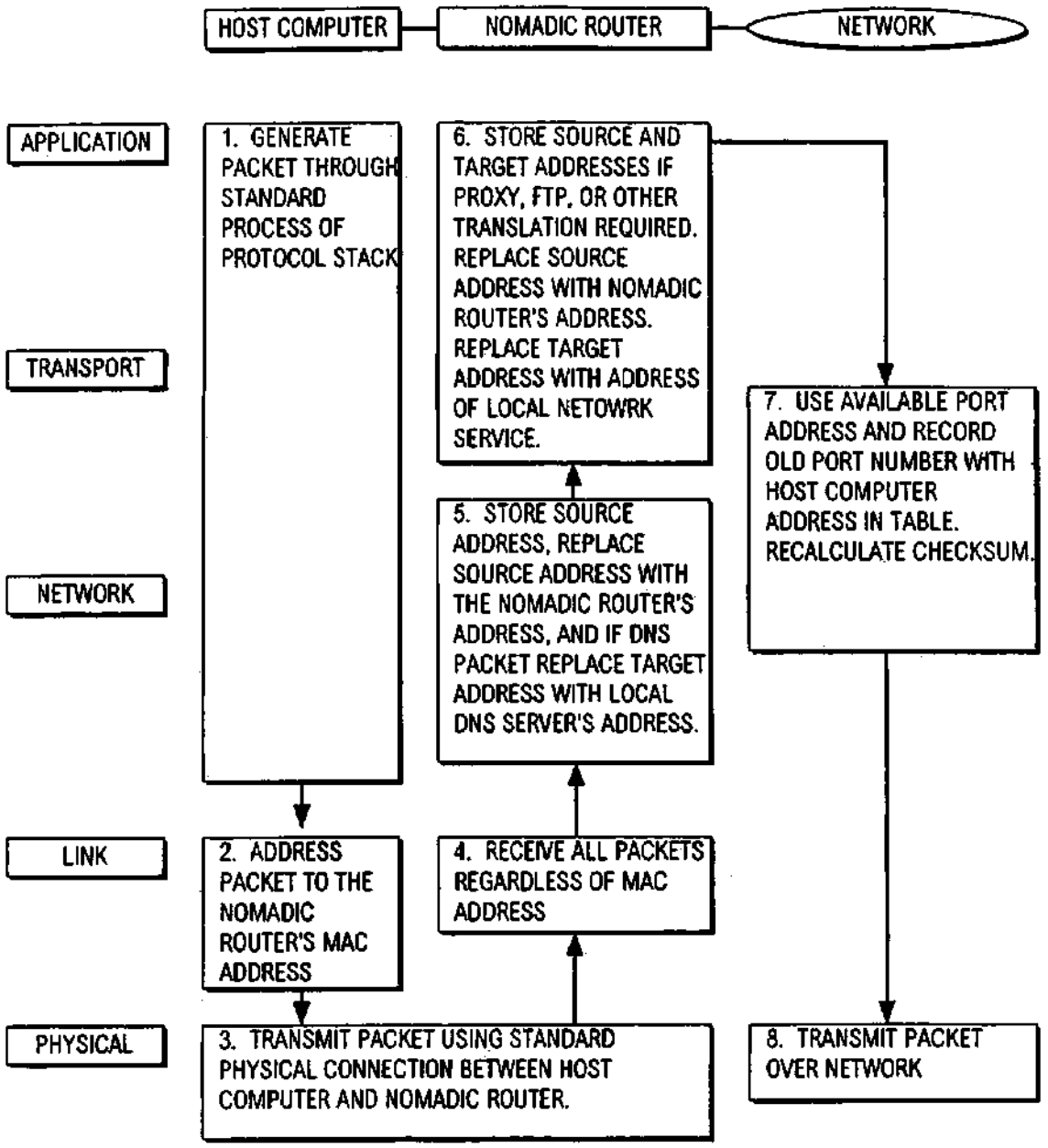

HOST COMPUTER
NOMADIC ROUTER
NETWORK
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
1. GENERATE PACKET THROUGH STANDARD PROCESS OF PROTOCOL STACK
2. ADDRESS PACKET TO THE NOMADIC ROUTER'S MAC ADDRESS
3. TRANSMIT PACKET USING STANDARD PHYSICAL CONNECTION BETWEEN HOST COMPUTER AND NOMADIC ROUTER.
4. RECEIVE ALL PACKETS REGARDLESS OF MAC ADDRESS
5. STORE SOURCE ADDRESS, REPLACE SOURCE ADDRESS WITH THE NOMADIC ROUTER'S ADDRESS, AND IF DNS PACKET REPLACE TARGET ADDRESS WITH LOCAL DNS SERVER'S ADDRESS.
6. STORE SOURCE AND TARGET ADDRESSES IF PROXY, FTP, OR OTHER TRANSLATION REQUIRED. REPLACE SOURCE ADDRESS WITH NOMADIC ROUTER'S ADDRESS. REPLACE TARGET ADDRESS WITH ADDRESS OF LOCAL NETOWRK SERVICE.
7. USE AVAILABLE PORT ADDRESS AND RECORD OLD PORT NUMBER WITH HOST COMPUTER ADDRESS IN TABLE. RECALCULATE CHECKSUM.
8. TRANSMIT PACKET OVER NETWORK

FIG. 9A

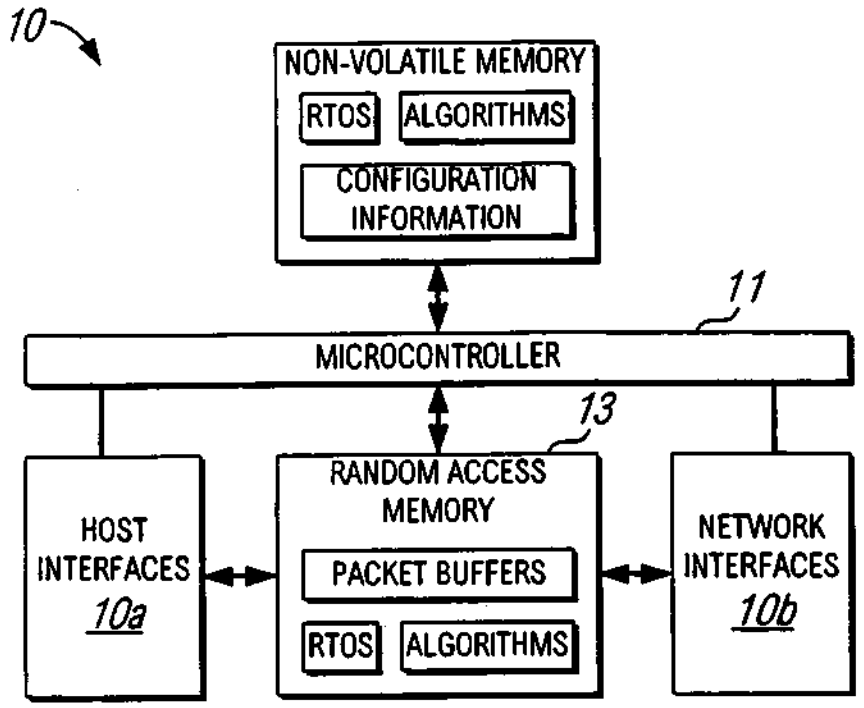

10
NON-VOLATILE MEMORY
RTOS
ALGORITHMS
CONFIGURATION INFORMATION
11
MICROCONTROLLER
13
HOST INTERFACES
10a
RANDOM ACCESS MEMORY
PACKET BUFFERS
RTOS
ALGORITHMS
NETWORK INTERFACES
10b

FIG. 10

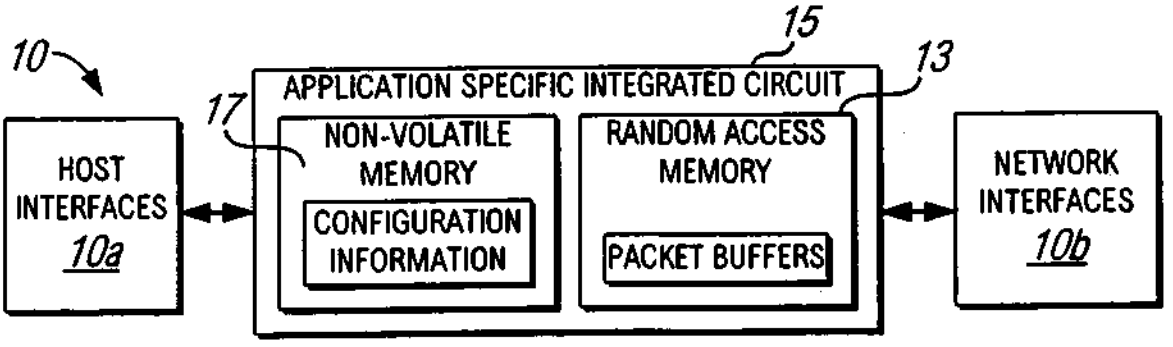

10
15
13
17
APPLICATION SPECIFIC INTEGRATED CIRCUIT
HOST INTERFACES
10a
NON-VOLATILE MEMORY
CONFIGURATION INFORMATION
RANDOM ACCESS MEMORY
PACKET BUFFERS
NETWORK INTERFACES
10b

FIG. 11

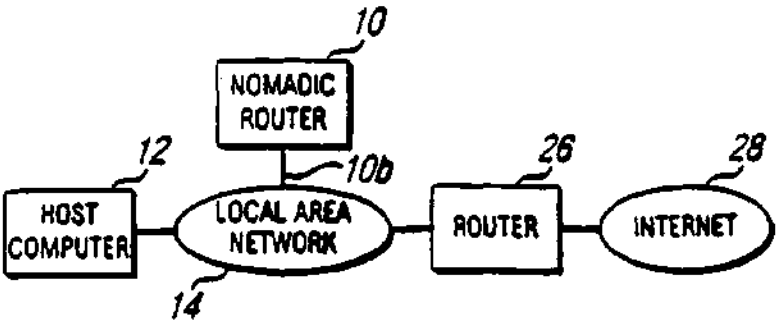


FIG. 12A

FIG. 12B

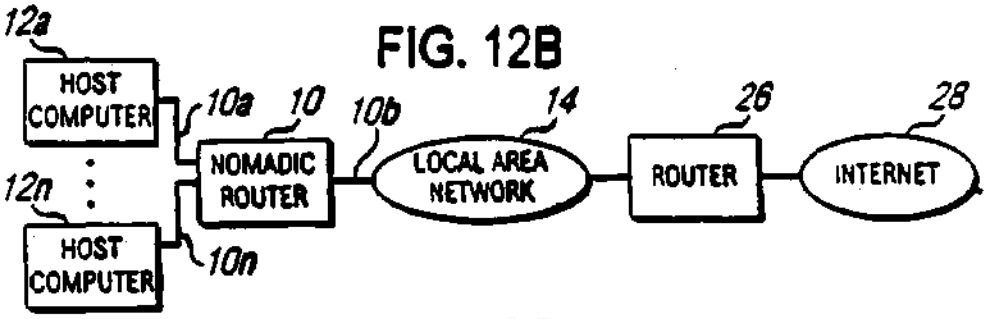


FIG. 12C

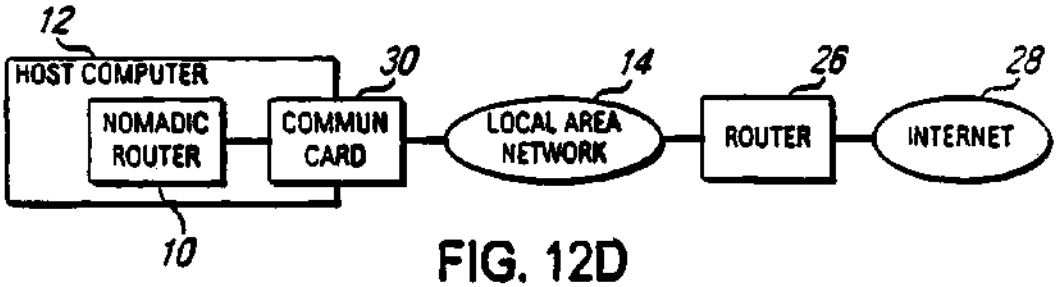


FIG. 12D

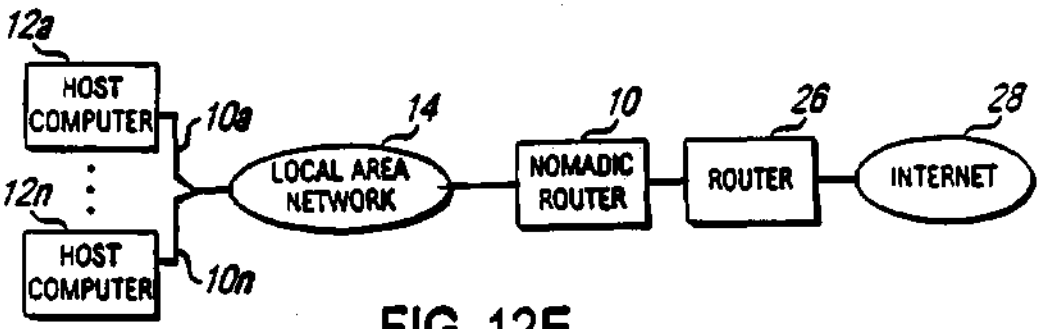


FIG. 12E

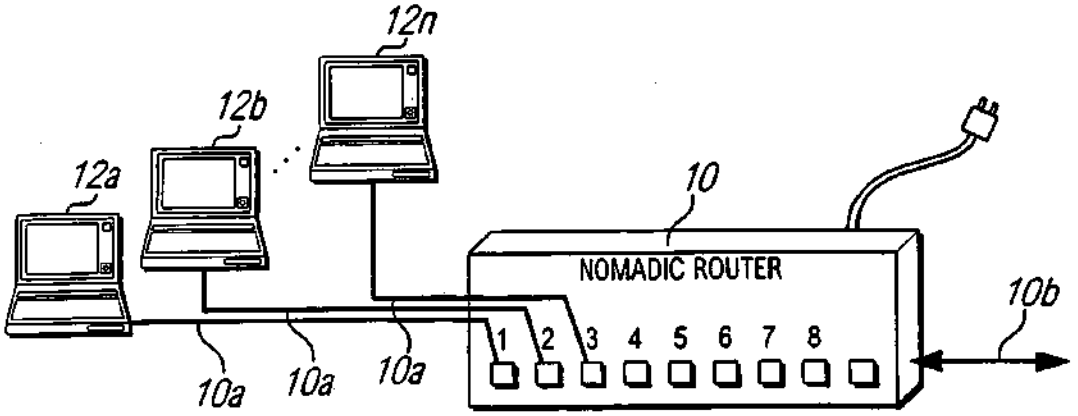


FIG. 13

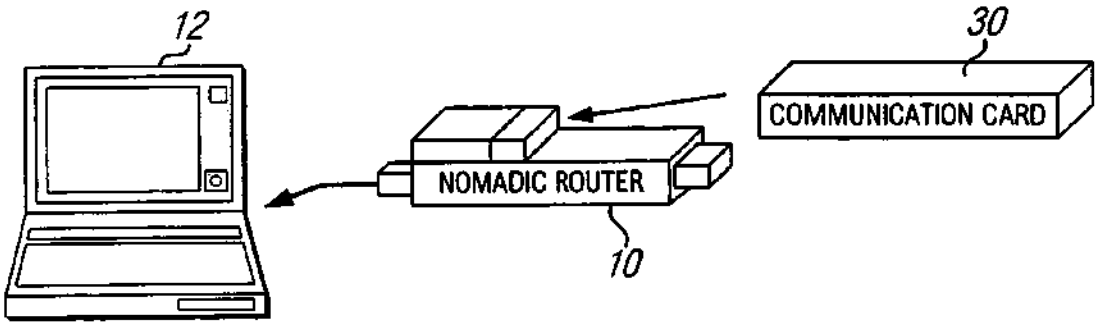


FIG. 14

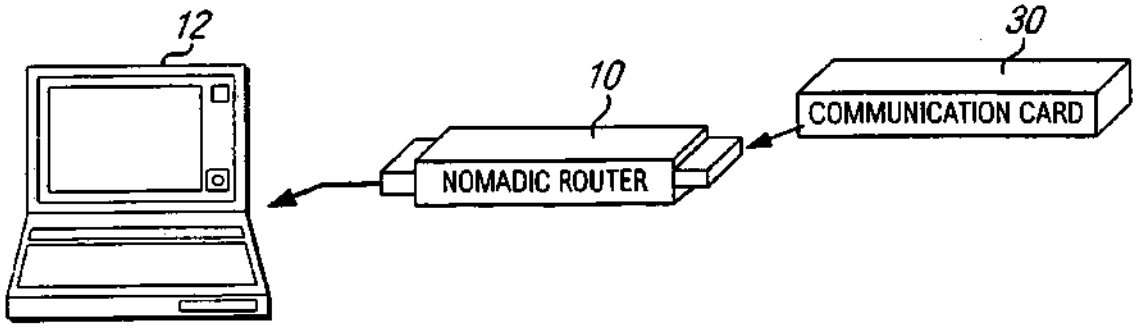


FIG. 15

SYSTEM AND METHOD FOR ESTABLISHING NETWORK CONNECTION WITH UNKNOWN NETWORK AND/OR USER DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. application Ser. No. 09/684,937, filed Oct. 6, 2000, now U.S. Pat. No. 7,088,727; which is a continuation-in-part of U.S. application Ser. No. 09/041,534, filed Mar. 12, 1998, now U.S. Pat. No. 6,130,892; which is a continuation-in-part of U.S. application Ser. No. 08/816,174, filed Mar. 12, 1997, now abandoned.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

The U.S. government may have rights in this invention as provided for by the terms of Contract No. DAAH01-97-C-R179 awarded by DARPA.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is generally related to the art of network communications.

2. Background Art

User digital communication addresses such as internet or IP addresses are conventionally associated with a fixed physical location, similar to a user's business telephone line. However, portable communication devices such as laptop computers are becoming increasingly popular, and it is common for a user to access the internet from locations as diverse as hotel rooms and airplanes.

Digital communication networks are set up to route communications addressed to a communication or network address to an associated destination computer at an established physical location. Thus, if a laptop computer is moved to a remote location, communications to and from the laptop computer may not reach the new physical location.

For a computer (host) to communicate across a network (e.g., the internet), software protocols (e.g., Transport Control Protocol/Internet Protocol (TCP/IP)) must be loaded into the host. A host computer sends information (i.e., packets of data) to another destination computer via devices on the network (routers) which receive the packets and send the packets to the network or segment of the destination host.

The destination host will route replies back using a similar process. Each host computer and router must therefore be configured to send the packets of data to an appropriate router to reach the intended destination. However, a router will receive the packets only if the host computers specifically send (address) the packets to that router at the link layer of the communication protocol. If a host is configured incorrectly (bad address or address of a router not on the local network), then the host computer and router will be unable to communicate, i.e., the router will not listen to the host or will "drop" packets.

With the advent of mobile computers (laptops) and the desire to plug them into various networks to gain access to the resources on the network and internet, a mobile computer must be reconfigured for each network. Traditionally this new configuration can be done either (i) manually in software on the mobile computer (usually causing the mobile computer to be restarted to load the new configuration), or (ii) with a new set of protocols which must be utilized on the mobile computer to obtain the configuration information from a device on the network to which the computer is being connected. When new services (protocols) are created to add functionality to the host computers, these new protocols may need to be updated in the host computers or routers, depending upon the type of new functionality being added.

SUMMARY OF THE INVENTION

In accordance with the present invention, a "Nomadic" router or translator enables a laptop computer or other terminal which is configured to be connected to a local home network to be connected to any location on the internet or other digital data communication system. The nomadic router automatically and transparently reconfigures packets sent to/from the terminal for its new location by processing outgoing and incoming data.

The nomadic router includes a processor which appears as the home network to the terminal, and appears as the terminal to the communication system. The terminal has a terminal address, the nomadic router has a router address, and the terminal transmits outgoing data to the system including the terminal address as a source address. Whether or not the message is addressed to the nomadic router at the link layer, the processor intercepts the message and translates the outgoing data by replacing the permanent address with the router address as the source address. Incoming data intended for the terminal from the system includes the translator address as a destination address, and the processor translates the incoming data by replacing the translator address with the permanent address as the destination address.

The terminal can be directly connected to a point on a local network, and the nomadic router connected to another point on the network. The nomadic router can be employed to implement numerous applications including nomadic e-mail, network file synchronization, database synchronization, instand networking, a nomadic internet, mobile virtual private networking, and trade show routing, and can also be utilized as a fixed nomadic router in hotels, or multi-dwelling units, or multiple tenant units, for example.

The nomadic router can be implemented as software and/or hardware. The nomadic router establishes location and device transparency for a digital communication terminal such as a laptop computer. The terminal can be connected to any of a variety of networks and locations which can employ a variety of communication interface devices.

The nomadic router automatically converts the actual location address to a unique communication address for the user such as an internet address, such that the terminal performs communications originating from the communication address regardless of the physical location of the terminal.

The nomadic router includes software and services which can be packaged in a personal portable device to support a rich set of computing and communications capabilities and services to accommodate the mobility of nomads (users) in a transparent, integrated, and convenient form. This is accomplished by providing device transparency and location transparency to the user.

There is a vast array of communication device alternatives such as Ethernet, Wireless LAN, and dialup modem among which the user switches when in the office, moving around the office, or on the road (such as at a hotel, airport, or home). The device transparency in the nomadic router provides seamless switching among those devices (easily, transparently, intelligently, and without session loss). The location transparency support in the nomadic router prevents users from having to

reconfigure (e.g., IP and gateway address) their network device (laptop) each time they move to a new network or subnetwork.

The present nomadic router provides a separation of location and identity by providing a permanent IP address to the network device (host). The nomadic router provides independence between the location, communication device, and the host operating system. There are no new standards which need to be adopted by the networking community. All specialized processing is stored internally to the nomadic router with standard interfaces to the host device and various communication devices.

The nomadic router supports the migration to Network Computers by providing identity and security services for the user. The nomadic router also supports multiple parallel communication paths across the communications network for soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates.

A portable router for enabling a data communication terminal to be location and device transparent according to the present invention, comprises: a first module for storing a digital communication address of a user; a second module for detecting a data communication network location to which the terminal is connected; a third module for detecting communication devices that are connected to the terminal; a fourth module for establishing data communication between the terminal and the network such that the communication address of the location from the second module is automatically converted to the communication address of the user from the first module; and a fifth module for automatically selecting a communication device which was detected by the third module for use by the fourth module.

The present nomadic router utilizes a unique process embodied in a self-contained apparatus which manipulates the packets of data being sent between the host computers and routers. This process provides an intelligent active universal translation of the content of the packets being transmitted between the host computer and nomadic router. The translation allows the host computer to communicate with the nomadic router, which intercepts packets from the host, even when the host computer is not configured to communicate with the nomadic router.

This is achieved by the nomadic router pretending to be the router for which the host is configured, and by the nomadic router pretending to be the host with which the router expects to communicate. Therefore, the nomadic router supports the mobility of computers in that it enables these computers to plug into the network at different locations (location independence) without having to install, configure, or utilize any net protocols on the mobile computer.

The mobile computer continues to operate without being aware of the change in location or configuration of the new network, and the nomadic router translates the data allowing the host to think that it is communicating with its home router. By putting this process in a self-contained apparatus, the deployment of new protocols can be performed independently of the host computer and its operating system (host independent).

All specialized processing and translation is stored internally in the nomadic router with standard interfaces to the host device and various communication devices. Thus, no new standards need be adopted. By removing the complexity of supporting different network environments out of the mobile computer and into this self-contained apparatus, the nomadic router allows the host computer to maintain a very minimal set of software protocols and functionality (e.g., the minimum functionality typically installed in network computers) to communicate across the network.

The nomadic router translation ability also enables the use of alternate communication paths (device independence) without the host computer being aware of any new communication device that utilizes an alternate communication path. The translation of the packets is done not just at the physical, link, or network layer of the protocol stack but at the transport and application layers as well. This allows the network card, protocol stack, and application running on the host computer to be independent of the network environment and configuration.

As an example of the communication device independence, the translation allows soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates. In addition, the nomadic router translation ability provides a flexible process for deploying enhanced nomadic and mobile computing software and services such as filtering of packets and determining which packets should be allowed to be transmitted between the mobile computer and the nomadic router or local area network (Internal Firewall).

The router apparatus can be: (i) carried with the mobile user (e.g., using an external box); (ii) attached to the mobile computer (e.g. PCMCIA card); (iii) installed inside the mobile computer (e.g., a chip in the laptop); (iv) or installed into the remote network infrastructure to provide network access for any mobile computer (e.g., a box which plugs into the remote or foreign local area network translating packets being sent between the host and its router, or a chip which is installed in routers on the remote network). The nomadic router can also be provided in the form of software which is loaded into and run in the mobile computer or another computer or router on a network.

These and other features and advantages of the present invention will be apparent to those skilled in the art from the following detailed description, taken together with the accompanying drawings, in which like reference numerals refer to like parts.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a diagram illustrating one implementation of a nomadic router positioned between the host computing device and various communication devices using standard interfaces;

FIG. **2** is a diagram illustrating a basic nomadic router architecture, which is referred to as the hardware implementation architecture;

FIG. **3** is a flowchart illustrating a configuration overview of the basic steps performed when a host device is attached to the present nomadic router and when a network interface is attached to the router;

FIG. **4** is a flowchart illustrating automatic adaptation to the host device when the first data packet from the host is sent to a home network router or when an activation interrupt or signal is received;

FIG. **5** is a flowchart illustrating a process initializing and checking the various communication device interfaces for initialization, activation, etc.;

FIG. **6** is a diagram illustrating a basic nomadic router architecture when implemented as software in the host device;

FIGS. **7**A to **7**G are diagrams illustrating protocol stack implementations for various network devices, with the translation function performed for all layers of the protocol stack in the nomadic router;

FIG. **8** is a flowchart illustrating a proxy ARP packet interception and host reconfiguration process;

FIGS. **9**A and **9**B provide a flowchart illustrating a translation process which takes place in the host computer and nomadic router at various levels in the protocol stack;

FIG. **10** is a diagram illustrating the architecture of the nomadic router implemented as a hardware device including a microcontroller and a non-volatile memory for storing algorithms implementing the translation function;

FIG. **11** is a diagram illustrating the architecture of the nomadic router apparatus implemented as an Application Specific Integrated Circuit (ASIC) chip;

FIGS. **12**A to **12**E are diagrams illustrating host and network interface modes in which the nomadic router is able to operate;

FIG. **13** is a simplified perspective view illustrating the nomadic router as implemented in a self-contained box which connects onto a local area network via a network interface port and has multiple ports to connect to host computers;

FIG. **14** is a simplified perspective view illustrating the nomadic router apparatus as implemented on a PCMCIA Type III card where the nomadic router plugs into the host computer's type II slot and the communication card device, of Type II, plugs directly into the nomadic router so both may be powered and stored in the portable host computer; and

FIG. **15** is a simplified perspective view illustrating the nomadic router as implemented on a PCMCIA Type II cared where the nomadic router plugs into the host computer via a type II interface slot and where the communication card device, Type II, plugs into the nomadic router type II card.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

FIG. **1** illustrates a "nomadic" translator or router **10** embodying the present invention as being connected between a host device or computer **12** and a communications device **14**. Host device **12** is a laptop computer or other fixed or mobile digital data communication terminal which is sufficiently portable or mobile that it can be carried from one location to another. A laptop computer, for example, can be used in any convenient location such as an airplane, customer's office, home, etc.

Communications device **14** can be part of any type of communication system to which host computer **12** can be connected. Such communication systems include, but are not limited to, local networks, wide area networks, dial-up and direct internet communications, etc. In a typical application, the communications device will connect the host computer to a local network which itself is connected to the internet Thus, host device **12** is able to communicate with an unlimited number of networks and nodes which are themselves interconnected with routers, switches, bridges, etc. in any known manner.

Router **10** includes a terminal interface **10***a* which normally is used to connect router **10** to host device **12**, and a system interface **10***b* which connects router **10** to communications device **14**. Router **10** generally includes a processor consisting of hardware and/or software which implements the required functionality. Router **10** is further configured to operate in an alternate mode in which host device **12** is connected directly to a network, and router **10** is also connected to a point in the network via system interface **10***b*. In this case, terminal interface **10***a* is unused.

Although device **10** is described herein as being a router, it will be understood that router **10** is not a conventional router in that it includes the capability for providing interconnectability between networks. Instead, router **10** is essentially a translator which enables host device **12** to be automatically and transparently connected to any communications device **14**, and process incoming and outgoing data for device **12**.

Host device **12** may be provided with a permanent internet address which conveniently need not be changed in accordance with the present invention. Device **12** is initially configured to communicate with a particular gateway or other home device at its base location. The gateway has a link layer address which device **12** attempts to locate when it is connected to any communication system. Without the functionality of the present nomadic router **10**, host device **12** would not be able to operate at a remote location because it would not find its gateway.

It will be understood that the term "home" does not relate to a residence, but is the network, gateway or other communication device or system to which the terminal is normally connected and which corresponds to the home internet or IP address.

FIG. **1** further illustrates a top protocol layer **16** representing host computer device **12** which generates and consumes data that is transferred through communications device **14**. Interface **16** is below the IP layer, and above the link layer in the typical OSI/ISO model. In the middle is a layer **18**, which represents router **10**, whose function is to adaptively configure and utilize the underlying communications device and provide router support. A lower layer **20** is a physical communication which carries out the communication (potentially wire-lined internet based, ad-hoc or wireless) as made available and determined for use by the nomadic router or user. Between router layer **18** and layers **16** and **20** are interfaces **22** and **24** which router **10** identifies and configures dynamically.

The present invention operates with host computers, routers, and other network devices through well-defined standard interfaces such as specified by the IETF (Internet Engineering Task Force) and IEEE standardization committees. These standards specify the packet format, content, and physical communication characteristics. As shown in FIG. **7**A, host computers have to be configured at various layers of the protocol stack depending on the communication capabilities and configurations of the current network.

Hubs, as shown in FIG. **7**B, provide a well defined interface to connect host computers and network devices by transmitting packets across multiple physical connections. Hubs do not provide any manipulation or translation of the content of the packets being transmitted.

Bridges or switches, as shown in FIG. **7**C, provide an intelligent filtering mechanism by which packets are transmitted across multiple physical connections based upon the physical connection the device is connected to, according to the link layer addressing (Media Access Control Address). Bridges and switches do not manipulate the content of the packet and do not provide any higher layer protocol functionality.

Routers, as shown in FIG. **7**D, accept packets based upon the destination address at the network layer in the packet. However, the host computer must explicitly address the packet to the router at the link layer. The router will then retransmit the packet across the correct physical connection based upon hos it is configured. No modification or translation of the packet is performed at any higher layer of the protocol stack than the network layer.

Firewalls, as shown in FIG. **7**E, filter packets at the network and transport layers to allow only certain packets to be retransmitted on the other physical connection. Firewalls do

not manipulate the content of the packet, only forward it on to the next hop in the network if it passes the transport (port) or network (IP address) filter.

Proxies and gateways, as shown in FIG. **7**F, only receive packets explicitly addressed to them by host computers. They only manipulate packets at the application level. The present nomadic router **10**, as shown in FIG. **7***g*, manipulates and content of the packets at the link, network, transport, and application layers of the protocol stack to provide a translation between the host computer configuration and the configuration of the remote or foreign network to which the host computer is currently attached.

Unlike all other devices shown in FIGS. **7**A to **7**F, router **10** will automatically intercept and translate packets without the other devices being aware of router **10** or being configured to use it, i.e., without packets being addressed to router **10**. The translation algorithms in router **10** which provide this location independence are provided completely internal to router **10**. Thus, no new standards need to be developed, accepted, or implemented in host computers **12** or routers **26** to deploy new network services when using the nomadic router.

Whenever a new or different communication device (which includes the link and physical layers) is utilized in a host computer **12**, the host computer's network layer must be aware of this new communication device. Since router **10** has its own network interface to the communication device, alternate communication devices can be utilized in router **10** which the host computer **12** can utilize but does not have to be configured to use.

Permanent Addressing not Location Based

Today we communicate with individuals in terms of the location of their communications instruments (for instance, their computer's IP address or their fax machine's phone number). To support mobility and changing communication environments and devices, it is necessary to create an environment where people communicate with other people, and not specifically with the devices they use. To transparently support mobility and adaptivity in a wireless, potentially ad-hoc, communication internetwork, a common virtual network must be provided by an intelligent device or agent which supports the various computing hosts and communication devices.

The present nomadic router **10** provides the mapping between the location based IP address used in the internet today and the permanent user based address housed in the host CPU in the device **12**. This is illustrated in FIG. **2** as "IP Mapping." This mapping is done without support or knowledge of such mapping by the host CPU or user.

The internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU but rather are internal to the nomadic router. The host configuration information, such as IP number, is discovered or determined as illustrated in FIG. **4** and stored in nomadic router **10** as illustrated in FIG. **2** as "Host Info." This configuration process is overviewed in FIG. **3**.

Optional Off-Loaded Processing

As illustrated in FIG. **2**, nomadic router **10** can provide off-load communication processing for the host CPU by being physically separate from host device **12**. The adaptation, selection, and transportation of information across the network is performed by nomadic router **10**. This allows the host terminal or device **12** to utilize the network without having to directly support the network protocols. By having the nomadic router be responsible for adapting to the current network substrate, the host CPU can maintain a higher performance because the routing, adaptation, packetization, etc. algorithms, or packet processing, are performed by router **10**.

The nomadic router can also queue, transmit, and receive data independent of whether the host device **12** is available or even attached. CPU **11** built into nomadic router **10** may provide all necessary computing routines to be a fully functional network co-processor independent of the host CPU. This will allow increased battery life for the user because the nomadic router does not have numerous user I/O devices as does the host device **12**.

Location Independence

The instant network nomadic router provides the ability to provide ubiquitous and reliable support in a location independent fashion. This removes any burden on the user for device reconfiguration (e.g., IP address configuration, gateway or next hop router address, netmask, link level parameters, and security permissions) or data transmission.

The problem with existing protocol stacks is that communicating devices have to be reconfigured every time the communication environment changes. TCP/IP requires a new network node and gateway number. Appletalk will automatically choose an unused node number and discover the network number, but all open communications are lost and services have to be restarted to begin using the new information.

This occurs, for example, when a PowerBook is plugged into a network, put to sleep, and then powered up in a different network. All network services are restarted upon wakeup, and network applications get confused if they are not restarted. The nomadic router solves this problem by providing temporary as well as permanent network and node numbers similar to that provided by Mobile IP. However, the nomadic router will also work with other protocol stacks (e.g., AppleTalk).

Mobile IP provides location independence at the network level and not at the link level. All link level parameters, which are device specific, will be automatically configured as illustrated in FIG. **5** when a new communications (network interface) device is attached to the nomadic router. The nomadic router completely eliminates the need for manual configuration by adaptively supporting device independence.

Multiple Substrates (Device Independence)

Another innovative feature of the nomadic router is the support for simultaneous use of multiple communication substrates. This is illustrated in FIG. **2** as "Device Selection." Users should be able to utilize two or more communication substrates, either to increase throughput or to provide soft-handoff capability. This functionality is not supported in today's typical protocol stacks (e.g., TCP/IP or AppleTalk).

For example, via the "network" control panel, the user can select between communications substrates such as EtherTalk, LocalTalk, Wireless, ARA, etc., but cannot remotely login across EtherTalk while trying to print via LocalTalk. Routers are typically able to bridge together various communication substrates, but merging the LocalTalk and EtherTalk networks together is often not desirable for many reasons, including performance and security.

A problem with existing routers is that they require manual configuration and exist external to the node. To overcome this, the nomadic router can support automatic configuration and full router functionality internally. This allows a mobile or nomadic node to adapt to various communication and network devices dynamically, such as when the user plugs in a PCMCIA card or attaches a communications device to the serial port.

Once the nomadic router becomes aware of the available communication devices and activates them, the transport of

data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use, is shown in FIG. **2** and FIG. **5** as part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface.

There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Another feature of the nomadic router is the support for alternate or simultaneous use of various communication substrates. This is performed as part of step **5** in FIG. **6** when the source address is that of the communication substrate on which the nomadic router is going to send the packet. Host computers will now indirectly be able to utilize two or more communication substrates, either to increase throughput or to provide soft-handoff capability.

This functionality is not supported in typical protocol stacks (e.g. TCP/IP or AppleTalk). Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use is part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface.

There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Hardware Specification

The nomadic router can run completely in software without any special hardware as shown in FIG. **6**, or without a CPU separate from the main host, or packaged in the form of a hardware device as shown in FIG. **2**. The nomadic router can also be provided as a digital storage medium which stores the software program that implements the functionality of the router's translation processing. Examples of digital storage media include optical media (e.g. CD-ROM), magnetic media (e.g. floppy disks), non-volatile or read-only memories, or any combination thereof. The program is loaded into and run on mobile terminal **12**, or alternatively into any other computer or router which is connected to a network.

One potential implementation of the nomadic router device uses Embedded PC Technology. As an example, the rugged PC/104 standard modules have a form-factor of 3.550" by 3.775" and typically 0.6" per module and weigh approximately 7 oz. per module. The PC/104 module's utilization of a self-stacking bus with minimum component count and power consumption (typically 1-2 Watts per module) eliminates the need for a backplane or card cage.

The nomadic router can run on a 16 bit bus with an 80486 processor, for example. The standard network access devices can support burst rates up to 10 Mbps with typical user data throughput around 1-2 Mbps. The user bandwidth is less depending on the available wireless communication device. For example, Proxim's 2 Mbps wireless LAN typically covers 500 yards with user data throughput around 500 Kbps. As illustrated in FIG. **1**, nomadic router **10** typically includes 3 modules; a processor **10**, host device or terminal interface **10***a*, and communication device or system interface **10***b*.

Another potential hardware implementation is with the CARDIO S-MOS System technology. This CPU board is basically the same size as a PCMCIA credit card adapter. It is 3.55×3.775×0.6 inches. The power requirements are +5V DC +/**31** 10% with an operating temperature of 0 to 70° C., a storage temperature of −40 to 85° C., and relative humidity of 10% to 85% non-condensing.

The CARDIO is the most compact PC/104 compatible system available which meets the one-stack mechanical and electrical PC/104 Rev. 2.2 specifications. Power fail indicator, battery backup, and automatic switchover are also possible.

The nomadic router can also be implemented on a small portable device such as a PCMCIA card or partially on a PCMCIA card. In the case of a full implementation on a PCMCIA card, the host CPU and power supply are used to execute the Nomadic Routing and other protocols, algorithms, operating system, and application services. A hybrid implementation with some components as part of a PCMCIA card and others as part of other hardware implementation can also be used.

Apparatus Components

By performing packet translation in a self-contained apparatus, processing done on the packets in the nomadic router does not affect the host computer. All specific translation of the packets to match the network's configuration and available services is done internally to the nomadic router. The nomadic router can queue, transmit, and receive data independent of whether the host computer is available or even attached. The algorithms and microcontroller built into the nomadic router provides all necessary computing routines to be a fully functional network co-processor independent of the host computer.

By allowing the nomadic router to process packets independently of the host computer, the host computer can be powered down or asleep while processing is taking place, providing an increase in battery life for the mobile host computer.

The nomadic router can be configured with various components in several different ways. In FIG. **10**, the nomadic router contains a processor or microcontroller **11** to translate the packets stored in packet buffers in random access memory. The translation functions are stored in non-volatile memory **13** with the Real Time Operating System (RTOS) and configuration information relative to the types of translation that need to be performed.

Upon startup (boot) of the nomadic router, the RTOS and translation algorithms are loaded from non-volatile memory into RAM where they are executed. There may be zero, one, or more host interfaces in which host computers are connected. There are one or more network interfaces. If no host interface is available, the nomadic router receives packets via the host computer from the network interface.

In FIG. **11**, nomadic router **10** is implemented as an Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA) **15**. These chips embed the algorithms for packet translation. The chip can include storage for non-volatile memory **17** which stores the configuration information such as when manually configured for the current network. The chip **15** can also include random access memory to buffer packets for translation in the nomadic router before being sent off to the host or network interface.

Apparatus Packaging

As described above, the nomadic router can be packaged in several different hardware configurations. The nomadic router can be embedded in the host computer, or a network device, such as a switch or router. It can also be implemented as a PCMCIA card which plugs into the host computer, or as a self-contained external box.

Each nomadic router can have from one to many interfaces. If router **10** is put into the network infrastructure, it does not have to be carried around with the mobile user. As shown in FIG. **12***a*, nomadic router **10** is attached to a Local Area. Network (LAN) of the network infrastructure (which constitutes the communications device **14**) through system interface **10***b*. LAN **14** is connected through a conventional router **26** to the internet **28**. In this case, host computer interface **10***a* of nomadic router **10** is not needed since packets from host computer **12** are received through LAN. **14**.

To provide a secure interface between host computer **12** and network **14** to prevent host computers from being able to watch (sniff) packets on network **14**, nomadic router **10** can have one interface to host computer **12** (terminal interface **10***a*) and a second interface (**10***b*) to network **14** as shown in FIG. **12**B. Nomadic router **10** can provide filtering of packets received and retransmitted between the various interfaces thus providing a firewall type of security device which operates internally on the network.

To support multiple host computers **12***a* . . . **12***n* with a single nomadic router **10**, nomadic router **10** may have multiple host interfaces $\mathbf{10}a_1 \ldots \mathbf{10}a_n$ as shown in FIG. **12**C and in FIG. **13**, and a network or system interface **10***b*.

If the nomadic router is carried around by the mobile user, it can take the form of a PCMCIA card. In FIG. **12**D, nomadic router **10** is implemented as a PCMCIA card. The processing and translation capability is stored inside the card and the interface to host computer **12** is through a PCMCIA BUS interface or communication card **30**.

The nomadic router may also be used as an interface between a local area network **14** and a router **26** as illustrated in FIG. **12**E. Local area network **14** may be a mobile or portable network with router **26** being fixed at a particular location with a physical connection to the internet. Such an arrangement may be used for a customer demonstration or trade show, for example, where the local area network **14** is established among computers previously configured to communicate with each other but not with the foreign network having router **26**.

As shown in FIG. **14**, the PCMCIA card can fit in a type III slot where there is a connector on nomadic router **10** which accepts communication card **30** (a type II PCMCIA card). In this mode, the nomadic router does not require internal communication device specific components.

Nomadic router **10** can also take the form of a type II PCMCIA card. In this form, the communication device or card **30** plugs into the opposite end of nomadic router card **10** as illustrated in FIG. **15**.

Translation Operation of the Nomadic Router

Initialization and Self Configuration

The nomadic router initialization and self configuration process provides the means by which the nomadic router is able to learn about the host computer and network so it knows what translation is necessary.

Host Learning

Depending on the particular application, the nomadic router may have to learn the configuration of the host computer, the remote/foreign network, or both. For example, when utilized as a fixed nomadic router in a hotel or multiple dwelling unit, the nomadic router will have already learned (or been manually configured for) the remote/foreign network. The nomadic router need only determine the settings of mobile hosts which are subsequently connected to the network. Similarly, when the nomadic router is implemented as a PCMCIA card which travels with the mobile host, the nomadic router need only learn the settings of the foreign/remote network (since the host settings were previously learned or manually configured). In some applications, the nomadic router learns both the network and host configurations as previously described.

Nomadic router **10** is able to learn the host computer **12** configuration by looking at the content of the packets sent from host computer **12**. Rather than host computer **12** sending packets directly to router **26** or other network device (which is what it is initially configured to do), nomadic router **10** is able to redirect all outbound packets from the host computer **12** to itself. This redirection can be accomplished in several ways as described below.

1. Proxy ARP Packet Interception and Host Reconfiguration

Whenever a host computer **12** has an IP packet to send to router **26** or other network device, host computer **12** uses the Address Resolution Protocol (ARP) to obtain the link layer Media Access Control address (MAC address). As illustrated in FIG. **8**, when host computer **12** broadcasts an ARP request for the MAC address of a destination node, nomadic router **10** intercepts this ARP request broadcast and responds with its own MAC address (rather than that of the destination node).

When host computer **12** receives the ARP reply from nomadic router **10** (which contains the MAC address of nomadic router **10**), host computer **12** will cache this MAC address and send all packets destined for the configured router or network device to the MAC address of nomadic router **10**. Host computer **12** will think that the MAC address is that of its originally configured IP network device. However, nomadic router **10** is only pretending (proxying) to be the device (its home gateway) that host computer **12** expects to find.

The nomadic router **10** is also able to reconfigure and intercept return packets from a router or other network device using the same process.

2. Promiscuous Mode Packet Interception

Since the MAC address is cached in host computer **12** for a short period of time, host computer **12** will not send out a new ARP request to obtain the MAC address again unless a timeout period occurs or the cache is cleared, such as when computer **12** is restarted.

When a conventional network device receives or hears a packet with a MAC address which does not match its own, it will ignore or drop the packet. Since it is possible to rapidly switch from one network environment to another using a portable computer, nomadic router **10** must be able to intercept packets even when the MAC address is not that of the nomadic router's home gateway or device.

This is accomplished by placing the nomadic router's network connection is promiscuous mode. In this mode, the network connection on the nomadic router accepts all packets being transmitted on the communication link, not just ones being broadcast or addressed specifically to it.

3. Dynamic Host Configuration Protocol (DHCP) Service

Nomadic router **10** may also provide other network services to host computer **12**. For example, host computer **12** may be able to utilize the DHCP service to obtain configuration information rather than being manually configured. However, a host computer utilizing the DHCP service requires that a DHCP server be installed on the network segment to which it is currently attached. If the host computer **12** is configured to use this service but a DHCP server is not available on the remote/foreign network, nomadic router **10** will intercept the DHCP requests and respond with configuration information for host computer **12** to use.

Network Learning

The nomadic router is able to learn about the network environment it is currently attached using several different methods as described below.

1. Dynamic Host Configuration Protocol (DHCP)

When the nomadic router is connected to a different network, it will broadcast a DHCP request to obtain configuration information for that network. If no DHCP service is available on the network, the nomadic router will use another method to learn about the network configuration.

2. Router Information Packets

For example, routers on the network will periodically broadcast router information packets which are used to build routing tables and allow routers to adapt to changes in the network. Nomadic router **10** will listen on the network for these router information packets. When a router information packet is received, the nomadic router will extract the configuration information from each packet and store the information for use in translating packets from the mobile host.

3. Passive Learning

By placing the nomadic router's network connection in promiscuous mode, the nomadic router receives all packets (not just ones addressed to the nomadic router). The nomadic router examines all packets received on the network interface to discover the network configuration. The nomadic router is also able to determine the IP addresses used on the current network and which machines are routers (by the final destination address not being the next hop address).

Using this method, nomadic router **10** is passively able to learn how the network is configured and will elect to use an unused IP address. If that IP address does become used by another network device, the nomadic router will switch over to another unused IP address.

4. Manual Configuration

The network configuration information can also be manually configured in the nomadic router **10** as described above. This information can be set using an embedded web server, Simple Network Management Protocol (SNMP) tools, an application running on one of the computers in the network, or other suitable means. When manual configuration is used to set the network configuration, nomadic router **10** will still automatically learn the host information and provide all the translation capabilities so the host computers do not have to be aware of the correct network information of the LAN to which they are currently connected.

Packet Translation

After learning the network and/or host computer configuration(s), the nomadic router has the necessary information to translate packets transmitted/received by the host computer. The nomadic router's packet translation function provides a mapping between location and service dependent configurations used by host computer **12** and that used by network **14** to which it is currently attached. For outbound traffic from host computer **12** to network **14**, the translation function changes the content of the packet such as the source address, checksum, and application specific parameters, causing all packets sent out to network **14** to be directed back to nomadic router **10** rather than to host computer **12**.

Inbound traffic from network **14** arriving at nomadic router **10** (which is really for host computer **12**), is passed through the translation function so host computer **12** thinks that the replies were sent directly to it. Host computer **12** will be completely unaware of all the translation being performed by nomadic router **10**.

The translation functions works as illustrated in FIGS. **9***a* and **9***b*. In these figures, the operations performed in the OSI/ISO model application, transport, network, link, and physical layers are illustrated in rows opposite the layer designations. The operations performed by host computer **12**, nomadic router **10** and network **14** are illustrated in columns below the device designations.

Host computer **12** will generate network packets using the current configuration stored in host computer **12** using the standard protocol stack as shown in step **1**. This configuration information is either manually configured in host computer **12** or obtained using DHCP (from the network or the nomadic router).

As shown in step **2**, when host computer **12** attaches the link level destination address (automatically obtained using the Proxy ARP packet interception routine described earlier), host computer **12** will send the packet to the network address of its standard router or home gateway device using the link level address of the nomadic router **10**.

In step **3**, the packet is transmitted across the standard physical connection between host computer **12** and nomadic router **10**. As shown in step **4**, nomadic router **10** will receive the packet at the link level either because the Proxy ARP function reconfigured the host computer's MAC address, or because nomadic router **10** has the network link level in promiscuous mode which causes it to receive the packet even if addressed to a different MAC address.

Once the packet is passed to the network layer, shown in step **5**, the nomadic router translation function will modify the content of the packet to change the source address to match that of the nomadic router's address instead of the host computer's address. It will also translate other location dependent information such as the name of the local Domain Name Service (DNS) server. when translating the DNS packet, it will change the source address to that of the nomadic router's address and the destination address to that of a local DNS server.

Once the network layer translation is complete, the packet can be translated at the application and transport layers. The application layer is translated next, as shown in step **6**, because the transport layer required a pseudo-network layer header which includes the course and destination addresses and the content from the application layer.

At the application layer translation, any addresses which describe the source address of the host computer, such as with FTP, are translated to be that of the nomadic router's address. Any application layer destination addresses, such as a local proxy server, are translated to match that of the server running on the current network.

Once this application layer translation is complete, the transport layer, as shown in step **7**, can complete the checksum and any port number manipulation. The port number is manipulated if more than one host computer **12** is attached to nomadic router **10**. Each request sent by any one of the host computers **12** include a specific port that is translated to match an available inbound port on the nomadic router **10**.

The port number assigned for use with each host computer **12** is stored in a table in nomadic router **10** and is utilized with the reply packet to route the reply to the corresponding host computer as describer later. Finally, the outgoing packet is transmitted over network **14** in step **8**.

When a reply packet is transmitted over network **14**, as shown in step **9**, nomadic router **10** will receive the packet. In step **10**, nomadic router **10** will perform the reverse network layer translation to set the destination address to that of host computer **12** rather than the nomadic router's address, and any source address to the source address replaced by nomadic router **10** in step **5**.

Once network translation is complete, the packet is translated at the application layer, as shown in step **11**, to change the destination address to that of host computer **12** and the source address to the original destination address stored from step **6**. In step **12**, any port manipulation performed in step **7** is changed to the original setting and a new checksum is computed. Finally, as shown in step **13**, the packet is sent to host computer **12** which then processes the packet normally.

Options of the Nomadic Router

There are numerous options and applications of the nomadic router. These applications include, but are not limited to, Nomadic E-mail, Remote Network File Synchronization, Nomadic Database Synchronization, Instant Network Nomadic Routing, Nomadic Intranets, and Trade Show Data Exchange. Each of these are described in more detail below.

Nomadic E-Mail

The Nomadic E-mail application provides a synchronized yet distributed means for updates, reconciliation, and replicas to propagate through the internet. Nomadic routers are located on various networks of the internet and are equipped with nomadic E-mail support to provide synchronization, etc. Each nomadic router enabled for nomadic E-mail can utilize protocols such as IMAP to provide support for mobile users without the host device having to support it (similar to the POP3 protocol standard in internet E-mail clients).

Remote Network File Synchronizer

The Remote Network File Synchronization option of the nomadic router provides copies of user files that are stored/cached at various locations (e.g., hotel, office, home) on other nomadic routers equipped for remote network file synchronization. Copies of updated files are automatically synchronized and distributed among all peer locations. Local updates can be made while the host is disconnected from the nomadic router and from the network.

Nomadic Database Synchronizer

The Nomadic Database Synchronizer houses the user's (synchronized) master databases (e.g., contacts, addresses, phone numbers). The nomadic router of the database synchronizer does not need to be used on the network because it will interface directly with various host devices such as laptops, desktops, personal digital assistants, handheld personal computers, pagers, etc. via various standard ports.

Instant Network Nomadic Router

The objective of the instant network nomadic router is to enable rapid deployment of a communication network in any environment with little or no fixed infrastructure. The host and communication devices do not have to directly support the rapid deployment functionality.

The instant network nomadic router distributedly and intelligently establishes a wireless (or wired) communication link between the host device and the desired communication system while performing configuration, security, multihop routing, and network level data transmission over various communication devices. The nomadic router performs all the necessary network creating and processing automatically to remove configuration and system support from the host system or user. The instant network nomadic router utilizes proprietary and existing/emerging wireless communication systems, and multihop routing protocols.

Many communication infrastructures are varied and fragmented, which is likely to be exacerbated as more technologies are introduced. For example, high performance LANs, wireless services, cellular telephony, satellite, and ubiquitous paging networks, all provide varying degrees of coverage, cost, and bandwidth/delay characteristics.

Conditions may range from no connectivity at all because of lack of service, to partial and/or intermittent connectivity as devices are plugged and unplugged from a system. Likewise, damage to communications infrastructures (deliberately or by accident), lossy communication as a system moves through various service areas or difficult domains, and times when multiple network devices (communication substrates) can be used at the same time complicate connectivity. The instant network nomadic router will dynamically adapt the communication internetwork (dynamically creating one if necessary) to provide survivable communication in a mobile chaotic environment without the need for centralized control or fixed infrastructures.

The rapidly deployable nomadic router is a device associated with each user host device (e.g., PDA or laptop computer). It transparently provides the following capabilities for host computer systems using various wireless communication devices for physical and link layer access: dynamic wireless network creation; initialization into existing wireless networks; automatic configuration; network and subnetwork level data transmission; and multihop routing functionality.

The nomadic router can detect another device by polling the interface, providing an interrupt signal, or through specialized signaling. This in turn activates the nomadic router to provide translation for the device (if necessary) and establish a communication link to an appropriate corresponding interface and wireless subnetwork. The nomadic router operates at a level between the host device generating data and the physical communication transmission device as illustrated in FIG. **1**.

Nomadic Intranet

The Nomadic Intranet application provides all network and server type services for users to dynamically create an adhoc network. This is similar to the instant network nomadic router except the nomadic intranet is a single device with multiple ports into which laptop/devices can be plugged. The instant network nomadic router is distributed to each host device. The nomadic intranet not only provides adhoc networking but can also provide services such as temporary file storage, protocol conversion, act as a print server, and provide other services described as part of the Basic nomadic router.

Trade Show Nomadic Router

The Trade Show nomadic router applications not only provide the basic nomadic router functionality for an exhibitor's computer that is brought to the show, but also provides lead capture and/or information distribution. Lead capture can be provided by interfacing with a badge reader to read attendees' information. This information is then captured by the nomadic router and made available in the exhibitor's lead database.

The nomadic router can also provide a mechanism for distributing information to the attendees' personalized web pages or sent via e-mail directly across the internet. The exhibit's computer is able to control the information flow with the nomadic router by running software, such as a web browser, which talks with the service/control software stored in the nomadic router. The standard web browser can control display and capture of lead information, collection of qualification information, and selection of information to be distributed back to the attendee.

Fixed Nomadic Router

As briefly described above, the fixed nomadic router applications provide the same basic functionality and architecture

as the portable nomadic router with the nomadic router stored in one location. The fixed nomadic router acts as a surrogate or "Home Agent" for the user when he/she is away on travel. When the user wishes to register or utilize their host device elsewhere in the network, the portable nomadic router will register with the fixed nomadic router where it is temporarily attached to the network so information can be forwarded to the user's new location. The fixed nomadic router can also be used to house the master copy of the user's E-mail for the nomadic E-mail service, or files for the nomadic file synchronizer.

Mobile Virtual Private Network

The nomadic router provides the mapping between the location-based IP address used in the internet today and the permanent user-based address housed in the host CPU. This mapping is done without support or knowledge of such mapping by the host CPU or user. The Internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU, but rather are internal to the nomadic router.

By implementing this protocol as part of the translation function in the nomadic router, the nomadic router can encapsulate packets from the host computer and transmit them back to the fixed nomadic router which are sent out (un-encapsulated) on the native (home) network. Replies from the home network are received by the fixed nomadic router and are encapsulated and sent back to the nomadic router. When packets are transmitted between the nomadic router and fixed nomadic router, the packets are encrypted and sent using the Internet Tunneling Protocol.

Since the (mobile) nomadic router provides location independence and the fixed nomadic router forwards all packets from a corresponding host to the host computer via the nomadic router, any changes in the location, failure of a network link, or attachment point of the mobile host computer does not cause any open session to be lost. This session loss prevention is possible since the fixed nomadic router pretends to be the mobile host computer, and the nomadic router pretends to be the home network. The fixed nomadic router and nomadic router translation functions hide the link and network loss from the transport and application session.

While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention. It is understood that the present invention is broadly applicable to the field of electronic data communications using computers and other devices.

What is claimed is:

1. A method of establishing a communications path for a user host device through a foreign gateway, wherein the user host device is configured to communicate through a home gateway by using an IP address of the home gateway, and wherein the foreign gateway has an IP address different from the home gateway, the method comprising the steps of:

receiving at the foreign gateway an ARP request packet transmitted from the user host device over the communications path, wherein the ARP request packet includes at least a sender IP address that corresponds to an IP address of the user host device, a sender hardware address that correspond to a hardware address of the user host device, and a target IP address that corresponds to the IP address of the home gateway;

responding by the foreign gateway to the ARP request packet by transmitting over the communications path an ARP response packet that includes at least a sender IP address that corresponds to the IP address of the home gateway, a sender hardware address that corresponds to a hardware address of the foreign gateway, a target IP address that corresponds to the IP address of the user host device, and a target hardware address that corresponds to the hardware address of the user host device; and

receiving at the foreign gateway a network packet transmitted from the user host device, wherein the network packet comprises at least a target IP address that is different from the IP address of the home gateway and a target hardware address that corresponds to the hardware address of the foreign gateway.

2. The method of claim **1**, wherein the communications path is wireless.

3. The method of claim **1**, wherein the communications path is wired.

4. The method of claim **1**, wherein the hardware addresses are MAC addresses.

5. The method of claim **1**, wherein the ARP request target hardware address is a broadcast address.

6. The method of claim **1**, wherein the network packet further comprises at least a sender IP address that corresponds to the IP address of the user host device and a sender hardware address that corresponds to hardware address of the user host device.

7. The method of claim **6**, further comprising:

modifying the received network packet so that the sender IP address corresponds to an IP address of the foreign gateway; and

forwarding the modified network packet to the target IP address of the received network packet.

8. The method of claim **7**, wherein forwarding comprises transmitting the modified network packet to a router.

9. The method of claim **7**, wherein a node of the foreign gateway that forwards the modified packet is different from a node of the foreign gateway that receives the unmodified network packet.

10. The method of claim **7**, further comprising:

receiving at the foreign gateway a second network packet, wherein the second network packet comprises at least a sender IP address that corresponds to the target IP address of the first network packet and a target IP address that corresponds to the IP address of the foreign gateway.

11. The method of claim **10**, further comprising:

modifying the second network packet so that the target IP address corresponds to the IP address of the user host device.

12. The method of claim **11**, further comprising:

modifying the second network packet so that the target hardware address corresponds to the hardware address of the user host device.

13. The method of claim **12**, further comprising:

transmitting the second modified network packet to the IP address of the user host device.

14. The method of claim **6**, wherein the received network packet is a DNS packet, the method further comprising:

modifying the received network packet so that the sender IP address corresponds to an IP address of the foreign gateway and the target IP address corresponds to an IP address of a domain name server, wherein the IP address

of the domain name server is different than the target IP address of the received network packet; and

forwarding the modified network packet to the domain name server.

15. The method of claim **14**, further comprising:

receiving at the foreign gateway a second network packet, wherein the second network packet comprises at least a sender IP address that corresponds to the different IP address of the domain name server and a target IP address that corresponds to the IP address of the foreign gateway.

16. The method of claim **15**, further comprising:

modifying the second network packet so that the target IP address corresponds to the IP address of the user host device, the target hardware address corresponds to the hardware address of the user host device, and the sender IP address corresponds to the target IP address of the first network packet; and

transmitting the second modified network packet to the IP address of the user host device.

17. A method of establishing a communications path between a user host device and a foreign gateway, wherein the user host device is configured to communicate through a home gateway by using an IP address of the home gateway, and wherein the foreign gateway has an IP address different from the home gateway, the method comprising the steps of:

receiving an ARP request packet transmitted from the user host device over the communications path, wherein the ARP request packet includes at least a sender IP address that corresponds to an IP address of the user host device, a sender hardware address that correspond to a hardware address of the user host device, a target IP address that corresponds to the IP address of the home gateway;

responding to the ARP request packet by transmitting over the communications path an ARP response packet that includes at least a sender IP address that corresponds to the IP address of the home gateway, a sender hardware address that corresponds to a hardware address of the foreign gateway, a target IP address that corresponds to the IP address of the user host device, and a target hardware address that corresponds to the hardware address of the user host device; and

receiving at the foreign gateway a network packet transmitted from the user host device, wherein the network packet comprises at least a target IP address that corresponds to the IP address of the home gateway and a target hardware address that corresponds to the hardware address of the foreign gateway.

18. The method of claim **17**, wherein the network packet is a DNS packet.

19. The method of claim **18**, further comprising:

modifying the received network packet so that the sender IP address corresponds to an IP address of the foreign gateway and the target IP address corresponds to an IP address of a domain name server, wherein the IP address of the domain name server is different than the target IP address of the received network packet; and

forwarding the modified network packet to the domain name server.

20. The method of claim **19**, further comprising:

receiving at the foreign gateway a second network packet, wherein the second network packet comprises at least a sender IP address that corresponds to the different IP address of the domain name server and a target IP address that corresponds to the IP address of the foreign gateway.

21. The method of claim **20**, further comprising:

modifying the second network packet so that the target IP address corresponds to the IP address of the user host device and the sender IP address corresponds to the IP address of the home gateway.

22. The method of claim **21**, further comprising:

modifying the second network packet so that the target hardware address corresponds to the hardware address of the user host device.

23. The method of claim **22**, further comprising:

transmitting the second modified network packet to the IP address of the user host device.

24. A system that establishes a communications path for a user host device through a foreign gateway, wherein the user host device is configured to communicate through a home gateway by using an IP address of the home gateway, and wherein the foreign gateway has an IP address different from the home gateway, the system comprising:

a foreign gateway configured to receive communications from the user host device, such that the foreign gateway receives an ARP request packet transmitted from the user host device over the communications path, wherein the ARP request packet includes at least a sender IP address that corresponds to an IP address of the user host device, a sender hardware address that correspond to a hardware address of the user host device, and a target IP address that corresponds to the IP address of the home gateway;

the foreign gateway further configured to respond to the ARP request packet by transmitting over the communications path an ARP response packet that includes at least a sender IP address that corresponds to the IP address of the home gateway, a sender hardware address that corresponds to a hardware address of the foreign gateway, a target IP address that corresponds to the IP address of the user host device, and a target hardware address that corresponds to the hardware address of the user host device; and

the foreign gateway further configured to receive a network packet transmitted from the user host device, wherein the network packet comprises at least a target IP address that is different from the IP address of the home gateway and a target hardware address that corresponds to the hardware address of the foreign gateway.

25. The system of claim **24**, wherein the communications path is wireless.

26. The method of claim **24**, wherein the communications path is wired.

27. The system of claim **24**, wherein the hardware addresses are MAC addresses.

28. The system of claim **24**, wherein the ARP request target hardware address is a broadcast address.

29. The system of claim **24**, wherein the network packet further comprises at least a sender IP address that corresponds to the IP address of the user host device and a sender hardware address that corresponds to hardware address of the user host device.

30. The system of claim **29**, further comprising:

a modification module configured to modify the received network packet so that the sender IP address corresponds to an IP address of the foreign gateway; and

the foreign gateway further configured to forward the modified network packet to the target IP address of the received network packet.

31. The system of claim 30, wherein the modification module transmits the modified network packet to a router.

32. The system of claim 30, wherein a node of the foreign gateway that forwards the modified packet is different from a node of the foreign gateway that receives the unmodified network packet.

33. The system of claim 30, wherein the foreign gateway is further configured to receive a second network packet, wherein the second network packet comprises at least a sender IP address that corresponds to the target IP address of the first network packet and a target IP address that corresponds to the IP address of the foreign gateway.

34. The system of claim 33, wherein the modification module is further configured to modify the second network packet so that the target IP address corresponds to the IP address of the user host device.

35. The system of claim 34, wherein the modification module is further configured to modify the second network packet so that the target hardware address corresponds to the hardware address of the user host device.

36. The system of claim 35, wherein the foreign gateway further configured to transmit the second modified network packet to the IP address of the user host device.

37. The system of claim 29, wherein the received network packet is a DNS packet, the system further comprising:

a modification module configured to modify the received network packet so that the sender IP address corresponds to an IP address of the foreign gateway and the target IP address corresponds to an IP address of a domain name server, wherein the IP address of the domain name server is different than the target IP address of the received network packet; and

the foreign gateway further configured to forward the modified network packet to the domain name server.

38. The system of claim 37, wherein the foreign gateway is further configured to receive a second data packet, wherein the second network packet comprises at least a sender IP address that corresponds to the different IP address of the domain name server and a target IP address that corresponds to the IP address of the foreign gateway.

39. The system of claim 38, wherein the modification module is further configured to modify the second network packet so that the target IP address corresponds to the IP address of the user host device, the target hardware address corresponds to the hardware address of the user host device, and the sender IP address corresponds to the target IP address of the first network packet; the foreign gateway further configured to transmit the second modified network packet to the IP address of the user host device.

40. A system that establishes a communications path between a user host device and a foreign gateway, wherein the user host device is configured to communicate through a home gateway by using an IP address of the home gateway, and wherein the foreign gateway has an IP address different from the home gateway, the system comprising:

a foreign gateway configured to receive communications from the user host device, such that the foreign gateway receives an ARP request packet transmitted from the user host device over the communications path, wherein the ARP request packet includes at least a sender IP address that corresponds to an IP address of the user host device, a sender hardware address that correspond to a hardware address of the user host device, and a target IP address that corresponds to the IP address of the home gateway;

the foreign gateway further configured to respond to the ARP request packet by transmitting over the communications path an ARP response packet that includes at least a sender IP address that corresponds to the IP address of the home gateway, a sender hardware address that corresponds to a hardware address of the foreign gateway, a target IP address that corresponds to the IP address of the user host device, and a target hardware address that corresponds to the hardware address of the user host device; and

the foreign gateway further configured to receive a network packet transmitted from the user host device, wherein the network packet comprises at least a target IP address that corresponds to the IP address of the home gateway and a target hardware address that corresponds to the hardware address of the foreign gateway.

41. The system of claim 40, wherein the network packet is a DNS packet.

42. The system of claim 41, further comprising:

a modification module configured to modify the received network packet so that the sender IP address corresponds to an IP address of the foreign gateway and the target IP address corresponds to an IP address of a domain name server, wherein the IP address of the domain name server is different than the target IP address of the received network packet; and

the foreign gateway further configured to forward the modified network packet to the domain name server.

43. The system of claim 42, wherein the foreign gateway is further configured to receive a second network packet, wherein the second network packet comprises at least a sender IP address that corresponds to the different IP address of the domain name server and a target IP address that corresponds to the IP address of the foreign gateway.

44. The system of claim 43, wherein the modification module is further configured to modify the second network packet so that the target IP address corresponds to the IP address of the user host device and the sender IP address corresponds to the IP address of the home gateway.

45. The system of claim 44, wherein the modification module is further configured to modify the second network packet so that the target hardware address corresponds to the hardware address of the user host device.

46. The system of claim 45, wherein the foreign gateway is further configured to transmit the second modified network packet to the IP address of the user host device.

47. A network device comprising:

a memory;

a broadcast handling function in the memory;

a processor executing the broadcast handling function;

a network interface configured to receive a resolution packet transmitted by a first device, the resolution packet including a sender IP address that corresponds to an IP address of the first device, a sender hardware address that corresponds to a hardware address of the first device, and a target IP address that corresponds to an IP address of a second device, the broadcast handling function adapted to responsively create a reply packet including a sender IP address that corresponds to an IP address of the second device, a sender hardware address that corresponds to a hardware address of the network device, a target IP address that corresponds to the IP address of the first device, and a target hardware address that corresponds to the hardware address of the first device, the broadcast handling function initiating transmission of the reply packet via the network interface; and

the network interface further configured to receive a network packet transmitted by the first device, the network

packet including a target IP address that is different from the IP address of the second device and a target hardware address that corresponds to the hardware address of the network device.

48. The network device of claim **47** wherein the communications link is a wireless communications link.

49. The network device of claim **47** wherein the hardware addresses are MAC addresses.

50. The network device of claim **47** wherein the network packet further includes a sender IP address that corresponds to the IP address of the first device and a hardware address that corresponds to the hardware address of the first device.

51. The network device of claim **47**, further comprising:

a translation function in the memory, the processor executing the translation function, the translation function adapted to create a modified network packet that includes a sender IP address that corresponds to the IP address of the network device, the translation function initiating transmission of the modified network packet via the network interface.

52. A network device comprising:

a memory;

a broadcast handling function in the memory;

a processor executing the broadcast handling function;

a network interface configured to receive a resolution packet transmitted by a first device, the resolution packet including a sender IP address that corresponds to an IP address of the first device, a sender hardware address that corresponds to a hardware address of the first device, and a target IP address that corresponds to an IP address of a second device, the broadcast handling function adapted to responsively create a reply packet including a sender IP address that corresponds to an IP address of the second device, a sender hardware address that corresponds to a hardware address of the network device, a target IP address that corresponds to the IP address of the first device, and a target hardware address that corresponds to the hardware address of the first device, the broadcast handling function initiating transmission of the reply packet via the network interface; and

the network interface further configured to receive a first network packet transmitted by the first device, the first network packet including a target IP address that corresponds to the IP address of the second device and a target hardware address that corresponds to the hardware address of the network device.

53. The network device of claim **52** wherein the communications link is a wireless communications link.

54. The network device of claim **52** wherein the first network packet is a DNS packet.

55. The network device of claim **52**, further comprising:

a translation function in the memory, the processor executing the translation function, the translation function adapted to create a second network packet that includes a sender IP address that corresponds to the IP address of the network device, the translation function initiating transmission of the second network packet via the network interface to a third device having an IP address different from the target IP address of the first network packet.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,554,995 B2
APPLICATION NO. : 11/097925
DATED : June 30, 2009
INVENTOR(S) : Joel E. Short et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 17, Line 67, Claim 1:

Delete "correspond" and
Insert -- corresponds --.

Column 18, Line 30, Claim 6:

After "corresponds to" and
Insert -- the --.

Column 20, Line 26, Claim 24:

Delete "correspond" and
Insert -- corresponds --.

Column 21, Line 21, Claim 36:

After "foreign gateway"
Insert -- is --.

Signed and Sealed this

Third Day of November, 2009

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

US006636894B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 6,636,894 B1**
(45) **Date of Patent: Oct. 21, 2003**

(54) **SYSTEMS AND METHODS FOR REDIRECTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE HAVING REDIRECTION CAPABILITY**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Frederic Delley**, Redwood City, CA (US); **Mark F. Logan**, Santa Monica, CA (US); **Florence C. I. Pagan**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/458,569**

(22) Filed: **Dec. 8, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/111,497, filed on Dec. 8, 1998.

(51) **Int. Cl.**[7] **G06F 15/173**

(52) **U.S. Cl.** **709/225**; 709/249

(58) **Field of Search** 709/225, 226, 709/227, 229, 249; 707/1; 713/200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,696,898	A *	12/1997	Baker et al.	713/201
5,761,683	A	6/1998	Logan et al.	
5,845,070	A *	12/1998	Ikudome	713/201
5,968,176	A	10/1999	Nessett et al.	
5,991,292	A *	11/1999	Focsaneanu et al.	370/352
6,219,694	B1 *	4/2001	Lazaridis et al.	709/206
6,317,790	B1 *	11/2001	Bowker et al.	709/225
6,317,837	B1 *	11/2001	Kenworthy	713/200
6,393,468	B1 *	5/2002	McGee	709/218
6,490,620	B1 *	12/2002	Ditmer et al.	709/224

FOREIGN PATENT DOCUMENTS

EP	0848338 A1	6/1998

(List continued on next page.)

OTHER PUBLICATIONS

Cisco; *Single–User Network Access Security TACACS+*; Mar. 30, 1995; 9 pages; *Cisco White Paper*; XP002124521.
D. Brent Chapman, Elizabeth D. Zwicky; *Building Internet Firewalls*, Nov. 1995; pp. 131–188; O'Reilly; XP002202789.

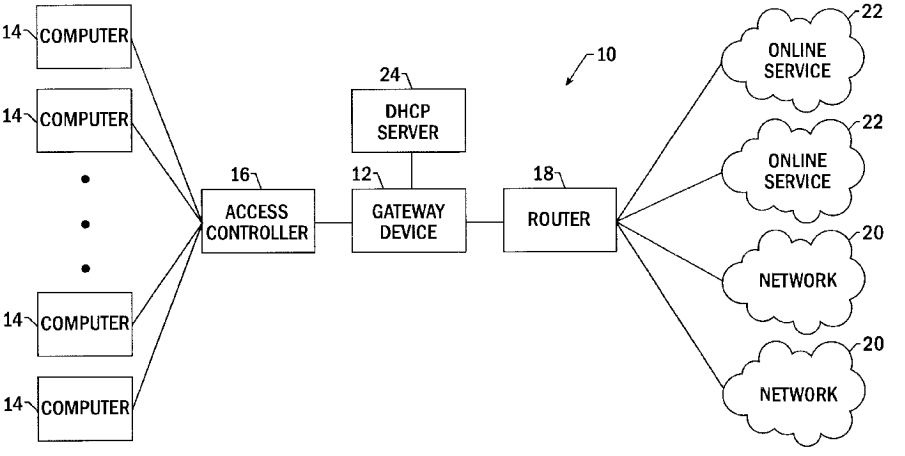
(List continued on next page.)

Primary Examiner—Mehmet B. Geckil
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

Systems and methods for dynamically creating new users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, a user profile database comprising stored access information and in communication with the gateway device, and an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database. The AAA server determines if user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network. The systems and methods of the present invention can also redirect users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings.

11 Claims, 1 Drawing Sheet



FOREIGN PATENT DOCUMENTS

EP	0889418 A2	1/1999
EP	0 909 073 A2	4/1999
EP	0986230 A2	3/2000
WO	WO 96/39668	12/1996
WO	WO 98/12643	3/1998
WO	WO 99/57865	11/1999
WO	WO 99/57866	11/1999
WO	WO 99/66400	12/1999

OTHER PUBLICATIONS

Susan Hinrichs; *Policy–Based Management Bridiging the Gap*; Dec. 6, 1999; pp. 209–218; Computer Security Applications Conference, 1999 (ACSAC 1999), Proceedings, 15th Annual Phoenix, Arizona, USA Dec. 6–10, 1999, Los Alamitos, California, IEEE Comput. Soc.; XP010368586.

* cited by examiner

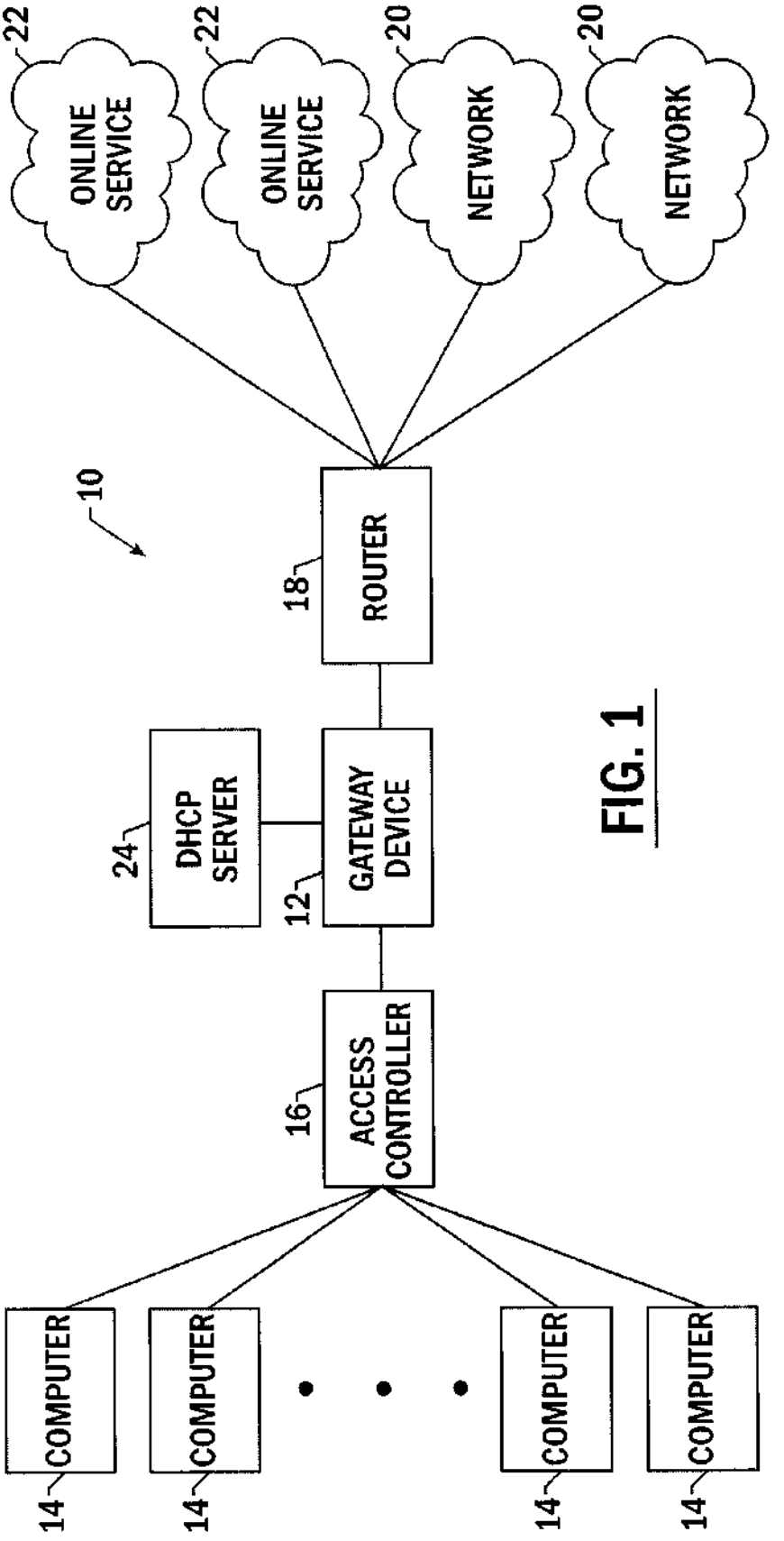

22
ONLINE SERVICE
22
ONLINE SERVICE
20
NETWORK
20
NETWORK
10
18
ROUTER
24
DHCP SERVER
12
GATEWAY DEVICE
16
ACCESS CONTROLLER
14
COMPUTER
14
COMPUTER
14
COMPUTER
14
COMPUTER

FIG. 1

SYSTEMS AND METHODS FOR REDIRECTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE HAVING REDIRECTION CAPABILITY

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claim priority from U.S. Provisional Patent Application Ser. No. 60/111,497, filed Dec. 8, 1988 the contents of which are incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to a gateway device and, more particularly, to a universal network gateway for redirecting to a portal page a computer transparently accessing a service provider network.

BACKGROUND OF THE INVENTION

In order for a computer to function properly in a network environment, the computer must be appropriately configured. Among other things, this configuration process establishes the protocol and other parameters by which the computer transmits and receives data. In one common example, a plurality of computers are networked to create a local area network (LAN). In the LAN, each computer must be appropriately configured in order to exchange data over the network. Since most networks are customized to meet a unique set of requirements, computers that are part of different networks are generally configured in different manners in order to appropriately communicate with their respective networks.

While desktop computers generally remain a part of the same network for a substantial period of time, laptops, handhelds, personal digital assistants (PDAs), cellphones or other portable computers (collectively "portable computers") are specifically designed to be transportable. As such, portable computers are connected to different networks at different times depending upon the location of the computer. In a common example in which the portable computer serves as an employee's desktop computer, the portable computer is configured to communicate with their employer's network, i.e., the enterprise network. When the employee travels, however, the portable computer may be connected to different networks that communicate in different manners. In this regard, the employee may connect the portable computer to the network maintained by an airport, a hotel, a cellular telephone network operator or any other locale in order to access the enterprise network, the Internet or some other on-line service. The portable computer is also commonly brought to the employee's residence where it is used to access various networks, such as, the enterprise network, a home network, the Internet and the like. Since these other networks are configured somewhat differently, however, the portable computer must also be reconfigured in order to properly communicate with these other networks. Typically, this configuration is performed by the user each time the portable computer is connected to a different network. As will be apparent, this repeated reconfiguration of the portable computer is not only quite time consuming, but is also prone to errors. The reconfiguration procedure may even be beyond the capabilities of many users or in violation of their employer's IT policy. Importantly, special software must also typically be loaded onto the user's computer to support reconfiguration.

As described by U.S. patent application Ser. No. 08/816,174 and U.S. Provisional Patent Application Nos. 60/111,497, 60/160,973, 60/161,189, 60/161,139, 60/160,890 and 60/161,182, a universal subscriber gateway device has been developed by Nomadix, Inc. of Westlake Village, Calif. The contents of these applications are incorporated herein by reference. The gateway device serves as an interface connecting the user to a number of networks or other online services. For example, the gateway device can serve as a gateway to the Internet, the enterprise network, or other networks and/or on-line services. In addition to serving as a gateway, the gateway device automatically adapts to a computer, in order that it may communicate with the new network in a manner that is transparent both to the user and the new network. Once the gateway device has appropriately adapted to the user's computer, the computer can appropriately communicate via the new network, such as the network at a hotel, at home, at an airport, or any other location, in order to access other networks, such as the enterprise network, or other online services, such as the Internet.

The portable computer user, and more specifically the remote or laptop user, benefits from being able to access a myriad of computer networks without having to undergo the time-consuming and all-too-often daunting task of reconfiguring their host computer in accordance with network specific configurations. In addition, no additional software need be loaded onto the computer prior to connection to the other network. From another perspective, the network service provider benefits from avoiding "on-site" visits and/or technical support calls from the user who is unable to properly re-configure the portable computer. In this fashion, the gateway device is capable of providing more efficient network access and network maintenance to the user and the network operator.

Gateway devices are typically used to provide network access to the remote portable computer user, such as users in hotels, airports and other location where the remote portable computer user may reside. Additionally, gateway devices have found wide-spread use in multi-resident dwellings as a means of providing the residents an intranet that networks the residents, broadband Internet access and the capability to adapt to the variances of the resident's individual enterprise network needs. With the advent of even smaller portable computing devices, such as handhelds, PDAs, and the like, the locations where these users may reside become almost limitless.

Through gateway devices Internet Service Providers (ISPs) or enterprise network (such as a LAN established by an entity such as a hotel) providers can permit a wide variety of users simple and transparent access to their networks and to other online services. To take advantage of transparent user access to their computer networks and online services enterprise networks or ISPs should be able to redirect users to portal pages that the enterprise or internet service providers wish the user to access or view. For instance, where users are located at an airport, the enterprise network administrator may wish to direct users to a portal page containing arrival and departure information, or to a portal page having the user's itinerary thereon to provide the user an incentive to access the network. ISPs, for example, may wish users to access the ISPs portal page for up to the date news and weather, information regarding the user's Internet service, and paid advertisements.

Homepage redirection has been accomplished in the prior art. For example, America Online (AOL) users, upon accessing the internet, are directed to an AOL homepage from which the users can select a variety of AOL services, and which includes advertising from various companies. Typically, direction of users to such a page benefits the ISP

because advertisers pay money to the ISP each time a user accesses the Internet, as subscribers are a captive audience to advertising. Advertisers pay for such advertising not only because of the captive audience, but because advertisers can tailor advertisements based upon the typical audience accessing the internet. Furthermore, AOL may market its services through its homepage, and its homepage may be attractive to potential subscribers. Directing users to a particular. page may serve an additional function. Users may be directed to a particular page, such as a login page, so that the user may enter login information to be authenticated and authorized access on the network. Furthermore, users may wish to establish their own specialized portal page, such as a page including favorite links, a page linking the user to the user's business, or a page including any other items relevant to the user.

However, such redirection of users to homepages has been traditionally based upon software installed on a user's computer and/or configurations of user computers in communication with a home network. For example, where a user's computer is appropriately configured for access to a home network, the user's computer can be configured to access a particular homepage on that network. This can be the case, for example, in businesses where users computers are configured to access an intranet homepage or an internet page specific to that company and located on the internet.

Therefore, a method and system would be desirable which enables a user transparent access to a computer network employing a gateway device where the computer network can provide access to users and direct the users to portal pages established by the user, network administrator or another entity, where the direction is preferably based upon attributes associated with a user, such as the user's location, identity, computer, or a combination thereof. Furthermore, such redirection should be able to redirect users to a login page when the user does not otherwise have access to online services or networks so that the user may login to be authenticated and authorized access on the network.

SUMMARY OF THE INVENTION

The present invention comprises a method and system for redirecting users to a portal page where users have transparent access to a computer network utilizing a gateway device. The method and system advantageously operates in a manner transparent to the user since the user need not reconfigure their computer and no additional software need be added to the computer for reconfiguration purposes.

According to the invention, users accessing the gateway device are redirected to a portal page. Where stored user profiles permit the users access to the destination network, the users can be forwarded to the destination network or a portal page established by the network, user, or another entity. Otherwise, users are directed to a login page in which the users must input user information so that the users can obtain access to networks and online services. The redirection function according to the present invention can be utilized to direct new or existing users to customized homepages established by the gateway device or individual users.

A method for dynamically creating new users having transparent computer access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The method includes receiving at a gateway device a request from a user for access to a destination network, determining if the user is entitled access to the destination network based upon a user profile corresponding to the user and stored within a user profile database in communication with the gateway device, and redirecting the user to a login page when the user profile does not include rights to access the destination network. Furthermore, the method of the present invention can include the step of forwarding the user to the destination network when the user profile includes rights to access the destination network. The method can also include the step of automatically redirecting the user to a portal page following receipt of a request for access to the destination network prior to determining if the user is entitled access to the destination network

According to one aspect of the invention, the method can include the step of establishing a login page on a webserver local to the gateway device prior to redirecting the user to the login page. The method can also include accepting user information at the login page which is thereafter utilized by the gateway device to authorize the user access to the destination network. The user profile database can be updated with the user information.

According to another aspect of the invention, the user may be forwarded from the login page and returned to a portal page or directed to a destination address which can be an Internet destination address. Redirecting the user to a login page can include redirecting a browser located on the user's computer to the login page. Furthermore, redirecting the browser located on the user's computer can include receiving a Hyper-Text Transfer Protocol (HTTP) request for the destination address and responding with an HTTP response corresponding to the login page.

According to another embodiment of the invention, a system for dynamically creating new users having transparent computer access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, and a user profile database comprising stored access information and in communication with the gateway device. The system further includes an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database, where the AAA server determines if a user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network. The system can also direct the user to a portal page upon the user's access to the network, prior to determining the access rights of the user.

According to one aspect of the invention, the login page is maintained local to the gateway device. The user profile database and AAA server can also be located within the gateway device. Furthermore, the user profile database can be located within the AAA server.

According to another embodiment of the invention, the user profile database includes a plurality of user profiles, wherein each respective user profile of the plurality of user profiles contains access information. In addition, each respective user profile may contain historical data relating to the duration of destination network access for use in determining the charges due for the destination network access.

According to another embodiment of the invention, a method for redirecting users having transparent computer

access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The method includes receiving at a gateway device a request from a user for access to a destination address, such as an Internet address, and redirecting the user to a portal page, wherein the user computer remains configured for accessing the home network, and wherein no additional configuration software need be installed on the user's computer. Furthermore, redirecting the user to a portal page can comprise redirecting the user to a portal page created by an administrator associated with the portal page, or redirecting the user to a portal page customized by the user.

According to another embodiment of the invention, a system for redirecting users having transparent computer access to a destination network is disclosed, where the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, and an AAA server in communication with the gateway device, where the AAA server intercepts the request from the user for access to the destination network and redirects the user to a portal page, wherein the user's computer remains configured for accessing the home network, and wherein no additional configuration software need be installed on the user's computer. According to one aspect of the invention, the AAA server is located entirely within the gateway device. The portal page of the system can also be maintained on a server local to the gateway device.

A unique advantage of the transparent redirection of users to a portal page, and, in certain circumstances from the portal page, to a login page where users subscribe for network access is that a user can obtain access to networks or online services without installing any software onto the user's computer. On the contrary, the entire process is completely transparent to the user. As such, the method and apparatus of the present invention facilitates transparent access to destination networks without requiring a user to reconfigure the home network settings resident on the user computer and without having to install reconfiguration software.

The method and system of the various embodiments facilitate transparent access to a destination network. According to one embodiment, the method and system facilitate the addition of new subscribers to the network. According to another embodiment, all users can be redirected to a portal page, which can include advertising, without requiring reconfiguration of the users' computers, or new software to be added on the users' computers.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system that includes a gateway device for automatically configuring one or more computers to communicate via the gateway device with other networks or other online services, according to one embodiment of the present invention.

DETAILED DESCRIPTION OF ONE EMBODIMENT OF THE INVENTION

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, a computer system **10** including a gateway device **12** is depicted in block diagram form. The computer system **10** typically includes a plurality of computers **14** that access a computer network in order to gain access to networks **20** or other online services **22**. For example, the computers **14** can be plugged into ports that are located in different rooms of a hotel, business, or a multi-dwelling unit. Alternatively, the computers **14** can be plugged into ports in an airport, an arena, or the like. The gateway device **12** provides an interface between the plurality of computers **14** and the various networks **20** or other online services **22**. One embodiment of a gateway device has been described by the aforementioned U.S. patent application Ser. No. 08/816,174.

Most commonly, the gateway device **12** is located near the computers **14** at a relatively low position in the overall network (i.e., the gateway device **12** will be located within the hotel, multi-unit residence, airport, etc.). However, the gateway device **12** can be located at a higher position in the system by being located closer to the various networks **20** or other online services **22**, if so desired. For example, the gateway device **12** could be located at a network operating center or could be located before or after a router **18** in the computer network. Although the gateway device **12** can be physically embodied in many different fashions, the gateway device **12** typically includes a controller and a memory device in which software is stored that defines the operational characteristics of the gateway device **12**. Alternatively, the gateway device **12** can be embedded within another network device, such as an access concentrator **16** or a router **18**. Moreover, the software that defines the functioning of the gateway device **12** can be stored on a PCMCIA card that can be inserted into a computer of the plurality of computers **14** in order to automatically reconfigure the computer to communicate with a different computer system, such as the networks **20** and online services **22**.

The computer system **10** typically includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a cable modem termination shelf (CMTS), a switch or the like. As also shown in FIG. **1**, the computer system **10** typically includes one or more routers **18** and/or servers (not shown in FIG. **1**) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately traffic to and from the various networks **20** or online services **22**. In

this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of other networks or other online service providers, such as internet service providers, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. **1** may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**.

The gateway device **12** of the present invention is specifically designed to adapt to the configuration of each of the computers **14** that log onto the computer system **10** in a manner that is transparent to the user and the computer networks **20** or online services **22**. In the embodiment shown in FIG. **1**, the computer system **10** employs dynamic host configuration protocol (DHCP) service, which is a protocol well known to those of skill in the art and currently implemented in many computer networks. In DHCP networks an IP address is assigned to an individual computer of the plurality of computers **14** when the computer logs onto the computer network through communication with the gateway device **12**. The DHCP service can be provided by an external DHCP server **24** or it can be provided by an internal DHCP server located within the gateway device.

In order to allow a user of the computer to communicate transparently with computer networks **20** or online services **22**, the gateway device must be able to communicate with the user computer, as well as the various online services **22** or networks **20**. In order to support this communication, the gateway device **12** generally performs a packet translation function that is transparent to both the user and the network. In this regard, for outbound traffic from a computer to a network or on-line service, the gateway device **12** changes attributes within the packet coming from the user, such as the source address, checksum, and application specific parameters, to meet the criteria of the network to which the user has accessed. In addition, the outgoing packet includes an attribute that will direct all incoming packets from the accessed network to be routed through the gateway device. In contrast, the inbound traffic from the computer network or other online service that is routed through the gateway device undergoes a translation function at the gateway device so that the packets are properly formatted for the user's host computer. In this manner, the packet translation process that takes place at the gateway device **12** is transparent to the host, which appears to send and receive data directly from the accessed computer network. By implementing the gateway device as an interface between the user and the computer network or other online service, however, the user will eliminate the need to re-configure their computer **12** upon accessing subsequent networks as well as the need to load special configuration software on their computer to support the reconfiguration.

Communication between users and networks or online services may be effectuated through ports, for example, located within hotel rooms or multi-dwelling units, or through conventional dial-up communications, such as through the use of telephone or cable modems. According to one aspect of the invention, users can be are redirected to a portal page, as described below. After being redirected to the portal page, the user is subjected to a AAA process. Based upon the AAA process, the user may be permitted transparent access to the destination network or may be redirected to a login page in order to gather additional information to identify the user.

Identifying the user is crucial in authorizing access to networks or online services, as such services are typically provided for a fee and may be customized based upon the user, user's location, or user's computer. As discussed below, the user's identification may be used to direct the user to a specific portal page, which can be a particular webpage. As such, the system of the present invention includes means for identifying a user based upon an attribute associated with the user that is contained within the packet transmitted from the user's computer. Attributes can include any data well known in the art for identifying the user, the user's location, and/or the user's computer. In general, identifying a user's computer that accesses a network can be done by a media access control (MAC) associated with the computer. Identifying a computer based upon a MAC address is well known to those of skill in the art, and will not be discussed in detail herein. Additionally, the attribute can be based upon a user name, ID, or according to one advantageous embodiment described below, a particular location, such as from a communications port in a hotel room. As such, the location of the user can be the identifiable attribute.

According to one embodiment of the present invention, after a user accesses the computer network using a computer in communication with the gateway device **12**, as described above, the user is directed to a portal page. The portal page may be maintained by an ISP or an enterprise network, or by any entry maintaining a webpage on the Internet. According to one aspect of the invention, the portal page can be a webpage containing any information whatsoever, and can be created by the ISP, enterprise network administrator or user. The portal page can contain information specific to the user accessing the network, as discussed in detail below.

Regardless of whether a user accessing the computer network is authorized access to the network, the user is redirected to a portal page. After being redirected to a portal page, the gateway device of the present invention determines the authorization and access rights of the user based upon an Authentication, Authorization and Accounting method, as described in U.S. patent application Ser. No. 09/458602 entitled "Systems And Methods For Authorizing, Authenticating And Accounting Users Having Transparent Computer Access To A Network Using A Gateway Device" filed concurrently with this application and incorporated by reference.

According to one aspect of the invention, a user may be identified and authorized access to the network or online services based upon attributes associated with the user, such as the user's location or the user's computer. When this occurs, the user can be forwarded to a portal page unique to that user. As described below, and in the U.S. patent application incorporated by reference immediately above, the user may be identified without being queried to input any identification information so that upon accessing the computer network the user is automatically directed to a generic portal page or a portal page established specifically for and unique to that user. According to another aspect of the invention, a user may be identified and authorized access based upon the user's identity after being redirected to the portal page. The user may have to enter a login name and password while at the portal page or after being directed to a login page so that the ISP or other entity maintaining the gateway device can identify the user. After entering identifying data, the user may be directed to a particular portal page, as in the first aspect described above. According to a third aspect of the invention, the user is not authorized access to the network. Where this occurs the user will be directed from the portal page to a login page where the user will have to input identification information, such as the user's name, address, credit card number, and other relevant

data so that the user may be authorized to access the network. After the user enters sufficient login data to establish authorization, the user may be redirected to a portal page.

The redirection is accomplished by a Home Page Redirect (HPR) performed by the gateway device, a AAA server, or by a portal page redirect unit located internal to or external to the gateway device. To accomplish the redirection of a user to a portal page, HPR utilizes a Stack Address Translation (SAT) operation to direct the user to the portal page, which is preferably local to the gateway device so that the redirection will be efficient and fast. This is accomplished by redirecting the user to a protocol stack using network and port address translation to the portal server that can be internal to the computer network or gateway device. More specifically, the gateway device, AAA server or portal page redirect unit receives the user's HTTP request for a web page and sends back the HTTP response reversing the network and port address translation the portal server, essentially acting as a transparent 'go-between' to the user and portal server. It will be appreciated, however, that to receive the HTTP request the gateway device, AAA server or portal page redirect unit must initially open a Transmission Control Protocol (TCP) connection to a server in line with the user-requested internet address.

According to one aspect of the present invention, when a user initially attempts to access a destination location, the gateway device, AAA server or portal page redirect unit receives this request and routes the traffic to a protocol stack on a temporary server, which can be local to the gateway device. This can occur where a user initially opens a web browser resident on the user's computer and attempts to access a destination address, such as an Internet site. The destination address can also include any address accessible via the network or an online service, and can include the portal page. The protocol stack can pretend to be the user-entered destination location long enough to complete a connection or 'handshake'. Thereafter, this protocol stack directs the user to the portal server, which can be local to the gateway device to facilitate higher speed communication. The redirection to the portal server can be accomplished by redirecting web pages only, rather than all traffic, including E-mails, FTPs, or any other traffic. Therefore, once authorized, if a user does not attempt to access a webpage through the user's internet browser, the gateway device can forward the communication transparently to the user's requested destination without requiring the user to access the portal page. Furthermore, according to one aspect of the invention specific user-input destination addresses may be authorized to pass through the gateway device without being redirected.

The portal page can also be specialized based on the user, user's location, user's computer, or any combination thereof For example, assuming that the user has been authenticated and has authorization, the gateway device can present users with a portal page that identifies, among other things, the online services or other computer networks that are accessible via the gateway device. In addition, the portal page presented by the gateway device can provide information regarding the current parameters or settings that will govern the access provided to the particular user. As such, the gateway administrator can readily alter the parameters or other settings in order to tailor the service according to their particular application. Typically, changes in the parameters or other settings that will potentially utilize additional resources of the computer system will come at a cost, such that the gateway administrator will charge the user a higher rate for their service. For example, a user may elect to increase the transfer rate at which signals are transmitted across the computer network and pay a correspondingly higher price for the expedited service.

The portal page may include advertising tailored to the specific needs of the user. The gateway device would be capable of tailoring the material based upon user profiles in the network. The portal page may also incorporate surveys or links to surveys to provide the network provider with beneficial statistical data. As an ancillary benefit, the user who responds to the surveys may be rewarded with network access credit or upgraded quality. Additionally, the service provided could offer additional services to the user by way of the portal page or links to these services may be offered on the portal page. These services offered by the network service provider are not limited to the services related to the network connection. For example, a hotel may desire to offer the user in-room food service or a multi-unit dwelling may want to offer house cleaning service.

The portal page may also comprise information related to the status of the current network session. By way of example this information may include, current billing structure data, the category/level of service that the user has chosen, the bandwidth being provided to the user, the bytes of information currently sent or received, the current status of network connection(s) and the duration of the existing network connection(s). It is to be understood, by those skilled in the art to which this invention relates that all conceivable useful information relating to the current network session could be displayed to the user in a multitude of combinations as defined by the user and/or the gateway administrator. The gateway administrator will have the capability to dynamically change the information supplied in the portal page based on many factors, including the location of the user, the profile of the user and the chosen billing scheme and service level. The information provided in the portal page may prompt the user to adjust any number of specific parameters, such as the billing scheme, the routing, the level of service and/or other user-related parameters.

The portal page may be implemented with an object-oriented programming language such as Java developed by Sun Microsystems, Incorporated of Mountain View, Calif. The code that defines the portal page can be embodied within the gateway device, while the display monitor and the driver are located with the host computers that are in communication with the gateway device. The object oriented programming language that is used should be capable of creating executable content (i.e. self-running applications) that can be easily distributed through networking environments. The object oriented programming language should be capable of creating special programs, typically referred to as applets that can be incorporated in portal pages to make them interactive. In this invention the applets take the form of the portal pages. It should be noted that the chosen object-oriented programming language would require that a compatible web browser be implemented to interpret and run the portal page. It is also possible to implement the portal page using other programming languages, such as HTML, SGML and XML; however, these languages may not be able to provide all the dynamic capabilities that languages, such as Java provide.

By re-directing the user to the portal page the gateway administrator or network operator is provided the opportunity to present the user with updated information pertaining to the remote location (i.e. the hotel, the airport etc.). By way of example the portal page may provide for links to the corporate home page, a travel site on the Internet, an Internet

search engine and a network provider home page. Additionally, the buttons or any other field within the portal page may include other types of information options, such as advertising fields or user-specific links or fields based upon data found in the user's profile or inputted by the user.

It will be appreciated that the portal page is not limited to supplying information related to the user's billing and service plans. It is also possible to configure the portal page to include information that is customized to the user or the location/site from which the user is remotely located. For example, the user may be located at a hotel for the purpose of attending a specific convention or conference either in the hotel or within the immediate vicinity of the hotel. The gateway device may have "learned" this information about the user through an initial log-on profile inquiry or the gateway administer may have inputted this information into a database.

The gateway device can store user profile information within a user-specific AAA database, as described below, or it can store and retrieve data from external databases. The gateway device can be configured to recognize these profiles and to customize the portal page accordingly. In the hotel scenario, the portal page may include a link for convention or conference services offered by the hotel.

In another example of location specific portal page data, the user may be remotely accessing the gateway device while located in a specific airport terminal. The gateway device will be configured so that it is capable of providing ready access to information related to that specific airport terminal, i.e. information pertaining to the current flights scheduled to depart and arrive that terminal, the retail services offered in that specific terminal, etc. In this manner, the portal page may include a link for terminal specific flight information and/or terminal specific retail services available to the user.

It will also be appreciated that the HPR may be configured so a user is redirected to a portal page upon specific default occurrences, such as a time out, or according to preset time. For example, the portal page may act as a screen-saver, where the user is redirected to a portal page after a given period of inactivity. These functions may be established by the ISP or enterprise network administrator.

Customization of the information comprising the portal page is not limited to the gateway administrator or the network operator. The user may also be able to customize the information that is provided in the portal page. The user customization may be accomplished either directly by the user configuring the portal page manually or indirectly from the gateway device configuring the portal page in response to data found in the user-specific profile. In the manual embodiment the user may be asked to choose which information or type of information they would like supplied in the portal page for that specific network session. For instance, the user may require an alarm clock counter to insure an appointment is met or the user may require periodical updates of a specific stock quote. The information that a user customizes for the portal page may be network session specific, may be associated with the duration of a gateway subscription or may be stored in a user profile for an indefinite period of time. The gateway device's ability to communicate with numerous user databases provides the basis for storing user specific profiles for extended periods of time.

As explained above, the portal page presented to the user can be dependent upon an attribute associated with the user, such as the user's identification, the user's location, an address associated with the user's computer, or a combination thereof The means in which a user is identified and access rights are determined is based upon an Authentication, Authorization and Accounting (AAA) method implemented by the AAA server, and disclosed in U.S. patent application Ser. No. 09/458,602, and filed concurrently with this application.

One function of the AAA server is to identify the user in communication with the gateway device in a manner that is transparent to the user. That is, the user will not be required to reconfigure the computer or otherwise change the home network settings, and no additional configuration software will have to be added to the computer. According to one embodiment of the present invention, after a user is directed to a portal page, the AAA server can be accessed to authorize and authenticate the user. Therefore, upon accessing the network, the user may be forwarded to a generic portal page, and after the user may be authenticated, the user can be forwarded via HPR and SAT to a specialized portal page, as described above.

After receiving a request for access from a user, forwarding the user to a portal page, and identifying the user or location the AAA server then determines the access rights of the particular user. In addition to storing whether users have valid access rights, the user profile database can also include specialized access information particular to a specific location or user, such as the bandwidth of the user's access, or a portal page to which a user should be directed. For example, a user accessing the network from a penthouse may receive a higher access band rate than someone accessing the destination network from a typical hotel room. Additionally, a user profile can include historical data relating to a user's access to the network, including the amount of time a user has accessed the network. Such historical information can be used to determine any fees which may be charged to the user, or due from the user, for access. Specialized access information contained within the user profile may be established by the system administrator, or by the user who has purchased or otherwise established access to the network. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room.

Assuming that a user does not have a subscription for access to the network, a login page enables new users to subscribe to the computer network so that they may subsequently obtain access to networks or online services transparently through the gateway device. The user may take steps to become authenticated so that the user's information may be recorded in the user profile database and the user is deemed valid. For example, a user may have to enter into a purchase agreement, requiring the user to enter a credit card number. If the user needs to purchase access, or if the system needs additional information about the user, the user is redirected from the portal page via HPR and SAT to a location, such as a login page, established to validate new users. SAT and HPR can intervene to direct the user to a webserver (external or internal) where the user has to login and identify themselves. Location-based information and authorization, as described in detail in U.S. patent application Ser. No. 60/161,093, incorporated herein by reference, can be sent to the portal page as part of this redirection process. This enables the portal page to be customized to

include customized information, such as locale restaurant ads or train schedules.

Assuming that a user has not been authorized access to the network based upon location based identification or user input identification, the user must provide the gateway device with sufficient information to become authorized access. Where the user is not authorized access the user is forwarded via HPR and SAT from the portal page to a login page. The login page enables new users to subscribe to the computer network so that they may subsequently obtain access to networks or online services transparently through the gateway device. To direct the users to a login page the AAA server calls upon the HPR function. The HPR directs the user to the login page, and after the user has entered requisite information into the login page, the AAA server adds the new information to the customer profile database and can direct the user to the user's desired destination, such as an Internet address or can return the user to a portal page, depending upon the design of the system. Thus, new users can gain access to networks or online services without being predefined in the user profile database.

After receiving the user's login information, the AAA server will create a user profile utilizing this information so that the user will be able to obtain immediate access to the network next time the user logs in without being required to enter login information again. The AAA server can create a profile for the user in a locally stored user profile database, or can update the user profile in a database external to the gateway device. Regardless of the location of the user profile, the next time the user attempts to login the user's profile will be located in the user profile database, the user's access rights determined, and the user allowed transparent access to networks or services.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

That which is claimed:

1. A method for redirecting an original destination address access request to a redirected destination address, the method comprising the steps of:

receiving, at a gateway device, all original destination address access requests originating from a computer;

determining, at the gateway device, which of the original destination address requests require redirection;

storing the original destination address if redirection is required;

modifying, at the gateway device, the original destination address access request and communicating the modified request to a redirection server if redirection is required;

responding, at the redirection server, to the modified request with a browser redirect message that reassigns the modified request to an administrator-specified, redirected destination address;

intercepting, at the gateway device, the browser redirect message and modifying it with the stored original destination address; and

sending the modified browser redirect message to the computer, which automatically redirects the computer to the redirected destination address.

2. The method of claim **1**, further comprising the step of directing the computer to the stored original destination address after the computer has been automatically redirected to the redirected destination address.

3. The method of claim **2**, wherein the step of directing the computer to the stored original destination address occurs after a predetermined length of time.

4. The method of claim **2**, wherein the step of directing the computer to the stored original destination address occurs after a predetermined computer input event has occurred.

5. The method of claim **1**, wherein the step of responding, at the redirection server, to the modified request with a browser redirect message that reassigns the modified request to an administrator-specified, redirected destination address further comprises responding, at the redirection server, to the modified request with a browser redirect message that reassigns the modified request to a redirected destination address associated with a login page.

6. A system for redirecting an original destination address access request to a redirected destination address, the system comprising:

a computer that initiates original destination address requests;

a gateway device in communication with the computer, that receives the original destination address requests from the computer, determines if redirection of any of the original destination address requests is required, stores the original destination address request if redirection is required and modifies the original destination address request if redirection is required, and

a redirection server in communication with the gateway device that receives the modified request from the gateway device and responds with a browser redirect message that reassigns the request to an administrator-specified, redirect destination address,

wherein the gateway device intercepts the browser redirect message and modifies the response with the stored original destination address before forwarding the browser redirect message to the computer and wherein the computer receives the modified browser redirect message and the computer is automatically redirected to the redirect destination address.

7. The system of claim **6**, further comprising a user profile database in communication with the gateway device that includes stored user-access information.

8. The system of claim **6**, further comprising an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database, the AAA server determines if a user of the computer is entitled to access the original destination address requests based upon the user-access information stored within the user profile database.

9. The system of claim **6**, wherein the redirection server is located within the gateway device.

10. The system of claim **7**, wherein the user-profile database is located within the gateway device.

11. The system of claim **8**, wherein the AAA server is located within the gateway device.

* * * * *

US006636894C1

(12) EX PARTE REEXAMINATION CERTIFICATE (5316th)

United States Patent
Short et al.

(10) **Number: US 6,636,894 C1**
(45) **Certificate Issued: Mar. 28, 2006**

(54) **SYSTEMS AND METHODS FOR REDIRECTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE HAVING REDIRECTION CAPABILITY**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Frederic Delley**, Redwood City, CA (US); **Mark F. Logan**, Santa Monica, CA (US); **Florence C. I. Pagan**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

Reexamination Request:
No. 90/007,220, Sep. 24, 2004

Reexamination Certificate for:
Patent No.: **6,636,894**
Issued: **Oct. 21, 2003**
Appl. No.: **09/458,569**
Filed: **Dec. 8, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/111,497, filed on Dec. 8, 1998.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/225**; 709/249; 709/226

(58) **Field of Classification Search** 709/217, 709/219, 202, 220, 223, 224, 226, 227, 229, 709/238
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,781,550	A		7/1998	Templin et al.
5,802,320	A		9/1998	Baehr et al.
5,948,061	A		9/1999	Merriman et al.
6,014,698	A		1/2000	Griffiths
6,052,725	A	*	4/2000	McCann et al. 709/223
6,098,172	A		8/2000	Coss et al.
6,119,162	A		9/2000	Li et al.
6,226,677	B1		5/2001	Slemmer

OTHER PUBLICATIONS

Complaint, Demand for Jury Trial; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 45 pages; Filed Jul. 23, 2004; United States District Court, Southern District of California.

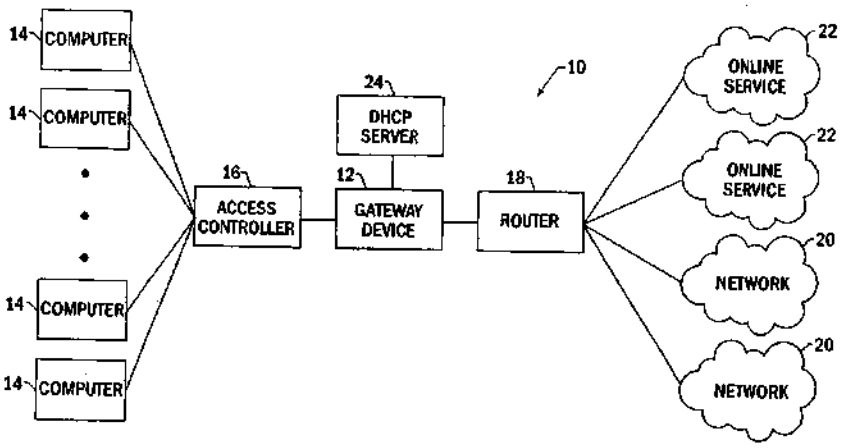
Amended Complaint, Demand for Jury Trial; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 48 pages; Sep. 20, 2004; United States District Court, Southern District of California.

(Continued)

Primary Examiner—Jeffrey Pwu

(57) **ABSTRACT**

Systems and methods for dynamically creating new users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, a user profile database comprising stored access information and in communication with the gateway device, and an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database. The AAA server determines if user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network. The systems and methods of the present invention can also redirect users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings.



OTHER PUBLICATIONS

Answer and Counterclaims of Nomadix Inc. to the Amended Complaint; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 44 pages; Filed Oct. 21, 2004; United States District Court, Southern District of California.

Plaintiff/Counter–Defendant IPE Networks Inc.'s Reply to Defendant Nomadix, Inc.'s Counterclaim; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 8 pages; Nov. 15, 2004; United States District Court, Southern District of California.

David C. Plummer; *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*; Nov. 1982; 8 pages; Network Working Group, Request for Comments 826.

Charles Hornig; *A Standard for the Transmission of IP Datagrams over Ethernet Networks*; Apr. 1984; 3 pages; Network Working Group, Request for Comments 894.

J. Postel; *Multi–Lan Address Resolution;* Oct. 1984; 14 pages; Network Working Group, Request for Comments 925.

R. Braden, J. Postel; *Requirements for Internet Gateways;* Jun. 1987; 50 pages; Network Working Group, Request for Comments 1009.

Smoot Carl–Mitchell, John S. Quarterman; *Using ARP to Implement Transparent Subnet Gateways*; Oct. 1987; 8 pages; Network Working Group, Request for Comments 1027.

P. Mockapetris; *Domain Names—Concepts and Facilities;* Nov. 1987; 49 pages; Network Working Group, Request for Comments 1034.

R. Droms; *Dynamic Host Configuration Protocol;* Oct. 1993; 35 pages; Network Working Group, Request for Comments 1531.

K. Egevang, P. Francis; *The IP Network Address Translator (NAT)*; May 1994; 9 pages; Network Working Group, Request for Comments 1631.

M. Chatel; *Classical Versus Transparent IP Proxies;* Mar. 1996; 32 pages; Network Working Group, Request for Comments 1919.

T. Berners–Lee, F. Fielding, H. Frystyk; *Hypertext Transfer Protocol—HTTP/1.0;* May 1996; 54 pages; Network Working Group, Request for Comments 1945.

Ari Loutonen, Kevin Altis; *World–Wide Web Proxies;* Apr. 1994; 8 pages.

John N. Stewart; *Working with Proxy Servers;* Mar. 1997; pp. 19–22; *WebServer Magazine.*

D. Wessels; *Squid Proxy Server Configuration File 1.93.2.2, "TAG deny_info";* Mar. 1997; 19 pages; available at <http://www.squid–cache.org/mail–archieve/squid–users/199703/att–0250/squid.conf>; (visited Feb. 1, 2005).

Cord Beerman; *Re: Support for cern like Pass/Fair proxy limits?;* 2 pages; available at <http://www.squid–cache.org/mail–archieve/squid–users/199611/0385.html> (visited Feb. 1, 2005).

Information Sciences Institute; *Internet Protocol, DARPA Internet Program, Protocol Specification;* Sep. 1981; 45 pages; available at <http://www.faqs.org/rfcs/rfc791.html> (visited 0002–01–2005).

Doug MacEachern; *Apache/Perl Integration Project;* README; 2 pages; available at <http://apache.perl.org>, <http://outside.organic.com/mail–archives/modperl>, and <http://www.ping.de/~fdc/mod_perl>.

Gisle Aas, Doug MacEachern; *Apache.pm;* 18 pages; available at <http://www.apache.org/docs>.

Mod_perl.c; Copyright; 1995–1997 The Apache Group; 20 pages.

* cited by examiner

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

NO AMENDMENTS HAVE BEEN MADE TO THE PATENT

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1–11** is confirmed.

* * * * *

US007194554B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 7,194,554 B1**
(45) **Date of Patent: Mar. 20, 2007**

(54) **SYSTEMS AND METHODS FOR PROVIDING DYNAMIC NETWORK AUTHORIZATION AUTHENTICATION AND ACCOUNTING**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Florence C. I. Pagan**, Los Angeles, CA (US); **Josh J. Goldstein**, Agoura Hills, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 465 days.

(21) Appl. No.: **09/693,060**

(22) Filed: **Oct. 20, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/458,569, filed on Dec. 8, 1999, now Pat. No. 6,636,894.

(60) Provisional application No. 60/161,182, filed on Oct. 22, 1999, provisional application No. 60/160,890, filed on Oct. 22, 1999, provisional application No. 60/161,139, filed on Oct. 22, 1999, provisional application No. 60/161,189, filed on Oct. 22, 1999, provisional application No. 60/160,973, filed on Oct. 22, 1999, provisional application No. 60/161,181, filed on Oct. 22, 1999, provisional application No. 60/161,093, filed on Oct. 22, 1999, provisional application No. 60/111,497, filed on Dec. 8, 1998.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/246**; 709/217; 709/220; 709/227; 709/230

(58) **Field of Classification Search** 709/229, 709/227, 225, 230, 217, 220, 246
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,113,499 A * 5/1992 Ankney et al. 340/5.74

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 762 707 A2 3/1997

(Continued)

OTHER PUBLICATIONS

USG Product Timeline, Nomadix, Inc., 2701 Ocean Park Blvd., Suite 231, Santa Monica, California 90405.

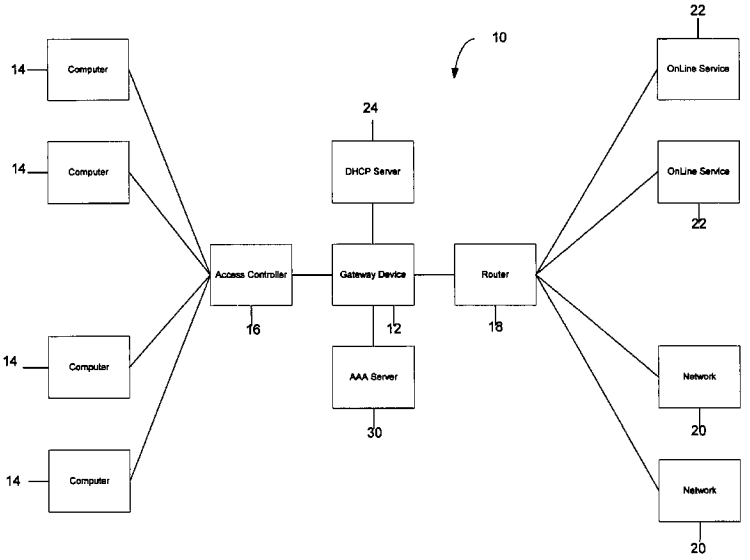
(Continued)

Primary Examiner—Saleh Najjar
Assistant Examiner—Michael Won
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

Systems and methods for selectably controlling and customizing source access to a network, where the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software need be installed on the source computer to access the network. A user may be prevented access from a particular destination or site based upon the user's authorization while being permitted to access to other sites that the method and system deems accessible. The method and system can identify a source without that source's knowledge, and can access customizable access rights corresponding to that source in a source profile database. The source profile database can be a remote authentication dial-in user service (RADIUS) or a lightweight directory access protocol (LDAP) database. The method and system use source profiles within the source profile database to dynamically authorize source access to networks and destinations via networks.

24 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

5,517,622	A *	5/1996	Ivanoff et al.	709/232
5,612,730	A	3/1997	Lewis	
5,623,601	A *	4/1997	Vu	713/201
5,742,668	A *	4/1998	Pepe et al.	455/415
5,864,610	A	1/1999	Ronen	
5,950,195	A	9/1999	Stockwell et al.	
5,968,176	A	10/1999	Nessett et al.	
6,130,892	A *	10/2000	Short et al.	370/401
6,161,139	A *	12/2000	Win et al.	709/225
6,226,752	B1 *	5/2001	Gupta et al.	713/201
6,317,790	B1 *	11/2001	Bowker et al.	709/225
6,385,653	B1 *	5/2002	Sitaraman et al.	709/230
6,502,131	B1 *	12/2002	Vaid et al.	709/224
6,598,167	B2 *	7/2003	Devine et al.	713/201
6,681,330	B2 *	1/2004	Bradford et al.	713/200
6,785,730	B1 *	8/2004	Taylor	709/230
6,856,676	B1 *	2/2005	Pirot et al.	379/201.01

FOREIGN PATENT DOCUMENTS

EP	0 909 073 A2	4/1999
WO	WO 98/16044	4/1998
WO	WO 99/57866	11/1999
WO	WO 99/66400	12/1999

OTHER PUBLICATIONS

Universal Subscriber Gateway, Nomadix, Inc., 2701 Ocean Park Blvd., Suite 231, Santa Monica, California 90405.

Schoen et al., *Convergence Between Public Switching and the Internet*, published Sep. 21, 1997 in *XVI World Telecom Congress Proceedings*, pp. 549-560.

Cisco; *Single-User Network Access Security TACACS+*; Mar. 30, 1995; 9 pages; *Cisco White Paper*; XP002124521.

D. Brent Chapman, Elizabeth D. Zwicky; *Building Internet Firewalls*; Nov. 1995; pp. 131-188; O'Reilly; XP002202789.

Susan Hinrichs; *Policy-Based Management Bridging the Gap*; Dec. 6, 1999; pp. 209-218; Computer Security Applications Conference, 1999 (ACSAC 1999), Proceedings, 15th Annual Phoenix, Arizona, USA Dec. 6-10, 1999, Los Alamitos, California; IEEE Comput. Soc.; XP010368586.

* cited by examiner

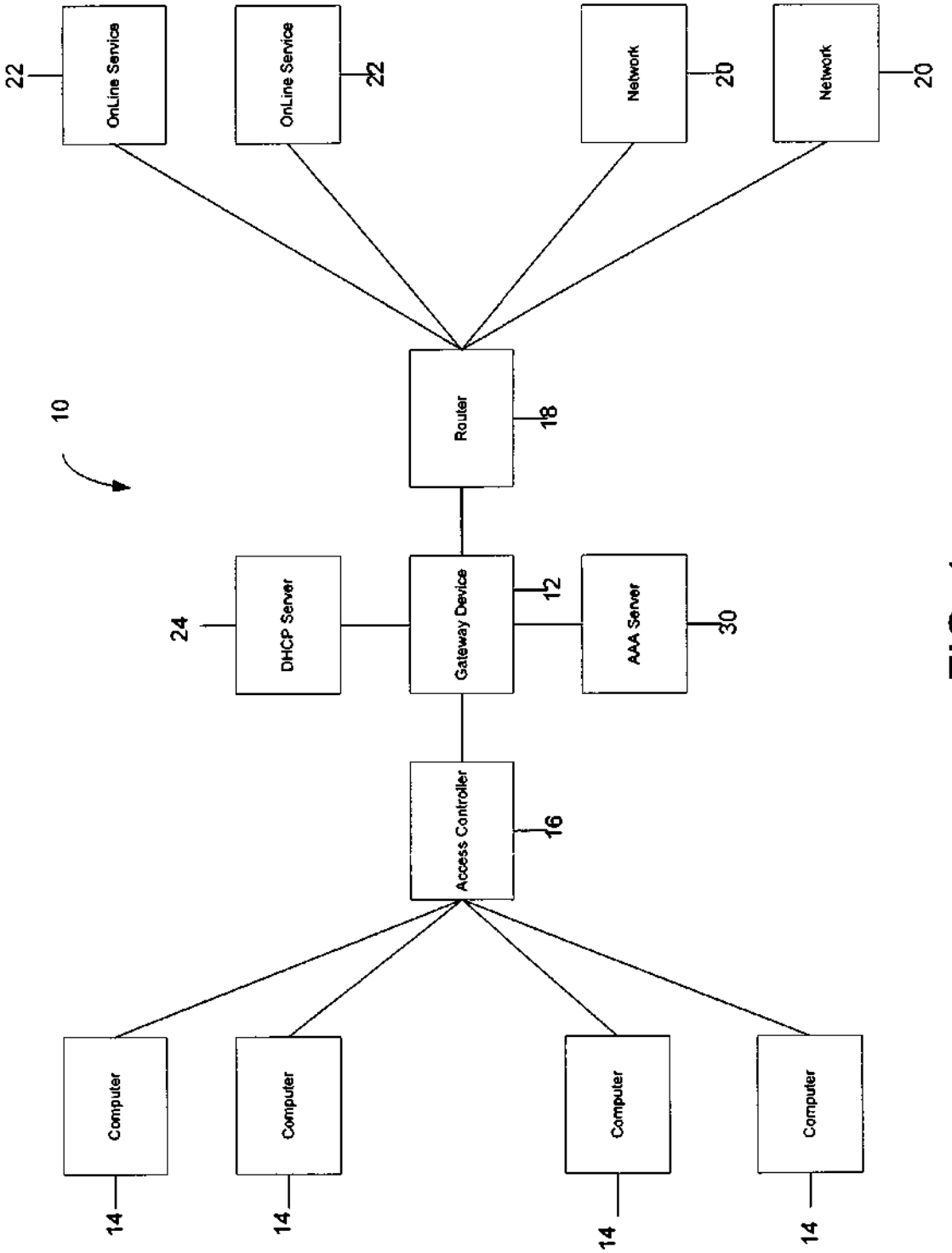

OnLine Service
22
OnLine Service
22
Network
20
Network
20
Router
18
10
DHCP Server
24
Gateway Device
12
AAA Server
30
Access Controller
16
Computer
14
Computer
14
Computer
14
Computer
14

FIG. 1

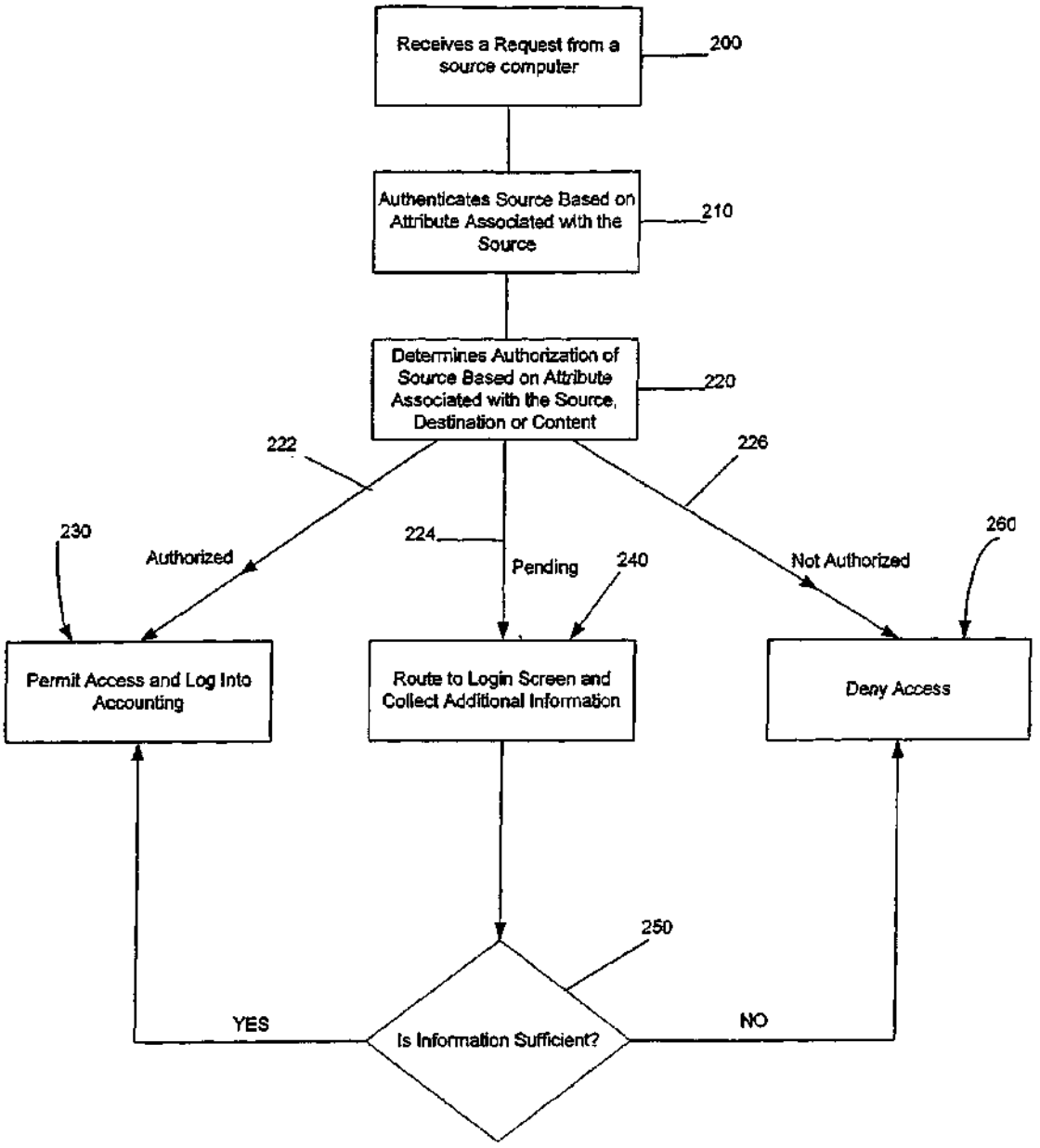

Receives a Request from a source computer
200
Authenticates Source Based on Attribute Associated with the Source
210
Determines Authorization of Source Based on Attribute Associated with the Source, Destination or Content
220
222
226
230
Authorized
224
Pending
240
Not Authorized
260
Permit Access and Log Into Accounting
Route to Login Screen and Collect Additional Information
Deny Access
250
YES
Is Information Sufficient?
NO

FIG. 2

SYSTEMS AND METHODS FOR PROVIDING DYNAMIC NETWORK AUTHORIZATION AUTHENTICATION AND ACCOUNTING

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of copending U.S. patent application Ser. No. 09/458,569, filed on Dec. 8, 1999, titled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability", issued as U.S. Pat. No. 6,636,894, which claims the benefit of the filing date and priority to U.S. Provisional Application Ser. No. 60/111,497 filed on Dec. 8, 1998. This application also claims priority from U.S. application Ser. No. 09/458,602, filed Dec. 8, 1999, titled "Systems and Methods For Authorizing, Authenticating and Accounting Users Having Transparent Computer Access To A Network Using A Gateway Device," U.S. Provisional Application Ser. No. 60/161,182, filed Oct. 22, 1999, titled "Systems and Methods for Dynamic Bandwidth Management on a Per Subscriber Basis in a Computer Network," U.S. Provisional Application Ser. No. 60/160,890, filed Oct. 22, 1999, titled "Systems and Methods for Creating Subscriber Tunnels by a Gateway Device in a Computer Network," U.S. Provisional Application Ser. No. 60/161,139, filed Oct. 22, 1999, titled "Information And Control Console For Use With A Network Gateway Interface," U.S. Provisional Application Ser. No. 60/161,189, filed Oct. 22, 1999, titled "Systems and Methods for Transparent Computer Access and Communication with a Service Provider Network Using a Network Gateway Device," U.S. Provisional Application Ser. No. 60/160,973, filed Oct. 22, 1999, titled "Systems and Methods for Enabling Network Gateway Devices to Communicate with Management Systems to Facilitate Subscriber Management," U.S. Provisional Application Ser. No. 60/161,181, filed Oct. 22, 1999, titled "Gateway Device Having an XML Interface and Associated Method," and U.S. Provisional Application Ser. No. 60/161,093, filed Oct. 22, 1999, titled "Location-Based Identification and Authorization for use With a Gateway Device." All of the above applications are incorporated by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to systems and methods for controlling network access, and more particularly, to systems and methods for establishing dynamic user network access.

BACKGROUND OF THE INVENTION

User access to computer networks has traditionally been based upon a two step authentication process that either provides a user total network access, or refuses the user any access whatsoever. In the first step of the process, a user establishes a communication link with a network via a telephone line, dedicated network connection (e.g., Broadband, Digital Signal Line (DSL)), or the like. In the second step of the authentication process, the user must input identification information to gain access to the network. Typically, the input identification information includes a user name and password. Using this information, the network or service provider verifies that the user is entitled to access the network by determining whether the identification information matches subscriber information contained in a

subscriber table (or database) that stores identification information for all users authorized to access the network. Where user input information matches subscriber data in the subscriber table, the user is authorized to access any and all services on the network. On the other hand, if the user input identification information fails to match subscriber data in the table, the user will be denied access to the network. Thus, once a user's identity is compared to data stored within a subscription table, the user is either entitled network access, or denied access altogether. Furthermore, where the user is authorized access to the network, the user is typically authorized to access any destination accessible via the network. Therefore, conventional authentication of users is based on an all-or-nothing approach to network access.

In many conventional network access applications, such as in conventional Internet access applications, the subscriber database (or table) not only stores data corresponding to the identity of subscribers authorized to access the network, but also stores information that can vary based upon the particular subscriber. For instance, the subscriber database can include subscriber profiles that indicate the type of access a subscriber should receive, and other related information, such as the fees due by the subscriber for network access. Although information in the subscriber database may vary from user to user, information unique to the database is generally used for billing or network maintenance purposes. For instance, conventional subscriber databases typically include data such as the cost the subscriber is paying for network access, and the amount of time the subscriber has accessed the network. Thus, where a subscriber to an Internet Service Provider (ISP) has purchased Internet access, a source profile database may contain information that enables a user to be authenticated and tracks the user's access for accounting purposes, such as maintaining a log of the user's time on the network.

Additionally, in conventional network access systems, in order for a user to connect to on-line services (e.g., the Internet), the user must install client side software onto the user's computer. Client side software is typically provided by a network administrator or network access provider, such as an ISP with whom the user has subscribed for Internet access, and enables the client to configure his or her computer to communicate with that network access provider. Continuing with the illustrative example of a user accessing the Internet via an ISP, the user must install ISP software on the client computer, and thereafter establish an account with the ISP for Internet access. Typically, a user subscribes to an ISP, such as America Online™, Earthlink™, Compuserve™ or the like, by contracting directly with the ISP for Internet access. Usually, the user pays for such Internet access on a monthly fixed fee basis. Regardless of the user's location, the user may dial up an access number provided by the ISP and obtain Internet access. The connection is often achieved via a conventional telephone modem, cable modem, DSL connection, or the like.

Because users accessing networks through conventional methods, such as through ISPs, are either allowed or denied access to a network in an all or nothing approach, users cannot be dynamically authorized access to a network such that the user's access and authorization to particular networks or sites is customizable. What is needed is a method and system that allows users dynamic and customizable access that may vary based upon any number of variables associated with a user, such as a user location, user name or password, user computer, or other attributes. For example, it would be advantageous for some users to be authorized access to all Internet sites, while others may be denied

access to particular sites. In addition to authorizing user access to a network, it would be advantageous for a network, such as an ISP or enterprise network, to selectively permit users a range of authorization, such that the user's access is not based upon an all or nothing approach.

SUMMARY OF THE INVENTION

The present invention includes a method and system for selectively implementing and enforcing Authentication, Authorization and Accounting (AAA) of users accessing a network via a gateway device. According to the present invention, a user may first be authenticated to determine the identity of the user. The authentication capability of the system and method of the present invention can be based upon a user ID, computer, location, or one or more additional attributes identifying a source (e.g., a particular user, computer or location) requesting network access. Once authenticated, an authorization capability of the system and method of the present invention is customized based upon the identity of the source, such that sources have different access rights based upon their identity, and the content and/or destination requested. For instance, access rights permit a first source to access a particular Internet destination address, while refusing a second source access to that same address. In addition, the authorization capability of the system and method of the present invention can be based upon the other information contained in the data transmission, such as a destination port, Internet address, TCP port, network, or similar destination address. Moreover, the AAA of the present invention can be based upon the content type or protocol being transmitted. By authenticating users in this manner, each packet can be filtered through the selective AAA process, so that a user can be identified and authorized access to a particular destination. Thus, each time the user attempts to access a different destination, the user is subject to the AAA, so that the user may be prevented access from a particular site the AAA system and method deem inaccessible to the user based upon the user's authorization while permitting access to other sites that the AAA method and system deem accessible. Additionally, according to one embodiment of the invention, source access to the network may be tracked and logged by the present invention for accounting and historical purposes.

According to one embodiment of the invention, there is disclosed a method for selectably controlling and customizing source access to a network, wherein the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software need be installed on the source computer to access the network. The method includes receiving at the gateway device a request from the source computer for access to the network, identifying an attribute associated with the source based upon a packet transmitted from the source computer and received by the gateway device, and accessing a source profile corresponding to the source and stored in a source profile database, wherein the source profile is accessed based upon the attribute, and wherein the source profile database is located external to the gateway device and in communication with the gateway device. The method also includes determining the access rights of the source based upon the source profile, wherein access rights define the rights of the source to access the network.

According to one aspect of the invention, determining the access rights of the source based upon the source profile includes determining the access rights of the source based upon the source profile, wherein the access rights define the rights of the source to access a requested network destination. According to another aspect of the invention, the method includes assigning a location identifier to the location from which requests for access to the network are transmitted, and the location identifier is the attribute associated with the source. Furthermore, according to the invention, accessing a source profile corresponding to the source can include accessing a source profile stored in a source profile database, where the source profile database includes a remote authentication dial-in user service (RADIUS), or a lightweight directory access protocol (LDAP) database.

According to yet another aspect of the invention, the method includes updating the source profile database when a new source accesses the network. Additionally, the method can include maintaining in the source profile database a historical log of the source's access to the network. Moreover, the attribute associated with the source can be based upon a MAC address, User ID or VLAN ID associated with the source computer from which the request for access to the network was transmitted. According to yet another aspect of the invention, receiving at the gateway device a request from a source for access can include the step of receiving a destination address from the source.

According to another embodiment of the invention, there is disclosed a system for selectably controlling and customizing access, to a network, by a source, where the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software need be installed on the source computer to access the network. The system includes a gateway device for receiving a request from the source for access to the network, and a source profile database in communication with the gateway device and located external to the gateway device, wherein the source profile database stores access information identifiable by an attribute associated with the source, and wherein the attribute is identified based upon a data packet transmitted from the source computer and received by the gateway device. The system also includes a AAA server in communication with the gateway device and source profile database, wherein the AAA server determines if the source is entitled to access the network based upon the access information stored within the source profile database, and wherein the AAA server determines the access rights of the source with the access rights defining the rights of the source to access destination sites via the network.

According to one aspect of the invention, the packet received by the gateway device includes at least one of VLAN ID, a circuit ID, and a MAC address. Additionally, according to another aspect of the invention, the source profile database includes a remote authentication dial-in user service (RADIUS) or a lightweight directory access protocol (LDAP) database. Furthermore, the source profile database can include a plurality of source profiles, wherein each respective source profile of the plurality of source profiles contains access information. According to the invention, each respective source profile can also contain historical data relating to the duration of network access for use in determining the charges due for the network access. According to yet another aspect of the invention, the source profile database can be located within the AAA server.

According to another embodiment of the present invention, there is disclosed a method for redirecting a source attempting to access a destination through a gateway device, wherein source is associated with a source computer, and wherein the gateway device enables the source to commu-

nicate with a network without requiring the source computer to include network software configured for the network. The method includes receiving at the gateway device a request from the source to access the network, identifying the source based upon an attribute associated with the source, and accessing a source profile database located external to the gateway device, where the source profile database stores access rights of the source. The method further includes determining the access rights of the source based upon the identification of the source, wherein the access rights define the rights of the source to access destination sites via the network.

According to one aspect of the invention, accessing a source profile database includes accessing a source profile database that includes a remote authentication dial-in user service (RADIUS), or a lightweight directory access protocol (LDAP) database. According to another aspect of the invention, the method can include assigning a location identifier to the location from which requests for access to the network are transmitted, wherein the location identifier is the attribute associated with the source. The method can also include updating the source profile database when a new source accesses the network, and maintaining in an accounting database a historical log of the source's access to the network, wherein the accounting database is in communication with the source profile database.

According to yet another aspect of the invention, receiving at the gateway device a request from a source for access can include the step of receiving a destination address from the source. Moreover, determining if the source computer is entitled to access the destination address can further include denying the source computer access where the source profile indicates that the source computer is denied access. Determining if the source is entitled to access the network can also further include directing the source to a login page when the source profile is not located within the source profile database.

According to yet another embodiment of the invention, there is disclosed a system for enabling transparent communication between a computer and a service provider network. The system includes a computer, and a network gateway device in communication with the computer for connecting the computer to a computer network, where the network gateway device receives source data that represents a user attempting to access said computer network. The system also includes a service provider network in communication with the network gateway device, where the service provider network includes an authentication server located external to the network gateway device and in communication with the network gateway device. The authentication server has therein a source profile database comprising source profiles that represent users authorized to access said computer network, and compares the source data to said source profiles to determine if the user attempting to access the computer network can access the computer network.

According to one aspect of the invention, the system can include an accounting system for maintaining historical data concerning use of the service provider network. According to another aspect of the invention, the authentication server includes a remote authentication dial-in user service (RADIUS), or a lightweight directory access protocol (LDAP) database. Furthermore, the source profile database can include a plurality of source profiles, where each respective source profile of the plurality of source profiles contains access information. According to yet another aspect of the invention, the source data includes an attribute associated with the computer and transmitted from the computer to the gateway device. According to anther aspect of the invention, the source data includes login information associated with a respective user.

The Authentication, Authorization and Accounting method and system according to the present invention enable users transparent access to a computer network employing a gateway device. Therefore, each user may have differing rights to access services, sites or destinations via the network. Thus, the present invention differs from conventional AAA methods and systems by offering dynamic AAA services which authenticate users and offer those users varying degrees of authorization to utilize the accessed network. Furthermore, the source profile database of the present invention can be located external to the gateway device, and on a network non-local to the network from which access is requested. An external source profile database is desirable because each gateway device allows a finite number of users to access the network, so that multiple gateway devices may be required. Additionally, administering and maintaining one consolidated database of authentication data is easier than multiple smaller databases. Moreover, locating the database external to the local network allows an ISP or third party provider to maintain the confidentiality of the information stored within the database and maintain and control the database in any manner the third party provider so desires.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system that includes a AAA server for authenticating, authorizing and accounting sources accessing networks and/or online services, according to one embodiment of the present invention.

FIG. **2** is a flow chart of a method in which a AAA server performs authentication, authorization, and accounting, according to one aspect of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, a computer system **10** is illustrated in block diagram form. The computer system **10** includes a plurality of computers **14** that can communicate with one or more online services **22** or networks via a gateway device **12** providing the interface between the computers **14** and the various networks **20** or online services **22**. One embodiment of such a gateway device has been described in U.S. patent application Ser. No. 08/816,174 (referred to herein as the Gateway Device Application), the contents of which are incorporated herein by reference. Briefly, the gateway device **12** facilitates transparent computer **14** access to the online services **22** or networks **22**, such that the computers **14** can access any networks via the device **12** regardless of their network configurations. Additionally, the gateway device **12** includes the ability to recognize computers attempting to access a network **12**, the

location of computers attempting to access a network, the identity of users attempting to gain network access, and additional attributes, as will be discussed below with respect to the dynamic AAA methods and systems of the present invention.

As illustrated in FIG. **1**, the computer system **10** also includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end (a Cable Modem Termination Shelf (CMTS)) for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a switch, or the like.

The computer system **10** further includes a AAA server **30** that dynamically authenticates and authorizes user access, as explained in detail below, such that users are subjected to a AAA process upon attempting to gain access to a network through the gateway device **12**. Finally, as is shown in FIG. **1**, the computer system **10** typically includes one or more routers **18** and/or servers (not shown in FIG. **1**) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks **20** or online services **22**. In this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of the networks **20** or online services **22**, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. **1** may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**.

Users and computers attempting to access a network **20** or online service **22** via the gateway device **12** are referred to hereinafter as sources. According to AAA methods and systems of the present invention, a source attempting to access a network via the gateway device **12** is authenticated based on attributes associated therewith. These attributes can include the identity of a particular user or computer, location through which access is requested, requested network or destination, and the like. As is explained in detail in the Gateway Device Application, these attributes are identified by data packets transmitted to the gateway device **12** from the computers through which access is requested. According to one embodiment, methods and systems of the present invention provide dynamic authentication, authorization and accounting based upon these attributes. Generally, as used herein authentication refers to the identification of the source, authorization refers to the determination of permittable source access, and accounting refers to the tracking of a source's access to a network.

Referring now to the authentication function of systems and methods of present invention, it will be appreciated that authenticating a source attempting to access the network is often crucial to network administration, as network access and services are not typically laid open for all users regardless of identity or payment. As stated above, a source may be identified by the gateway device **12** by one or more attributes contained within data packets transmitted to the device from the computer associated with the source attempting to access a network or service, referred to hereinafter as the source computer. For instance, where the source is a user, the source computer is the computer through which the user is attempting to access a network or network destination. On the other hand, where the source is a computer through which one or more user may request access to a network, the source computer is that computer through which access is requested.

According to one aspect of the invention, a source computer attempting to access a network via the gateway device **12** may be identified one or more attributes that include a circuit ID, MAC address, user name, ID and/or password, or particular location (e.g., a communications port in a hotel room), or the like, transmitted to the gateway device **12** via data packets generated by the source computer, as described in U.S. Provisional Application Ser. No. 60/161,093, titled "Location-Based Identification and Authorization for use With a Gateway Device." It will be appreciated that one or more of these attributes can be used in the present invention to identify the source accessing the network. By means of an illustrative example, where sources are different users having dissimilar authentication and authorization rights, the users may identify themselves by their respective login information (e.g., user name and password) such that they will be independently identified despite the use of the same equipment, such as the same computer. On the other hand, where the source is a computer, diverse users using the computer will have like authentication and authorization rights regardless of the individual rights of each user, as the rights are associated with the computer (e.g., identified by MAC address), rather than with the respective users.

The authentication of sources via an attribute associated with the source is performed by the AAA server **30**, illustrated in FIG. **1**. The AAA server **30** stores source profiles corresponding to sources identified by the AAA server **30**. According to one aspect of the present invention, the AAA server **30** is located entirely within the gateway device **12**. According to another aspect of the invention, the AAA server **30** can comprise a plurality of components, at least some of which are external to the gateway device **12**, or alternatively, the AAA server **30** can be located entirely external to the gateway device **12**. For example, the location of the AAA server **30** may be such that the gateway device **12** communicates with the AAA server **30** via internet protocol.

According to one embodiment of the invention, the AAA server **30** can be maintained by an ISP, which identifies sources authorized to communicate with the network via the ISP. Therefore, it will be appreciated that the AAA server **30** may be located at any internet address and stored on any computer accessible via internet protocol.

According to one aspect of the invention, a separate source profile exists for each source accessing the system. Source profiles are maintained in a source profile database, which may be an internal component of the AAA server **30**, an external component of the AAA server **30**, or a separate component in communication with the AAA server **30**. Preferably, the source profile database is located external to the gateway device and network to alleviate administrative burden on the network so that the network does not have to set up and maintain separate authentication databases on each network or gateway device. This is also preferable because each gateway device **12** allows a finite number of users to access the network, which requires multiple gateway devices to accommodate a large number of sources. Secondly, administering and maintaining one consolidated

database of authentication data is easier than multiple smaller databases. Lastly, locating the source profile database external to the local network can allow an ISP or third party provider to maintain the confidentiality of the information stored within the database and maintain and control the database in any manner the third party provider so desires.

The source profile includes one or more names, passwords, addresses, VLAN tags, MAC addresses and other information pertinent to identify, and, if so desired, bill, a source. Upon a source's attempt to access a network via the gateway device **12**, the AAA server **30** attempts to authenticate the source by comparing stored source profiles in the source profile database with the attributes received from the gateway device **12** or source to determine the source identity. As an illustrative example, where a user attempts to access the network by entering a user ID and password, the user ID and password are compared against all IDs and passwords stored in the source profile database to determine the identity of the user. As such, the source profile database generally comprises a database or data storage means in communication with processing means located within the AAA server **30** or gateway device **12**, where the source profile database and processor work in conjunction to compare received attributes to stored source profile information, as is well known in the art.

The source profile database may comprise programmable storage hardware or like means located on a conventional personal computer, mainframe computer, or another suitable storage device known in the art. Additionally, the means for comparing the received data to the data within the database can comprise any software, such as an executable software program, which can compare data. For example, the AAA server **30** may store source profiles on a hard drive of a personal computer, and the means for comparing the received source data to the source profiles resident on the computer can include computer software, such as Microsoft Excel (Microsoft Excel is a trademark of Microsoft Corporation, Redmond, Wash.). According to another embodiment of the invention, the AAA server **30** or source profile database can comprise a Remote Authentication Dial-In User Service (RADIUS) or a Lightweight Directory Access Protocol (LDAP) database, which are well known to those of skill in the art.

If a source fails to correspond to a source profile in the AAA server **30** at the time of authentication, the source will not be permitted access to the network. When this occurs, a user or user associated with a non-user source may be requested to input source profile information to the AAA server **30** so that the AAA server **30** can add the source's profile to the AAA server **30**, and more specifically, to the source profile database. For example, this may occur the first time a user attempts to access the gateway device **12**. According to another aspect of the invention, where the source cannot be identified, the source may be directed to a login page in order to gather additional information to identify the source. For instance, the information may be entered with the aid of a webpage, a pop-up control panel or user interface, which can open when the source initially connects to the gateway device **12**, as effectuated by a home page redirection capability, described herein and in U.S. patent application Ser. No. 09/458,569, filed Dec. 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability" (referred to hereinafter as the "Redirection Application"), in U.S. patent application Ser. No. 09/458,579, filed Dec. 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability," and in U.S. patent application, Entitled "Systems and Methods for Redirecting Users Attempting to Access a Network Site," filed concurrently herewith, inventors Joel Short and Florence Pagan, the contents of each of which are incorporated herein by reference.

According to one aspect of the invention, the AAA server **30** can identify the source in communication with the gateway device in a manner that is transparent to computer users via a packet translation learned during a self configuration. That is, according to one aspect of the invention, a user will not be required to input identification, reconfigure the source computer or otherwise change the source computer's primary network settings. Furthermore, no additional configuration software will have to be added to the source computer. After a packet is received by the gateway device, attributes identified by the data packet can be compared with the data contained in the source profile database. Therefore, in addition to not requiring the reconfiguration of computers accessing the network, AAA servers of the present invention have the ability to authenticate sources without requiring interactive steps by the computer user, such as the entering of a user ID. For instance, the AAA server **30** may automatically identify the source based upon a MAC address, so that authorization of the source can be readily determined. Therefore, it will be appreciated that the AAA server **30** can determine the user, computer, or location from which the access is requested by comparing the attributes associated with the received data packet (such as in a header of the data packet) with data drawn from the source profile database. As will be described below, the access rights associated with the source may also be stored within the source profile database so that the system and method of the present invention can dynamically authorize access to particular services or destinations.

Once the source has established the network service connection via the authentication process discussed above, and a tunnel has been opened to facilitate a communication line between the source computer and a network, the gateway device **12** communicates with the AAA server **30** to assemble source profile information, or source-specific data. The source profile information that the gateway device assembles may include a MAC address, name or ID, circuit ID, billing scheme related data, service level data, user profile data, remote-site related data, and like data related to the source. As such, the AAA server **30** can transmit to the gateway device **12** any requisite information relating to the source's authorization rights and use of the network, as is next explained in detail.

In addition to authenticating users, the AAA server **30** of the present invention provides an authorization function, in which the source access rights are determined. The present invention enables dynamic authorization of sources, such that each source might have different respective network usage or access rights. After authentication, the AAA server **30** compares the attributes of the source with the access rights of the source associated with the user, computer, location or attribute(s). The access rights may be stored within the source profile database or within a separate subscription database located internal or external to the gateway device **12**. Therefore, separate databases may be utilized, where one stores identification information on sources for authentication, and another database stores the access rights of those sources that have been authenticated. However, because the profiles of all sources, identified by

attribute or a combination of attributes, are stored in a source profile database, it may be advantageous to locate information regarding access rights in the source profile database, which already contains information regarding each authenticated source, as described above.

According to one aspect of the invention the source profile database stores information defining the access rights of a source. For example, a source profile database may contain information indicating that a source having a particular MAC address has purchased pre-paid access, or that a given circuit ID has free access or unlimited access. Guests in a particular room or rooms of a hotel, for example, suites and penthouses, may receive free unlimited Internet access. Therefore, access rights can be available contingent upon the source's location (e.g. room) or location status (e.g. suite). In this event, no further identification is required, as the location from which the source is requesting access is known to the gateway device and stored in the source profile database.

In addition to storing information concerning what each source is authorized to access, the source profile database can also include specialized access information associated with a particular source, such as the bandwidth of the source's access, or a homepage to which the source should be directed. For example, a user accessing the network from a penthouse may receive a higher access baud rate than someone accessing the network from a typical hotel room. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the source profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room. Additionally, the user may establish the information to be contained within the source profile database upon first accessing the gateway device. For instance, a new user may be directed to enter a credit card number, e-wallet account information, pre-paid calling card number or like billing information to obtain access to the system. A source profile can also include historical data relating to a source's access to the network, including the amount of time a source has accessed the network. Specialized access or accounting information contained within the source profile database may be established by the system administrator, or by the source who has purchased or otherwise established access to the network.

According to one aspect of the invention, the authorization capability of the AAA server **30** can be based upon the type of services the source is attempting to access, such as a destination address, identified by the gateway device **12** based upon data received from the source computer. The destination can be a destination port, Internet address, TCP port, network, or the like. Moreover, the authorization capability of the AAA server **30** can be based upon the content type or protocol being transmitted. According to the system and method of the present invention, each packet can be filtered through the selective AAA process, so that any or all sources can be authorized access to a particular destination based on the access rights associated with the respective sources. Therefore, according to the present invention, each time the source attempts to access a different destination, the source is subject to the AAA, so the source may be prevented access from a particular site the AAA server **30** deems inaccessible to the source based upon the source's authorization. Alternatively, the AAA method according to the present invention allows some or all sources to connect directly to a specific site, such as credit card or billing servers for collecting billing information, which can collect payment or billing information so that the source profile can be updated and the source thereafter authorized access to networks. According to the system and method of the present invention, a source's authorization can also depend upon objective criteria, such as a specific time, so that the session can be terminated at a specific time, after a specific time has elapsed, or according to other dynamic information determined by the network provider. Furthermore, authorization can be associated with a combination of attributes. For example, a user may be authorized access to a network where the user has input the user's identification and has accessed the network from a particular room. Such a requirement could prevent unauthorized users also staying in a particular room from obtaining network access. Therefore, AAA can be based upon the origination, destination, and type of traffic.

By way of further explanation, a flow chart of the operation of the AAA server **30** will be described with respect to FIG. **2**, according to one aspect of the invention. In operation, a source computer requests (block **200**) access to a network, destination, service, or the like. Upon receiving a packet transmitted to the AAA server **30**, the AAA server **30** examines the packet to determine the identity of the source (block **210**). The attributes transmitted via the packet are temporarily stored in the source profile database so that the data can be examined for use in determining authorization rights of the source. The attributes contained in the packet can include network information, source IP address, source port, link layer information, source MAC address, VLAN tag, circuit ID, destination IP address, destination port, protocol type, packet type, and the like. After this information is identified and stored, access requested from a source is matched against the authorization of that source (block **230**).

Once a source profile has been determined by accessing the authorization rights stored in the source profile database, three possible actions can result. Specifically, once a source's authorization rights have been retrieved the AAA server **30** may determine a source to have access **222**, to be pending or in progress **224**, or to not have access **226**. First, a source is deemed valid (i.e., to have access) where the source profile database so states. If a source is determined to be valid, the source's traffic can be allowed to proceed out of the gateway device to the networks or online services the user associated with the source wishes to access (block **230**). Alternatively, the source may be redirected to a portal page, as described in the Redirecting Application, prior to being allowed access to the requested network. For example, a user may be automatically forwarded to a user-input destination address, such as an Internet address, for example, where a user has free access associated with the user's hotel room. Alternatively, this may occur where the user has already purchased access and the user has not exhausted available access time. Furthermore, an accounting message may be initiated **230** to log the amount of time the user is utilizing the gateway device such that the user or location may be billed for access.

If the second scenario occurs, in which the source is deemed pending **224** or in progress, the source may take steps to become authenticated (block **240**) so that the source information is recorded in the source profile database. For example, a user may have to enter into a purchase agreement, requiring the user to enter a credit card number. If the user needs to purchase access, or if the system needs additional information about the user, the user can be

redirected from the portal page via Home Page Redirect (HPR) and Stack Address Translation (SAT) to a location, such as a login page, established to validate new users. SAT and HPR can intervene to direct the user to a webserver (external or internal) where the user has to login and identify themselves. This process is described in detail in the Redirecting Application. After inputting any necessary and sufficient information, the user is then be permitted access to a destination address (block **230**, **250**). Where the information provided is insufficient the user will not be authorized access (block **260**). Finally, a third scenario can occur in which a source is deemed not to have access **226** so that the user is not permitted to access a destination via the network (block **260**).

Referring now to the accounting function of systems and methods of the present invention, upon authorizing a source network access, the AAA server **30** can register an accounting start to identify that the source is accessing the network. Similarly, when the source logs off or terminated the network session, an accounting stop can be registered by the AAA server **30**. Accounting starts or stops can be identified by the gateway device **12** or by the AAA server **30** upon a source's authentication or authorization to access a desired destination. Furthermore, accounting starts or stops can be registered in the source profile, or can be stored in a database separate from the AAA server **30** and located external to the network. Typically, accounting starts and stops include time stamps that indicate the amount of time a source has been accessing the network. Using this data, the time between the accounting start and accounting stop can be tallied so that the source's total connection time may be computed. Such information is valuable where the source is charged by an increment of time, such as an hour. A billing package, as are well known in the art, could then tally a user's total time accessing the network over a set period, such as each month, so that a bill can be created for the source. Because networks and ISPs often may charge a set rate for a specific duration of time (i.e., flat rate pricing), such as a month, regardless how much time is being spent accessing the network, accounting stops and starts may not be required for billing purposes. Nevertheless, accounting starts and stops may generally be recorded by the network provider or ISP for usage statistics.

An ISP or similar access provider would additionally benefit from being able to track subscriber's use of the ISP to establish bills, historical reports, and other relevant information. Preferably, the AAA server **30** is in communication with one or more processors for determining any fees which may be charged to the source, or due from the source, for network access or services. The AAA server **30** retrieves the historical accounting data in a real time basis or after a specific interval of time has elapsed. Preferably, the AAA server **30** retains such data in an easily accessible and manipulatable format such that the access provider (e.g., ISP) can produce reports representative of any desired type of historical data. For example, to project future use of the access provider, the AAA server **30** produces reports tallying the number of users accessing the Internet at certain time periods and from specific locales. Moreover, where the access provider provides alternative access to users, such as charging for faster connections (i.e., higher baud rate) for additional fees, the access provider may wish to analyze historical data using the AAA server **30** to best meet future customer demands. Such data may relate to network sessions currently on-going, the duration of those sessions, the bandwidth currently being used, the number of bytes that have been transferred and any other pertinent information. The AAA server **30** may be implemented using well known programs, such as Eclipse Internet Billing System, Kenan Broadband Internet Billing Software (manufactured by Lucent Technologies), or TRU RADIUS Accountant.

It will be appreciated that the AAA server **30** can dynamically account source access to a network in the same manner in which access is customizable on a source by source basis. That is, the AAA server **30** can maintain accounting records that vary depending upon the identity of a source, source location, source requested destination, or the like. Like the access or authorization rights, this information can be maintained in the source profile database or a similar accounting database. For instance, the AAA server **30** may determine that a particular source is only charged for accessing particular sites, and will only register an accounting site when those particular sites are accessed. Therefore, the AAA server **30** will identify account information stored in the subscriber's source profile to determine accounting starts, accounting stops, billing rates, and the like.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

The invention claimed is:

1. A method for selectably controlling and customizing source access to a network, wherein the source is associated with a source computer, comprising:

receiving at the gateway device a request from the source computer for access to the network wherein the gateway device enables the source computer to access any network regardless of network configurations via a packet translation learned during a self configuration and no configuration software need be installed on the source computer to access the network;

identifying an attribute associated with the source based upon a packet transmitted from the source computer and received by the gateway device;

accessing a source profile corresponding to the source and stored in a source profile database, wherein the source profile is accessed based upon the attribute, and wherein the source profile database is located external to the gateway device and in communication with the gateway device, and

determining the access rights of the source based upon the source profile, wherein access rights define the rights of the source to access the network.

2. The method of claim **1**, wherein determining the access rights of the source based upon the source profile comprises determining the access rights of the source based upon the source profile, wherein access rights define the rights of the source to access a requested network destination.

3. The method of claim **1**, further comprising assigning a location identifier to the location from which requests for access to the network are transmitted, and wherein the location identifier is the attribute associated with the source.

4. The method of claim **1**, wherein accessing a source profile corresponding to the source comprises accessing a source profile stored in a source profile database, wherein the source profile database comprises a remote authentication dial-in user service (RADIUS).

5. The method of claim 1, wherein accessing a source profile corresponding to the source comprises accessing a source profile stored in a source profile database, wherein the source profile database comprises a lightweight directory access protocol (LDAP) database.

6. The method of claim 1, further comprising updating the source profile database when a new source accesses the network.

7. The method of claim 1, further comprising maintaining in the source profile database a historical log of the source's access to the network.

8. The method of claim 1, wherein the attribute associated with the source is based upon one of a MAC address, User ID or VLAN ID associated with the source computer from which the request for access to the network was transmitted.

9. The method of claim 1, wherein receiving at the gateway device a request from a source for access comprises the step of receiving a destination address from the source.

10. A system for selectably controlling and customizing access, to a network, by a source, where the source is associated with a source computer, and wherein no configuration software need be installed on the source computer to access the network, comprising:

a gateway device, wherein the gateway device receives a request from the source for access to the network and provides the source computer with access to the network regardless of network configurations via a packet translation learned during a self configuration;

a source profile database in communication with the gateway device and located external to the gateway device, wherein the source profile database stores access information identifiable by an attribute associated with the source, and wherein the attribute is identified based upon a data packet transmitted from the source computer and received by the gateway device, and

an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and source profile database, wherein the AAA server determines if the source is entitled to access the network based upon the access information stored within the source profile database, and wherein the AAA server determines the access rights of the source, wherein access rights define the rights of the source to access destination sites via the network.

11. The system of claim 10, wherein the packet received by the gateway device include at least one of VLAN ID, a circuit ID, and a MAC address.

12. The system of claim 10, wherein the source profile database comprises a remote authentication dial-in user service (RADIUS).

13. The system of claim 10, wherein the source profile database comprises a lightweight directory access protocol (LDAP) database.

14. The system of claim 10, wherein the source profile database includes a plurality of source profiles, wherein each respective source profile of the plurality of source profiles contains access information.

15. The system of claim 14, wherein each respective source profile contains historical data relating to the duration of network access for use in determining the charges due for the network access.

16. The system of claim 10, wherein the source profile database is located within the AAA server.

17. A method for redirecting a source attempting to access a destination through a gateway device, wherein source is associated with a source computer, and wherein the gateway device enables the source to communicate with a network, comprising:

receiving at the gateway device a request from the source to access the network regardless of network configurations via a packet translation learned during a self configuration and without requiring the source computer to include network software configured for the network;

identifying the source based upon an attribute associated with the source;

accessing a source profile database located external to the gateway device, the source profile database storing access rights of the source;

determining the access rights of the source based upon the identification of the source, wherein the access rights define the rights of the source to access destination sites via the network; and

directing the source to a redirection site when the source profile is not located within the source profile database.

18. The method of claim 17, wherein accessing a source profile database comprises accessing a source profile database comprising a remote authentication dial-in user service (RADIUS).

19. The method of claim 17, wherein accessing a source profile database comprises accessing a source profile database comprising a lightweight directory access protocol (LDAP) database.

20. The method of claim 17, further comprising assigning a location identifier to the location from which requests for access to the network are transmitted, and wherein the location identifier is the attribute associated with the source.

21. The method of claim 17, further comprising updating the source profile database when a new source accesses the network.

22. The method of claim 17, further comprising maintaining in an accounting database a historical log of the source's access to the network, wherein the accounting database is in communication with the source profile database.

23. The method of claim 17, wherein receiving at the gateway device a request from a source for access comprises the step of receiving a destination address from the source.

24. The method of claim 19, wherein determining if the source computer is entitled to access the destination address further comprises denying the source computer access where the source profile indicates that the source computer is denied access.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,194,554 B1
APPLICATION NO. : 09/693060
DATED : March 20, 2007
INVENTOR(S) : Short et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page at Item (63), Line 2, after "Pat. No. 6,636,894" insert --and Continuation-in-part of application No. 09/458,602, filed on Dec. 8, 1999.--

Signed and Sealed this

Eighth Day of December, 2009

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

US006868399B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 6,868,399 B1**
(45) **Date of Patent: Mar. 15, 2005**

(54) **SYSTEMS AND METHODS FOR INTEGRATING A NETWORK GATEWAY DEVICE WITH MANAGEMENT SYSTEMS**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Denis I. Perelyubskiy**, Van Nuys, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 427 days.

(21) Appl. No.: **09/693,061**

(22) Filed: **Oct. 20, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/160,973, filed on Oct. 22, 1999, provisional application No. 60/161,182, filed on Oct. 22, 1999, provisional application No. 60/161,139, filed on Oct. 22, 1999, provisional application No. 60/161,189, filed on Oct. 22, 1999, provisional application No. 60/161,181, filed on Oct. 22, 1999, and provisional application No. 60/161,093, filed on Oct. 22, 1999.

(51) **Int. Cl.**[7] **G06F 17/60**
(52) **U.S. Cl.** **705/34**; 709/224
(58) **Field of Search** 705/34; 709/224

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,612,730	A		3/1997	Lewis	
5,745,884	A	*	4/1998	Carnegie et al.	705/34
5,802,502	A	*	9/1998	Gell et al.	705/34
5,852,812	A	*	12/1998	Reeder	705/34

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

EP	0 762 707 A2		3/1997	
JP	2000-354127 A	*	12/2000	H04N/1/00
JP	2002-111870 A	*	4/2002	H04M/3/42
WO	WO 98/16044		4/1998	

OTHER PUBLICATIONS

"Atreus Systems Corporations and B2B Connect, Inc. Partner to Deliver Bundled Broadband Services to Multi– Tenant, High Ri Buildings", Feb. 14, 2000, Business Wire.*

"NetGame Ltd. Announces its High–Speed, In–Room Hotel Internet Access Product to be Displayed at HITEC 99", Jun. 16, 1999, Business Wire.*

"Copper Mountain Introduces CopperPowered Hotel Initiative to Deliver Cost–effective Always–on or Usage–based Broadband Access to Hotel Guests", Dec. 6, 1999, Business Wire.*

"Nomadix Joins Copper Mountain Networks to Provide High–Speed Internet Access to Hotels Guests", Dec. 6, 1999, Business Wire.*

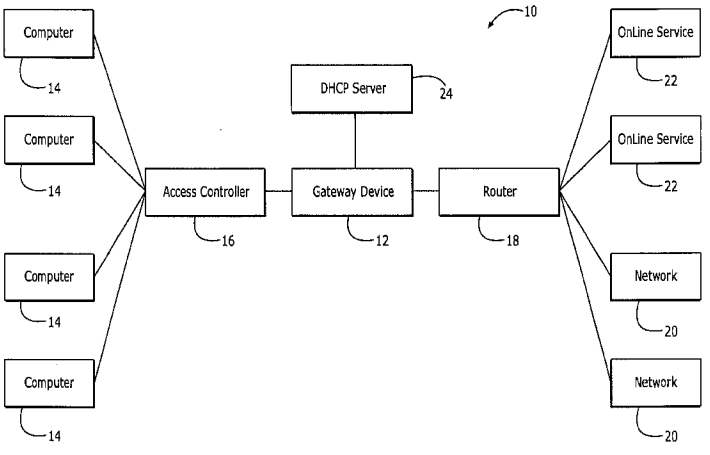
(List continued on next page.)

Primary Examiner—Bryan J Jaketic
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

Systems and methods enabling a management system to communicate with a network gateway device to automatically manage a user accessing a computer network, such as a local network. The system includes a computer, and a network gateway device in communication with the computer for connecting the computer to a computer network, wherein the network gateway device maintains data representative of the user's access to the computer network and wherein the network gateway device reconfigures the data. The system also includes a management system connected to said network gateway device for automatically billing the user based upon usage of the computer network, wherein the management system is configured to communicate according to at least one compatible protocol. The network gateway device reconfigures the data to meet one of the predetermined protocols supported by the management system, and the management system receives the data reconfigured by the network gateway device and utilizes the data reconfigured by the network gateway device for automatic billing purposes.

21 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

5,864,610	A		1/1999	Ronen	
5,893,077	A	*	4/1999	Griffin	705/34
5,950,195	A		9/1999	Stockwell et al.	
5,987,430	A	*	11/1999	Van Horne et al.	705/34
6,119,160	A	*	9/2000	Zhang et al.	709/224
6,208,977	B1	*	3/2001	Hernandez et al.	705/34
6,338,046	B1	*	1/2002	Saari et al.	705/34
6,349,289	B1	*	2/2002	Peterson et al.	705/34
6,496,850	B1	*	12/2002	Bowman-Amuah	709/224

OTHER PUBLICATIONS

"Ascend Communications and ATCOM/INFO Announce Development Alliance", Jun. 22, 1999, Business Wire.*

Schoen et al., *Convergence Between Public Switching and the Internet*, published Sep. 21, 1997 in *XVI World Telecom Congress Proceedings*, pp. 549–560.

* cited by examiner

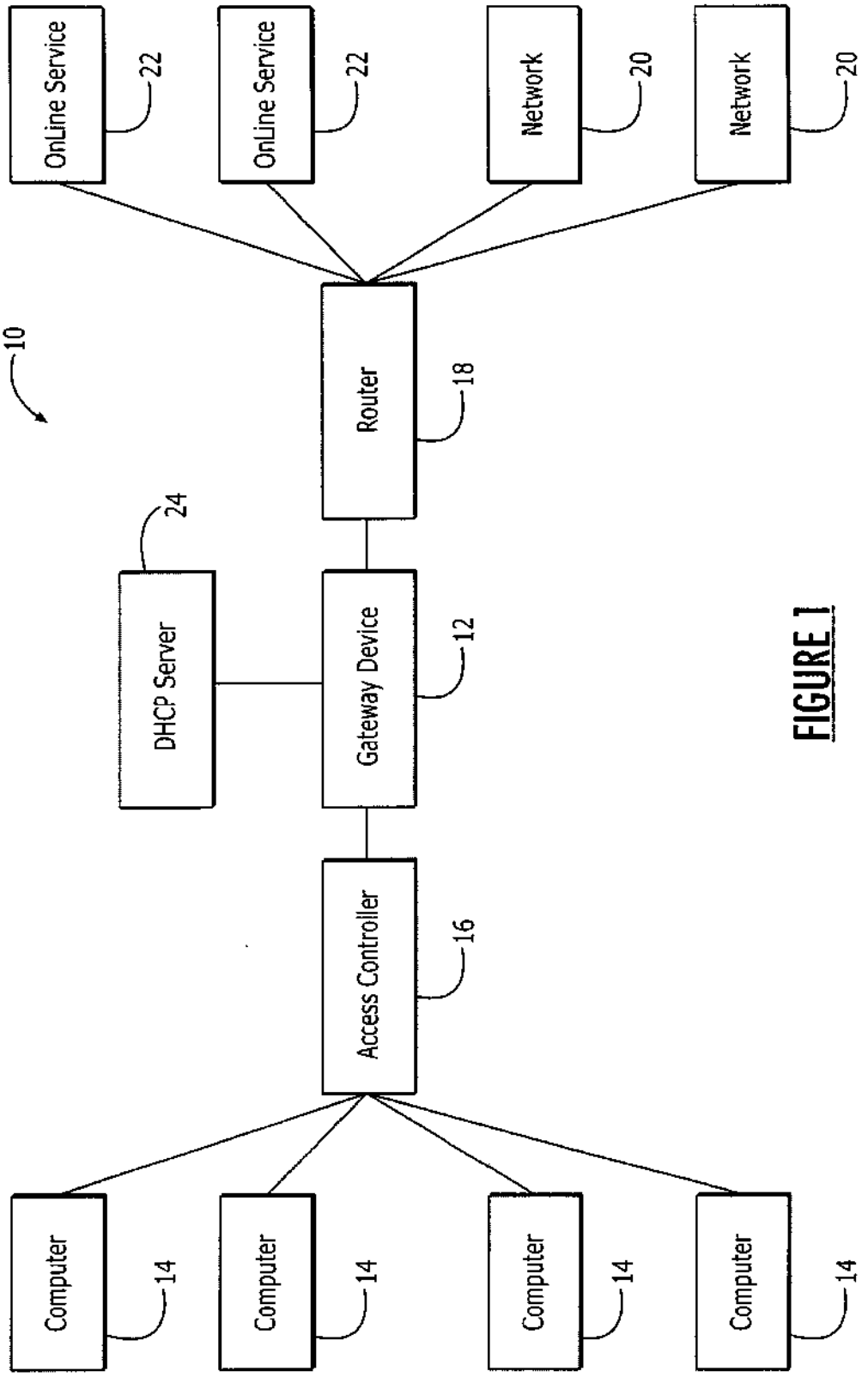

OnLine Service
22
OnLine Service
22
Network
20
Network
20
10
Router
18
DHCP Server
24
Gateway Device
12
Access Controller
16
Computer
14
Computer
14
Computer
14
Computer
14

FIGURE 1

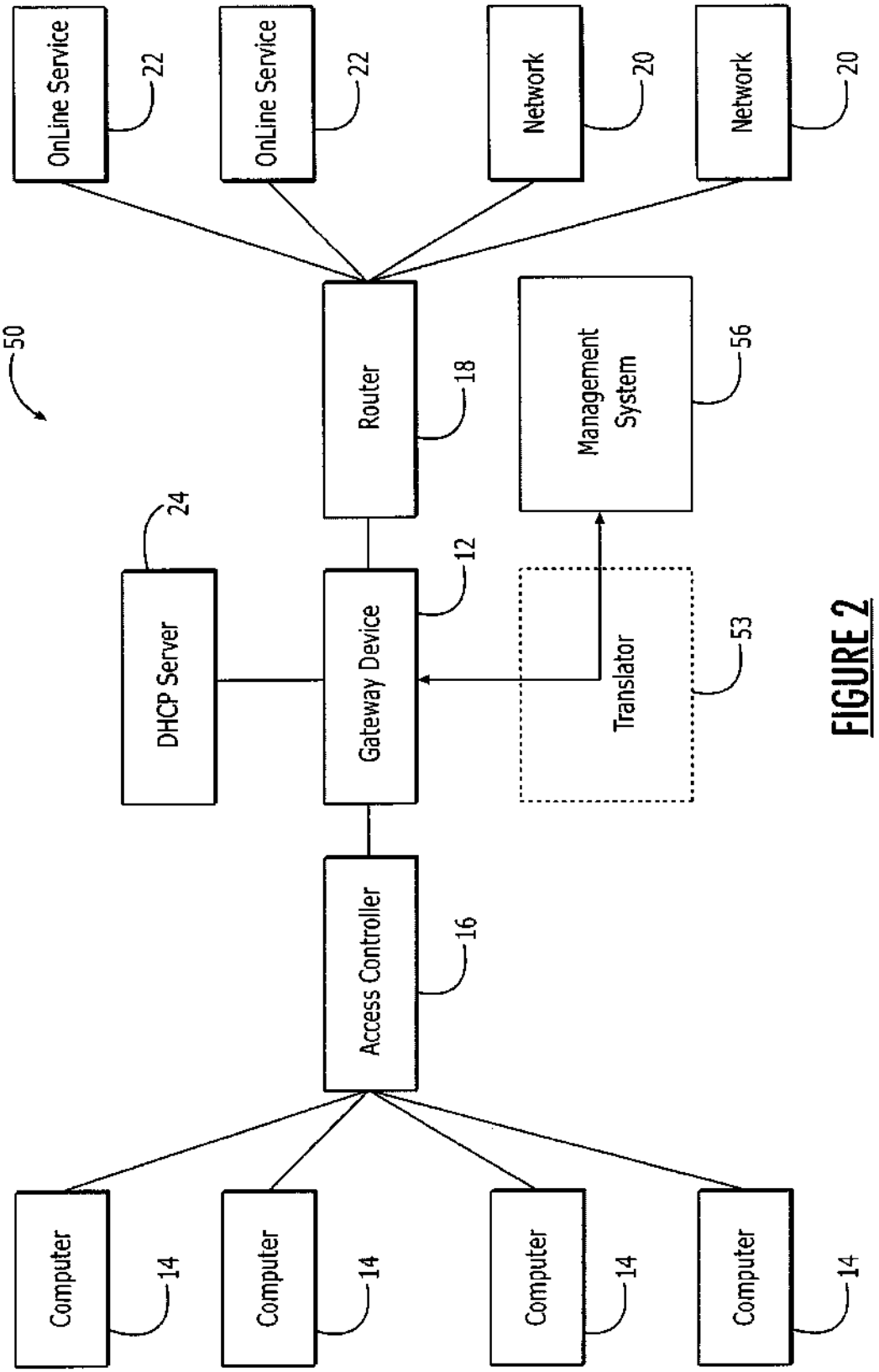

OnLine Service
22
OnLine Service
22
Network
20
Network
20
50
Router
18
Management System
56
24
DHCP Server
12
Gateway Device
Translator
53
Access Controller
16
Computer
14
Computer
14
Computer
14
Computer
14

FIGURE 2

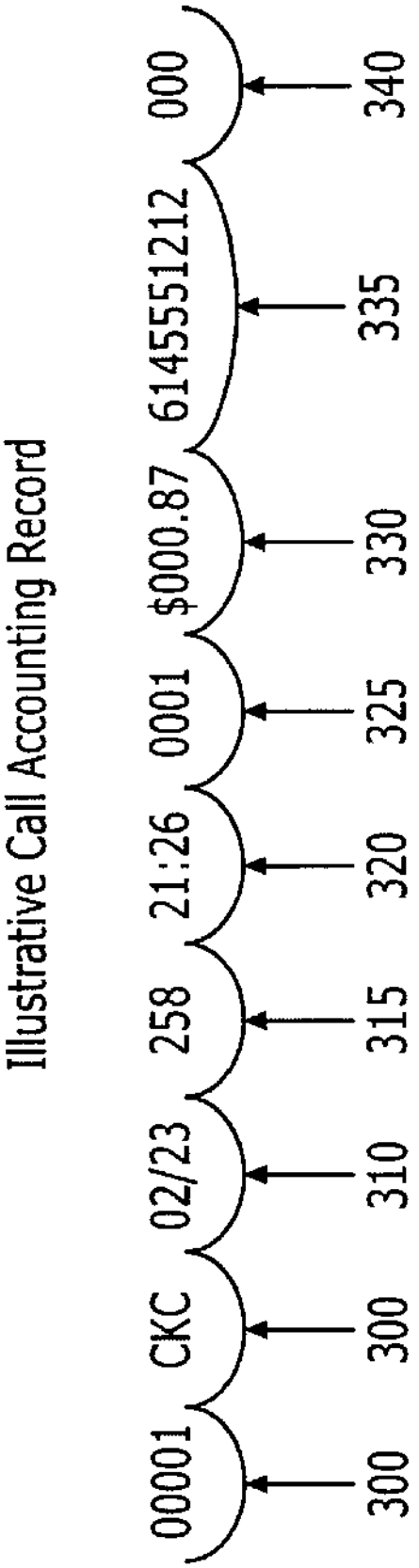

Illustrative Call Accounting Record
00001
300
CKC
300
02/23
310
258
315
21:26
320
0001
325
$000.87
330
6145551212
335
000
340

FIGURE 3

SYSTEMS AND METHODS FOR INTEGRATING A NETWORK GATEWAY DEVICE WITH MANAGEMENT SYSTEMS

CROSS-REFERENCE TO RELATED APPLICATIONS

The present invention claims priority from U.S. Provisional Application Ser. No. 60/160,973, filed Oct. 22, 1999, titled "Systems and Methods for Enabling Network Gateway Devices to Communicate with Management Systems to Facilitate Subscriber Management," U.S. Provisional Application Ser. No. 60/161,182, filed Oct. 22, 1999, entitled "Systems and Methods for Dynamic Bandwidth Management on a Per Subscriber Basis in a Computer Network," U.S. Provisional Application Ser. No. 60/161,139, filed Oct. 22, 1999, titled "Information And Control Console For Use With A Network Gateway Interface," U.S. Provisional Application Ser. No. 60/161,189, filed Oct. 22, 1999, titled "Systems and Methods for Transparent Computer Access and Communication with a Service Provider Network Using a Network Gateway Device," U.S. Provisional Application Ser. No. 60/161,181, filed Oct. 22, 1999, titled "Gateway Device Having an XML Interface and Associated Method," and U.S. Provisional Application Ser. No. 60/161,093, filed Oct. 22, 1999, titled "Location-Based Identification and Authorization for use With a Gateway Device," the contents of each of which are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to a network gateway device and, more particularly, to systems and methods for integrating one or more gateway devices with management systems.

BACKGROUND OF THE INVENTION

Through gateway devices or routers Internet Service Providers (ISPs) or enterprise network (such as a LANS) providers can permit a wide variety of users access to their networks and to other online services. Because high speed access to enterprise networks, the Internet and on-line services is a desirable commodity, like long distance telephone service, costs associated with the service are typically passed on to the remote user/subscriber. Therefore, in many instances the remote user/subscriber is concerned with being able to acquire network access and service in the most cost efficient and convenient manner.

In this regard, service concerns of subscribers accessing local networks through gateway devices parallel those concerns of customers utilizing internet service providers for conventional telephone line dial-up Internet access. In both cases, users typically want inexpensive, flexible and customer friendly service options. Correspondingly, a gateway device administrator desires the capability to be able to offer the user/subscriber numerous and different service and billing rate options, like those available in conventional dial-up internet access. For example, the remote user in a hotel environment may desire a subscription for only a day, or for the duration of their stay at the hotel. The user/subscriber may be charged on an hourly rate, a daily rate, a weekly rate, or at any other interval. Such flexible plans offer cost savings to consumers and are an attractive incentive to lure customers into buying access time to the enterprise network, online services or the internet.

Unlike conventional dial-up internet access, however, gateway devices permit remote users to access various

computer networks and on-line services without having a prior service contract or an ongoing relationship with the service provider. Therefore, unlike conventional dial up access plans, which can bill subscribers on a set monthly schedule, gateway devices make recouping remote access charges more challenging. This is especially true for nomadic users, who may utilize a remote connection to a network only once before relocating. Once the traveler has moved onward, the network provider may have difficulty in collecting any unpaid service charges. Furthermore, billing of nomadic users is another hurdle to fast and easy access to the enterprise network, on-line services and the internet. The benefits of remote plug and play access therefore may be overshadowed by time consuming payment methods. For example, where a user is required to complete an onerous billing procedure to pre-purchase local network time or to pay for the network use after each session, the user may decide not to use the network. Thus, any convenience provided by the computer network is superceded by the inconvenient billing method.

Gateway device administrators also desire convenient methods in which to bill users/subscribers. Because the gateway device enables subscribers immediate plug and play connections to computer networks, such as hotel or airport networks, the computer network provider and/or service provider of the high speed network would like to quickly and immediately bill the users/subscribers. This billing should be able to easily track a user/subscriber's usage of the network so as to recoup costs for the network hardware and network connection. Furthermore, such billing should be automated such that system administrators do not need to individually bill each user.

Therefore, it is desirable for customers, network providers and service providers to implement automatic billing through a gateway device utilizing a management system already used for billing customers. Such automatic billing utilizing the present invention to automatically send a billing record to a management system would benefit customers by facilitating fast and easy access, and also would benefit network providers who could appropriately charge customers for obtaining network or Internet access.

SUMMARY OF THE INVENTION

The present invention relates generally to a network gateway device and, more particularly, to network gateway devices communicating with management systems or servers, such as hotel property management systems, to facilitate subscriber management and billing.

According to one embodiment of the invention, there is provided a system for enabling a management system to communicate with a network gateway device in order to automatically bill a user for access to a computer network such as a local network or the Internet. The system includes a computer, and a network gateway device in communication with the computer for connecting the computer to a computer network and for maintaining data representative of the user's access to the computer network. The system also includes a management system connected to the network gateway device that is designed to automatically bill the user for network or Internet access, or services facilitated by the network access, such as room service, business services, and the like. The management system is also designed to communicate with a third party device according to at least one predetermined protocol. According to the present invention, the gateway device is therefore designed to supply billing data using one of the predetermined protocols supported by

the management system. As such, the management system receives the billing data supplied by the network gateway device and utilizes the data for automatic billing purposes.

Furthermore, in the system for enabling a management system to communicate with a network gateway device to bill a user for access to a computer network, the management system can be located within the computer network. Additionally, the system can include a translator in communication with the gateway device and management system for receiving the data supplied by the network gateway device. The translator can further reconfigure the supplied billing data received from the network gateway device, and can transmit the further reconfigured data to the management system. The data representative of the user's access to the computer network can include data representative of the user's location, access time, date which access was obtained, billing rate, and other pertinent information.

According to another embodiment of the invention, a method for enabling a remote server, such as an Internet website, to communicate with a network gateway device in order to automatically bill a customer via the management system such as a hotel's Property Management System.

According to yet another embodiment of the present invention, there is disclosed a system for integrating a gateway device with a management system, wherein the management system can activate communication with the gateway device. The system includes a computer, and a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device maintains data representative of the user's access to the computer network. The system further includes a management system connected to said network gateway device, wherein the management system receives the data representative of the user's access to the computer network, and wherein the management system initiates communication with the gateway device to manage the computer network.

According to one aspect of the invention, the management system communicates with the network gateway device in at least one predetermined protocol selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol. According to another aspect of the invention, the management system is a hotel property management system.

The ability to bill customers for service automatically and track customers without administrator intervention allows the local network service provisioning to be done economically, efficiently, and securely, as no administrator intervention is required. That is, the gateway device generates accounting records that are formatted and forwarded to the PMS to facilitate automatic billing. This automatic billing generates a bill that can be paid by a customer electronically (e.g., via the Internet), or at checkout of the hotel. Alternatively, a customer may have pre-purchased network access.

The present invention provides an: incentive for hotels, airports, and other computer networks to provide network connections to users because the computer network has a captive customer base. Furthermore, automatic billing can enable usage-based billing for network access and services, which is desirable to customers. Finally, automatic billing can reduce the risk of network use by an unauthorized user.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system including a gateway device facilitating communication between computers and networks or other online services, according to one embodiment of the invention.

FIG. **2** shows a block diagram of the computer system of FIG. **1**, including a gateway device integrated with a management system, according to one aspect of the invention.

FIG. **3** shows a call accounting record generated by the gateway device, according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, there is shown in block diagram form a computer system **10** including a plurality of computers **14** that can communicate with one or more online services **22** or networks via a gateway device **12** providing the interface between the computers **14** and the various networks **20** or online services **22**. One embodiment of such a gateway device has been described in U.S. patent application Ser. No. 08/816,174 and U.S. Provisional Application No. 60/111,497 (collectively referred to herein as the Gateway Device Applications), the contents of which are incorporated herein by reference. Briefly, the gateway device **12** facilitates transparent computer access to the online services **22** or networks **20**, such that the computers **14** can access any networks via the device **12** regardless of their network configurations. Additionally, the gateway device **12** includes the ability to recognize computers attempting to access a network **20**, the location of computers attempting to access a network, the identity of users attempting to gain network access, and additional attributes, as is discussed in the Gateway Device Applications.

As illustrated in FIG. **1**, the computer system **10** also includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end (a Cable Modem Termination Shelf (CMTS)) for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, an Ethernet switch or the like.

The computer system **10** further includes one or more routers **18** and/or servers (not shown in FIG. **1**) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks **20** or online services **22**. In this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of the

networks **20** or online services **22**, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. **1** may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**. Furthermore, additional elements may be included in the computer system **10**, such as elements disclosed in the Gateway Device Application, or network elements known to those of ordinary skill in the art.

FIG. **2** shows a block diagram of the computer system **50** of FIG. **1**, integrated with a management system **56**, according to one embodiment of the present invention. It will be appreciated by those of skill in the art that the embodiment shown in FIG. **2** is for illustrative purposes, and that the gateway device **12** may be integrated with virtually any network server or management system, such as computer networks used in corporate offices, airports, arenas, apartment complexes, office buildings or the like. As a result, the embodiment shown in FIG. **2** is for illustrative purposes only, and is not intended to limit the scope of the present invention.

According to one aspect of the invention, the gateway device **12** is in direct communication with the management system **56** through a serial connection **57**. Optionally, the gateway device **12** may be connected to the management system **56** through a translator **53**, illustrated with phantom lines to indicate that the translator **53** is not a required component of the management system **56**, as is explained in detail below. Because the gateway device **12** comprises similar components to the system illustrated in FIG. **1**, it will be appreciated that the systems can be implemented in like manners with like components. Furthermore, additional embodiments of the present invention discussed with respect to FIG. **1** and in the Gateway Device Applications may also be implemented in the system **56** shown in FIG. **2**.

As shown in FIG. **2**, each of the plurality of computers **14** is located in a different hotel room **60**, **70**, **80** and **90** to allow multiple guests to access the hotel's computer network. The computers **14** are connected to the access controller **16** through a communications port in each room using a communications device such as a DSL modem, an Ethernet card, a coaxial cable, or another well known communication device. Most preferably, the connection between the computers **14** and the access controller **16** is a high speed connection, so that the computers **14** can receive data as fast as the gateway device **12** can forward the data. The data transmitted from the gateway device **12** to the computers **14** may originate from any devices located within the computer system **50**, such as communications via the Internet.

Management systems **56** are typically implemented through the use of one or more conventional computers. It will be appreciated that management systems **56** may include any well known computer based systems implemented in hotels, airports, arenas or other venues to manage operations or network access. For instance, where the gateway device **12** is located in a corporate office the gateway device **12** may be in communication with one or more central servers to which all computers in the corporate office are connected. In the embodiment of FIG. **2**, the management system **56** can be a property management system located within a hotel. Typical hotel property management systems automate operations such as room reservations, room assignments, guest check-in and check-out, and other front desk activities. Furthermore, typical hotel property management systems maintain a log of telephone calls and telephone charges for each guest room, and are in communication with the Internet to facilitate on-line reservation systems.

Where the management system **56** is illustrative of a property management system in a hotel, the gateway device **12** is in communication with the management system **56** such that each user/subscriber's access and connection to the hotel network via the gateway device **12** can be monitored by the management system **56**. Typically, the gateway device **12** is connected via a serial connection **57**, Ethernet connection, or LAN to the management system **56**. According to one preferred embodiment the gateway device **12** is connected to the management system **56** via a serial interface. The connection may operate at a variety of baud rates, such as at 9,600 or 56,000 bits per second, or at much higher rates. The primary purpose for integrating the gateway device **12** with the management system **56** is to allow the hotel to bill each specific user/subscriber for their use and connection to the hotel's network or to automatically bill such use directly to the room from which access was obtained. As disclosed in detail in the Gateway Device Applications, the identity of a user or a location from which a user communicates with the network can be determined by the gateway device **12**. According to one aspect of the invention, a user will not be authorized access to networks **20** or online serves **22** until the user is authorized access. This may require a user to enter a user name and ID to identify the user, or may require registration (e.g., input of a credit card number) or pre-payment for use of the system. Furthermore, the user may be authenticated based upon the AAA process described in U.S. patent Application titled "Systems And Methods For Providing Dynamic Network Authorization, Authentication And Accounting," inventors Joel Short and Florence Pagan, the contents of which are incorporated herein by reference. As described in the application, the gateway device **12** can identify users based upon the user's computer, location, or computer from which access is requested.

The gateway device **12** can thus monitor and record information such as the identity of the user, the room from which the user obtained access, the amount of time that the user utilized the network, the cost of each network access, the time, date and duration of the network access, and other additional information. Through this integration, systems of the present invention offer user/subscribers of computer networks integrated with management systems convenient payment plans in which users do not have to pre-pay for network access or physically pay each time the network is accessed, and features, such as billing status, that are otherwise available only by directly accessing management systems.

Traditional hotel property management systems are configured to communicate with various third party systems, such as point of sale systems, PBX systems, pay per view systems, and credit card authorization servers through serial ports, modem communications, dedicated connections, or through other well known communication means. Such connections allow the management system **56** to function as a fully integrated system, which allows customers to use a variety of hotel resources while automatically being billed for each transaction. Hotel property management systems are generally configured to receive such communications because these third party systems are typically used in the vast majority of hotels. To receive data from each of these third party systems, management systems typically include software for communicating with the third party systems based upon the data protocol and data structure implemented by the management system. The software allows data from third party systems to be received and reconfigured, if necessary, so that the data is in a format appropriate to be

utilized by the management system. However, because typical management systems that are currently deployed are not designed to receive data from a gateway device **12**, the gateway device **12** can be designed to interface with the management system **56** without requiring additional programming of the management system software.

For instance, it will be appreciated by those of skill in the art that the information passed from the gateway device **12** to the management system **56** can be configured, in most respects, identical to information received by the management system **56** from a private branch telephone system (PBX), which are commonly utilized in hotels. PBX systems allow room to room, local and long distance telephone calls to be made by guests, and are typically connected to hotel property management systems to facilitate billing of hotel guests based upon the room in which the call is made. Charges for calls can then be paid by the guest upon checkout, automatically billed to the guest's credit card or automatically billed to the guest with room charges. Although the gateway device **12** may be configured to communicate with the management system **56** in the same manner as PBX systems, it will be appreciated that this configuration is not required by the present invention. However, such a configuration is preferred such that the gateway device can be integrated in existing hotels with minimum or no impact on the configuration of preexisting management system equipment. Because the gateway device **12** can communicate with management systems by any means well known to those of skill in the art for transmitting network access and usage data to management systems, it will be appreciated that the device **12** can be configured in any manner that results in the least significant impact on management systems or on the user or administrator.

Therefore, in a preferred embodiment the gateway device **12** of the present invention formats data such that the data has the same data protocol and data structure as that of a third party service, such as a PBX, that the management system **56** is designed to receive. The management system **56** is adapted to communicate using different protocols specific to different types of devices or third party systems. Thus, the gateway device **12** can masquerade as a PBX or another third party system. The gateway device **12** creates a data record corresponding to an individual user/subscriber's use of the computer system, including the user/subscriber's location (room number), access charge, and additional information, as discussed above. The gateway device **12** formats the data record to fit the proper format required by the property management system vendor. The data is then transmitted to the management system **56** using low level protocol format. Typically, such formats are well known to those of skill in the art of management system design. According to one embodiment of the invention, the gateway device **12** can format the data as a call accounting record (CAR), illustrated in FIG. **3**.

The CAR of FIG. **3** is in a standard PBX format that the gateway device **12** can modify as needed to conform to the format requested by the management system **56**. The CAR includes data representative of month/day **310**, extension/room **315**, time **320**, duration **325** (e.g., in minutes), charge **330**, phone number **335**, routing code **340**, and the like, as well as additional data **300** that may be necessary for accurate ordering, transmittal and/or reception of the call accounting record. It will be appreciated that additional formats containing similar data can also be generated by the gateway device **12** for transmission to the management system **56**. Because management systems can differ, each system utilizing different user interfaces, variables, and operating systems, the gateway device **12** should communicate data to the management system **56** using data formats acceptable to a large number of management systems. In this manner, the gateway device **12** may be compatible with a majority of property management systems. For example, the gateway device **12** may be compatible to operate with the most popular management systems and formats, such as Micros Fidelio (manufactured by MICROS Systems, Inc., Beltsville, Md.), HOBIC, Autoclerk (manufactured by AutoClerk, Inc., Lafayette, Calif.), and other well known systems and formats.

However, there are many different management system standards, none of which are universal and implemented in all property management systems. As a result, although the gateway device **12** can be configured to conform to a large number of differing management systems, the gateway device **12** is set up to communicate with the management system in which is integrated. Furthermore, it will be appreciated that although the gateway device **12** may include a number of configuration settings, the device may not be able to conform to some systems. As a result, a translator **53** may be optionally used to manipulate the data output by the gateway device **12** in such a manner as to allow the data to be utilized by the management system **56**. In one embodiment, the translator may comprise a Lodging Link II device (LL) (manufactured by Protocol Technologies, Inc., Scottsdale, Ariz.) to convert incoming data from the gateway device **12** to data acceptable to the property management system device, such as UHALL protocol. Additionally, the translator **53** may also be connected to one or more devices or systems in =communication with the property management system, such as the pay per view system or credit card authorization system, to format data output by any system or component having data protocols which differ from those of the management system **56**.

Additionally, according to one aspect of the invention, it should be appreciated that a gateway device **12** in located within a network may not have a relationship with a billing company, and as a result, the gateway device **12** may not obtain a CAR from a third party. In this instance, a management system **56** can rely on the gateway device **12** to create its own call accounting record that can be sent to a standard printer. The printed data (call accounting record generated by the gateway device **12**) can then be manually entered into the management system accounting records, such as a hotel/business accounting record, and thus added to the user's bill.

Because data may be transferred to the management system in a CAR format, data typically within such format must be altered to accurately reflect the computer network service being provided to the user/subscriber. For example, in PBX systems, CAR format usually includes the phone number to which a telephone call is being made. However, when a user/subscriber is obtaining access to the hotel network via the gateway device **12**, no telephone number is dialed or called. Therefore, when possible, data within the CAR format (i.e., telephone record), such as telephone numbers, may be replaced with a descriptive record that indicates some other data that the property management systems wishes to track or record. On the other hand, where the CAR records cannot be replaced, a mock field, such as a mock telephone number, may be included so that the property management system receives the entire record it is programmed to receive. Thereafter, the mock number is not utilized by the management system **56**. Additional problems may also exist, for example, where the management system

56 is not devised to support the normumeric ASCII characters typically transmitted by the gateway device **12**. In this situation, the gateway device can be configured to replace the ASCII characters with numeral designations.

Integrating the gateway device **12** with the management system **56** allows a user/subscriber's account to be billed directly to that user?s hotel bill in a like manner as telephone calls billed to a hotel room. For example, where the management system **56** receives data representing a user's access to the local system, from the gateway device **12** and as described in the Gateway Device Applications, the management system **56** can automatically bill the operator through the use of a credit card authorization system in communication with the management system **56**. It will be appreciated that this can be accomplished because the property management system can register network access, identified by the gateway device, in one or more fields existing or established in the management system **56**. For instance, the management system **56** can register network access as a long distance call, or can establish a special fee for such access and add the cost of that access to a customer's bill in the same manner as a long distance call. In this manner, the customer's payment can be fast, easy, automated and transparent to the user.

Additionally, once the data transmitted by the gateway device **12** is received by the management system **56**, the management system **56** can display the data using a management system **56** interface. Preferably, the data may be displayed in a easily readable and printable form to allow a user/subscriber to view a summary of access information. Moreover, the data should be accessible to the user/subscriber's accounting record. In this manner, charges due to network access may be automatically placed on a customer's pre-existing bill, such as a hotel bill. Where access is obtained at another location, such as at an airport, the airport system manager (i.e., equivalent to the hotel property management system in the above example) may automatically bill the customer, can automatically charge the customer's credit card, or can add the charges to an account which the customer maintains. In this regard, while the management system has primarily been described in conjunction with a hotel computer network, the management system can be utilized in a variety of other applications in which a user/subscriber obtains access to a computer network or other on-line service via a gateway device.

Although the invention has been described herein as using a gateway device to monitor and facilitate network access of a user, and to transmit accounting information to the management system, it will be appreciated that the gateway device **12** can also be used to account for a variety of charges incurred as a result of the user's interaction with online services **22** or networks **20**. For instance, a remote system can bill the user directly to the management system. This could occur, for instance, where the user orders goods or services online. In this event, the gateway device can add the charge directly to the user's account in the management system.

Additionally, although the management system has been discussed herein as receiving data from the gateway device, in a passive manner, the management system can additionally transmit information to the user or gateway device **12**. Therefore, the management system can activate communication with the gateway device **12** to aid in managing the computer network. For instance the management system may inform the gateway device **12** that a particular room or user should be allowed or denied access to the system **50**, or that a particular port should be turned on or off. Additionally, the management system may request information from the gateway device, such as whether or not a particular user is using the system. This request may be automated or facilitated by a network administrator. Therefore, it will be appreciated that the system **50** may operate both downstream (from the user/computer or network or online service to the management system) and upstream (from the management system to the user/computer or online service or network.)

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

That which is claimed:

1. A system for integrating a gateway device with a management system to automatically bill a user for access to a computer network, comprising:

a computer;

a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device communicates with the computer absent additional agents implemented by the computer and wherein the network gateway device maintains data representative of the user's access to the computer network; and

a management system connected to said network gateway device for automatically billing the user based upon usage of the computer network, wherein said management system is configured to communicate according to at least one predetermined protocol,

wherein the network gateway device formats the data into call accounting record format, and wherein said management system receives the data formatted by the network gateway device and utilizes the data formatted by the network gateway device for billing purposes.

2. The system of claim **1**, further comprising a translator in communication with the gateway device and management system for receiving the data reconfigured by the network gateway device, said translator adapted to further reconfigure the reconfigured data, and to transmit the further reconfigured data to the management system.

3. The system of claim **1**, wherein the data representative of the user's access to the computer network comprises data representative of the user's location.

4. The system of claim **1**, wherein said management system is a hotel property management system.

5. The system of claim **1**, wherein the management system stores data reconfigured by the network gateway device, and wherein at least some of said data is accessible by the computer.

6. A method for integrating a gateway device with a management system to automatically bill a customer for access to a computer network, comprising:

enabling a user to access, via a network gateway device, a computer network absent additional agents implemented by a user's computer;

collecting data corresponding to the user's access to said computer network in said network gateway device;

reconfiguring said data into call accounting record format; and

transmitting the reconfigured data to the management system.

7. The method of claim **6**, further comprising providing a translator for reconfiguring said data and transmitting said reconfigured data to the management system.

8. The method of claim **6**, wherein transmitting the reconfigured data to the management system includes transmitting the reconfigured data to a hotel property management system.

9. The method of claim **6**, further comprising storing said reconfigured data at the management system, wherein at least some of said reconfigured data is accessible by said user.

10. A system for integrating a gateway device with a management billing system, wherein the billing system can activate communication with the gateway device, comprising:

a computer;

a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device communicates with the computer absent additional agents implemented by the computer and wherein the network gateway device maintains data representative of the user's physical location and the user's access to the computer network; and

a management billing system connected to said network gateway device, wherein the management system receives the data representative of the user's access to the computer network, and wherein the management system initiates communication with the gateway device to control a user's access to the computer network and a physical location's access to the computer network.

11. The system of claim **10**, wherein the management system communicates with the network gateway device in at least one predetermined protocol selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol.

12. The system of claim **10**, wherein said management system is a hotel property management system.

13. A system for integrating a gateway device with a management system to automatically bill a user for access to a computer network, comprising:

a computer;

a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device communicates with the computer absent additional agents implemented by the computer and wherein the network gateway device maintains data representative of the user's physical location and usage of the computer network; and

a management system connected to said network gateway device for automatically billing the user based upon the physical location of the user and the usage of the computer network, wherein said management system is configured to communicate according to at least one predetermined protocol,

wherein the network gateway device formats the data to meet one of the predetermined protocols supported by said management system, and wherein said management system receives the data formatted by the network gateway device and utilizes the data formatted by the network gateway device, including the physical location of the user and the user's network usage, for billing purposes.

14. The system of claim **13**, further comprising a translator in communication with the gateway device and management system for receiving the data reconfigured by the network gateway device, said translator adapted to further reconfigure the reconfigured data, and to transmit the further reconfigured data to the management system.

15. The system of claim **13**, wherein the at least one predetermined protocol is selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol.

16. The system of claim **13**, wherein said management system is a hotel property management system.

17. The system of claim **13**, wherein the management system stores data reconfigured by the network gateway device, and wherein at least some of said data is accessible by the computer.

18. A method for integrating a gateway device with a management system to automatically bill a customer for access to a computer network, comprising:

enabling a user to access, via a network gateway device, a computer network, absent additional agents implemented by a user's computer;

collecting data corresponding to the user's access to said computer network, including a physical location of the user and the user's network usage, in said network gateway device;

reconfiguring said data to one of the predetermined data formats which may be received by a management system; and

transmitting the reconfigured data to the management system.

19. The method of claim **18**, further comprising providing a translator for reconfiguring said data and transmitting said reconfigured data to the management system.

20. The method of claim **18**, wherein reconfiguring said data comprises reconfiguring said data to one of said predetermined formats selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol.

21. The method of claim **18**, wherein transmitting the reconfigured data to the management system includes transmitting the reconfigured data to a hotel property management system.

* * * * *

US006857009B1

(12) **United States Patent**
Ferreria et al.

(10) **Patent No.: US 6,857,009 B1**
(45) **Date of Patent: Feb. 15, 2005**

(54) **SYSTEM AND METHOD FOR NETWORK ACCESS WITHOUT RECONFIGURATION**

(75) Inventors: **Manuel Ferreria**, Los Angeles, CA (US); **Barry R. Robbins**, San Diego, CA (US); **Ken Caswell**, Santa Monica, CA (US); **Joel E. Short**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 823 days.

(21) Appl. No.: **09/694,577**

(22) Filed: **Oct. 23, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/161,138, filed on Oct. 22, 1999.

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/219**; 370/401; 370/475; 709/245; 709/224; 709/206; 709/223; 714/57; 713/200

(58) **Field of Search** 709/219, 223, 709/224, 246, 200; 370/401, 475; 714/57

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,309,437 A		5/1994	Perlman	
5,412,654 A		5/1995	Perkins	
5,539,736 A		7/1996	Johnson	
5,557,748 A		9/1996	Norris	
5,586,269 A		12/1996	Kubo	
5,724,355 A		3/1998	Bruno et al.	
5,793,763 A		8/1998	Mayes	
5,822,526 A	*	10/1998	Waskiewicz	709/206
5,909,549 A		6/1999	Compliment	
6,012,088 A		1/2000	Li	
6,070,187 A		5/2000	Subramaniam et al.	
6,128,739 A	*	10/2000	Fleming, III	713/200
6,130,892 A	*	10/2000	Short et al.	370/401
6,134,680 A	*	10/2000	Yeomans	714/57
6,182,141 B1		1/2001	Blum et al.	
6,212,560 B1		4/2001	Fairchild	
6,425,003 B1	*	7/2002	Herzog et al.	709/223
6,434,627 B1	*	8/2002	Millet et al.	709/245
6,591,306 B1	*	7/2003	Redlich	709/245
6,618,398 B1	*	9/2003	Marchetti et al.	370/475
6,675,208 B1	*	1/2004	Rai et al.	709/224
6,691,227 B1	*	2/2004	Gopal et al.	713/162
6,742,036 B1	*	5/2004	Das et al.	709/226

OTHER PUBLICATIONS

Hierarchical admission control scheme for supporting mobility in mobile IP Ki–Il Kim; Sang–Ha Kim; Jung–Mo Moon; Yeong–Jin Kim. MILCOM 2002. Proceedings, vol. 1, Iss., Oct. 7–10, 2002 pp. 431–435 vol. 1.*

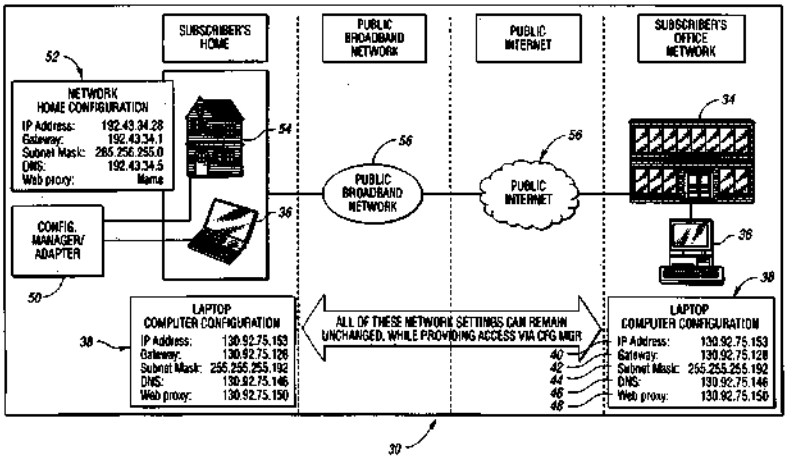
(List continued on next page.)

Primary Examiner—Saleh Najjar
Assistant Examiner—Uzma Alam
(74) *Attorney, Agent, or Firm*—Brooks Kushman P.C.

(57) **ABSTRACT**

A system and method for providing connectivity to a foreign network for a device configured for communication over a home network without reconfiguring the device include intercepting packets transmitted by the device, selectively modifying intercepted packets which are incompatible with the foreign network to be compatible with network settings of the foreign network, and selectively providing network services for the device corresponding to network services available on the home network to reduce the delay associated with accessing the network services from the foreign network, or to provide network services otherwise inaccessible from the foreign network. Network services are provided by or through a configuration adapter connected to the device or to the foreign network. The configuration adapter accommodates incompatibilities resulting from proxy server requests, domain name server requests, and/or outgoing email service requests to provide transparent network access for mobile users without reconfiguration of the users computing device.

35 Claims, 20 Drawing Sheets



OTHER PUBLICATIONS

Mobile Networks and Applications. Perkins, Charles E. vol. 3, Issue 4 1999. Special issue: mobile networking in the Internet pp. 319–334 Year of Publication: 1998 ISSN:1383–469X. Kluwer Academic Publishers Hingham, MA.*

International Conference on Mobile Computing and Networking. Zhao, Xinhua; Castelluccia, Claude; Baker, Mary. Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. pp. 145–156. ACM Press New York,NY;1998.*

"Provisioning Server", Cable Access: Provisioning Server, www.northnetworks.com (Oct. 14, 1999).

"Linux IP Masquerade Resource", Limus IP Masquerade Recourse, www.wiznet.ca (Sep. 30, 1999).

"Implementing an Intelligent Service Gateway Architecture", RedBack Networks.

"The Subscriber Management System", The Catalyst for DSL Deployment, RedBack Networks.

"Strengths of the Redback Subscriber Management System", RedBack Networks (© 1999 Redback Networks).

"Implementing a Cost–Effective, Highly–Scalable DSL Service", RedBack Networks.

"PPP Over Ethernet", A Comparison of Alternatives for PC–to xDSL Modem Connectivity, RedBack Networks (Revised 9/98).

"Leveraging Subscriber Management to Empower Data over Cable Networks", RedBack Networks (Apr., 1999).

"Windows 2000 Server Operating System", Plug and Play Networking with Microsoft Automatic Private IP Addressing (201 1996 Microsoft Corp.).

"IBM Research Report", TCP Splicing for Application Layer Proxy Performance, Computer Science/Mathematics RC 21139 (Mar. 17, 1998).

"IBM Research Report", Impriving HTTP Caching Proxy Performance with TCP Tap, Computer Science/Mathematics, RC 21147 (Mar. 26, 1998).

"Introduction", www.suse.de. (Oct. 18, 1999) 1 pg.

"History", www.suse.de (Oct. 18, 1999) 3 pages.

"NAT and Networks", www.suse.de (Oct. 18, 1999) 12 pgs.

"Virtualizing the Network", www.suse.de (18/18/99) 2 pgs.

"Example Implementation", www.suse.de (18/18/99) 7 pgs.

"Using NAT", www.suse.de (18/18/99) 12 pgs.

David A. Maltz, "MSOCKS: An Architecture for Transport Layer Mobility", Carnegie Mellon Univ.

"SOCKS V5", www.socks.nec.com (Oct. 21, 1999) 3 pgs.

"SOCKS Protocol Version 5", www.socks.nec.com (10/21/99) 7 pgs.

"SOCKS 4A: A Simple Extension to Socks 4 Protocol", www.socks.nec.com (10/21/99) 1 pg.

"SOCKS: A Protocol for TCP Proxy Across Firewalls", www.socks.nec.com (Oct. 21, 1999) 3 pgs.

"Introduction to Socks", www.socks.nec.com (Oct. 21, 1999) 3 pgs.

David B. Johnson & David A Maltz, "Protocols for Adaptive Wireless and Mobile Networking" IEEE Personal Communications (Feb. 1996).

"SQUID Frequently Asked . . . About Squid, this FAX, and other Squid Information Resource", www.squid.nlanr.net (18/18/99) 6 pgs.

"SQUID Frequently Asked Questions: Communication Between Browsers and Squid", www.squid.nlanr.net (18/18/99) 6 pgs.

"SQUID Frequently Asked Questions: How does Squid Work?", www.squid.nlanr.net (Oct. 18, 1999) 11 pgs.

* cited by examiner

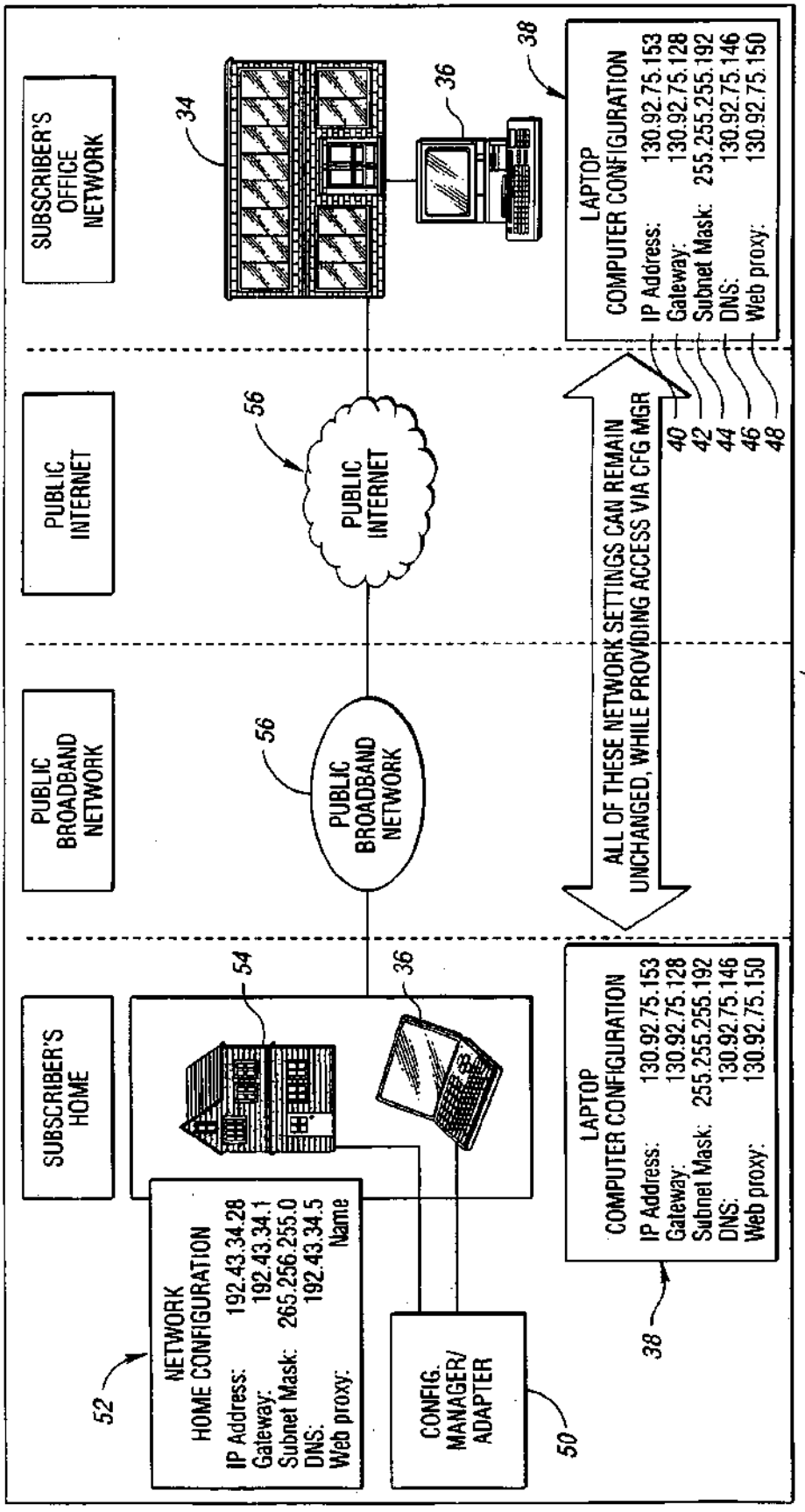

SUBSCRIBER'S OFFICE NETWORK
PUBLIC INTERNET
PUBLIC BROADBAND NETWORK
SUBSCRIBER'S HOME
34
36
38
LAPTOP COMPUTER CONFIGURATION
IP Address: 130.92.75.153
Gateway: 130.92.75.128
Subnet Mask: 255.255.255.192
DNS: 130.92.75.146
Web proxy: 130.92.75.150
56
PUBLIC INTERNET
PUBLIC BROADBAND NETWORK
ALL OF THESE NETWORK SETTINGS CAN REMAIN UNCHANGED, WHILE PROVIDING ACCESS VIA CFG MGR
40
42
44
46
48
30
54
36
NETWORK HOME CONFIGURATION
IP Address: 192.43.34.28
Gateway: 192.43.34.1
Subnet Mask: 265.256.255.0
DNS: 192.43.34.5
Web proxy: Name
52
CONFIG. MANAGER/ ADAPTER
50
LAPTOP COMPUTER CONFIGURATION
IP Address: 130.92.75.153
Gateway: 130.92.75.128
Subnet Mask: 255.255.255.192
DNS: 130.92.75.146
Web proxy: 130.92.75.150
38

Fig. 1

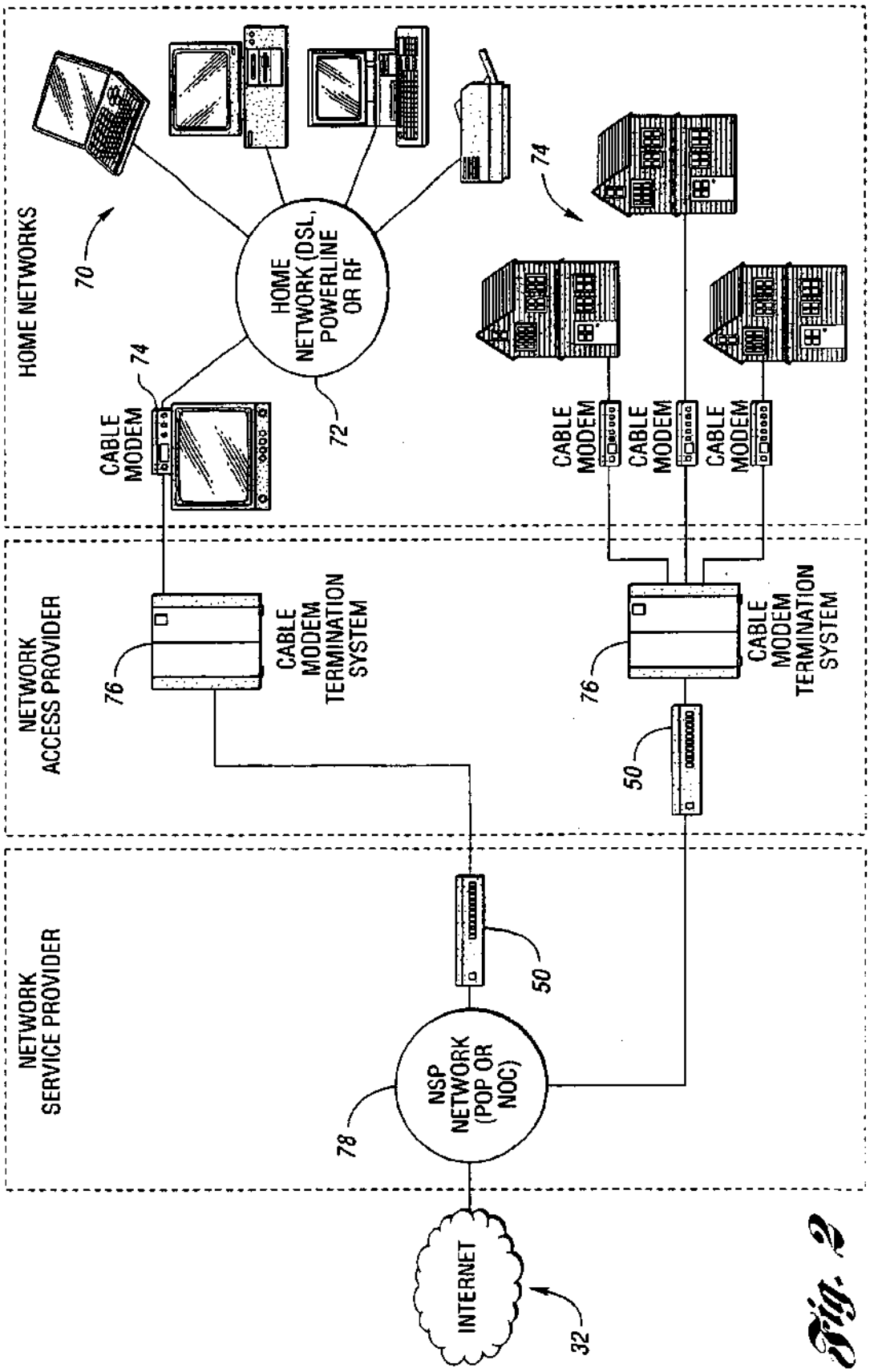

HOME NETWORKS
70
HOME NETWORK (DSL, POWERLINE OR RF
72
74
CABLE MODEM
74
CABLE MODEM
CABLE MODEM
CABLE MODEM
NETWORK ACCESS PROVIDER
76
CABLE MODEM TERMINATION SYSTEM
76
CABLE MODEM TERMINATION SYSTEM
50
50
NETWORK SERVICE PROVIDER
NSP NETWORK (POP OR NOC)
78
INTERNET
32

Fig. 2

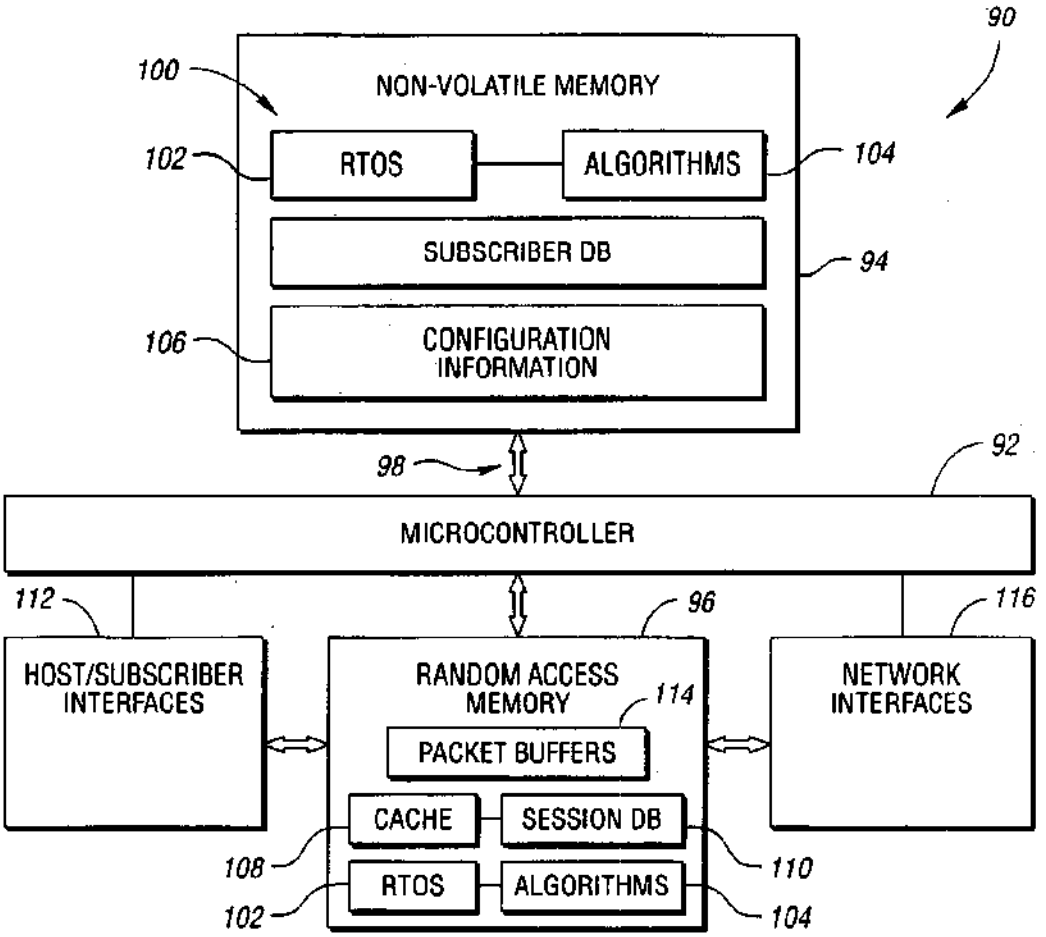

90
100
NON-VOLATILE MEMORY
102
RTOS
ALGORITHMS
104
SUBSCRIBER DB
94
106
CONFIGURATION INFORMATION
98
92
MICROCONTROLLER
112
96
116
HOST/SUBSCRIBER INTERFACES
RANDOM ACCESS MEMORY
114
PACKET BUFFERS
NETWORK INTERFACES
CACHE
SESSION DB
108
110
RTOS
ALGORITHMS
102
104

Fig. 3

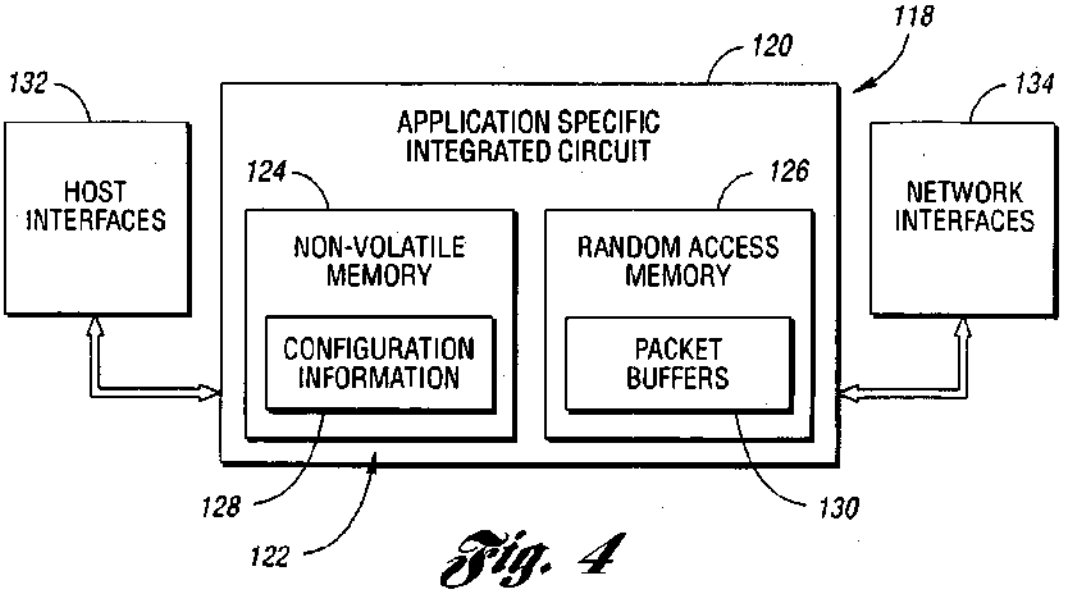

118
120
132
134
APPLICATION SPECIFIC INTEGRATED CIRCUIT
HOST INTERFACES
124
126
NON-VOLATILE MEMORY
RANDOM ACCESS MEMORY
NETWORK INTERFACES
CONFIGURATION INFORMATION
PACKET BUFFERS
128
130
122

Fig. 4

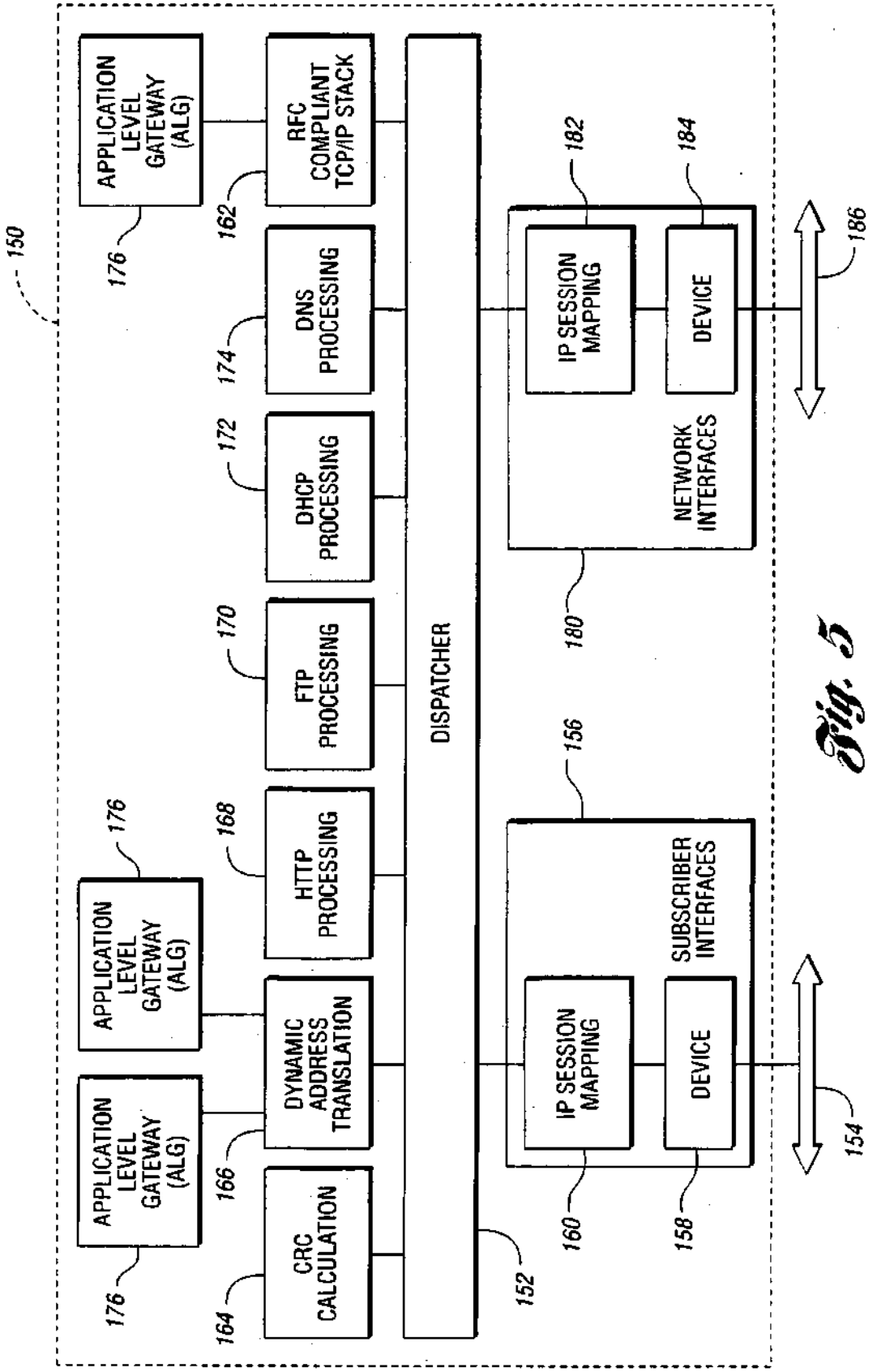

150
APPLICATION LEVEL GATEWAY (ALG)
176
RFC COMPLIANT TCP/IP STACK
162
DNS PROCESSING
174
DHCP PROCESSING
172
FTP PROCESSING
170
HTTP PROCESSING
168
DYNAMIC ADDRESS TRANSLATION
166
CRC CALCULATION
164
DISPATCHER
152
IP SESSION MAPPING
160
DEVICE
158
SUBSCRIBER INTERFACES
156
154
IP SESSION MAPPING
182
DEVICE
184
NETWORK INTERFACES
180
186

Fig. 5

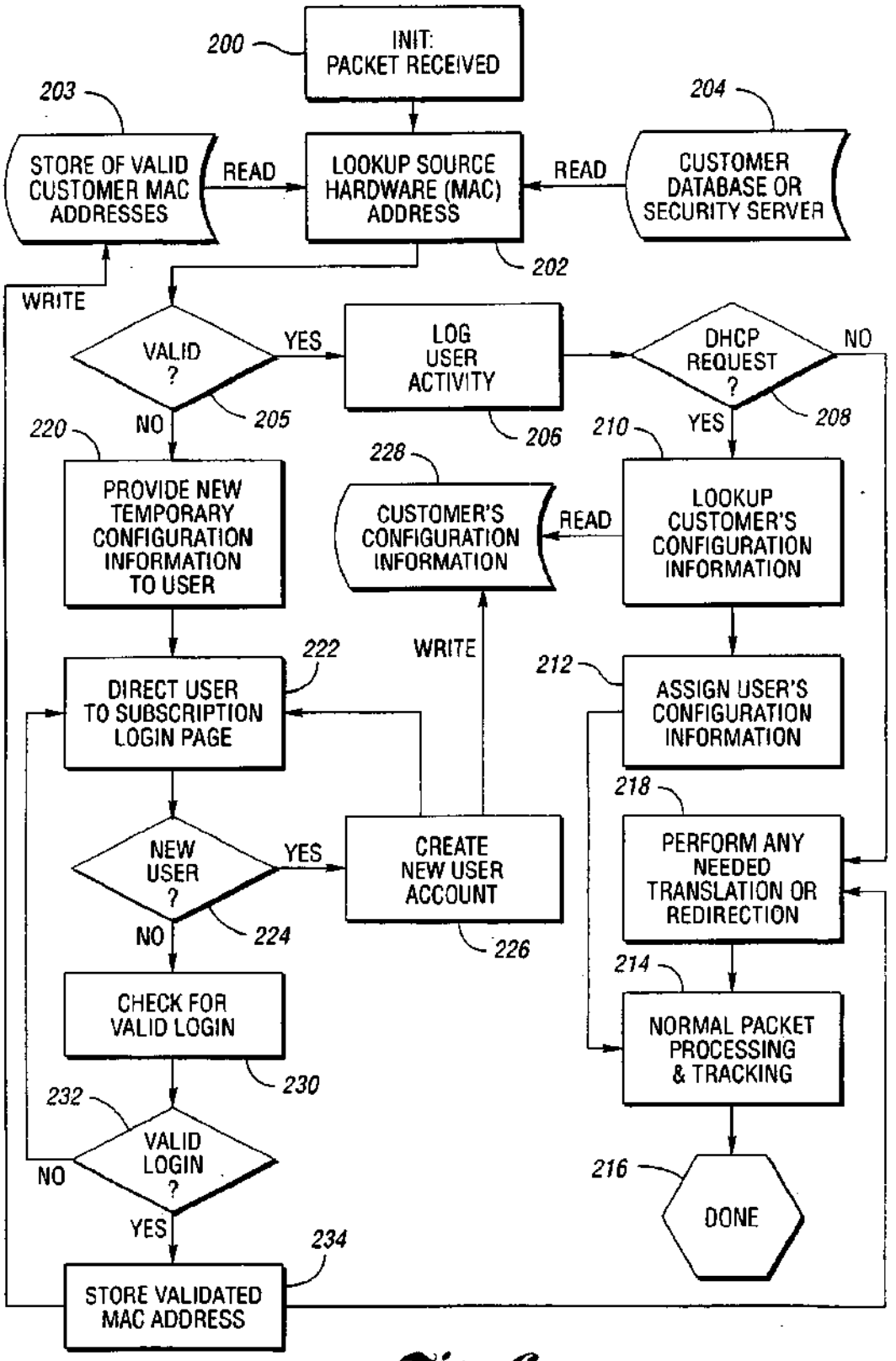

200
INIT: PACKET RECEIVED
203
STORE OF VALID CUSTOMER MAC ADDRESSES
READ
LOOKUP SOURCE HARDWARE (MAC) ADDRESS
READ
204
CUSTOMER DATABASE OR SECURITY SERVER
202
WRITE
VALID ?
YES
205
LOG USER ACTIVITY
206
DHCP REQUEST ?
NO
208
YES
220
NO
PROVIDE NEW TEMPORARY CONFIGURATION INFORMATION TO USER
228
CUSTOMER'S CONFIGURATION INFORMATION
READ
210
LOOKUP CUSTOMER'S CONFIGURATION INFORMATION
222
DIRECT USER TO SUBSCRIPTION LOGIN PAGE
WRITE
212
ASSIGN USER'S CONFIGURATION INFORMATION
218
NEW USER ?
YES
CREATE NEW USER ACCOUNT
226
PERFORM ANY NEEDED TRANSLATION OR REDIRECTION
224
NO
214
CHECK FOR VALID LOGIN
230
NORMAL PACKET PROCESSING & TRACKING
232
VALID LOGIN ?
NO
YES
216
DONE
234
STORE VALIDATED MAC ADDRESS

Fig. 6

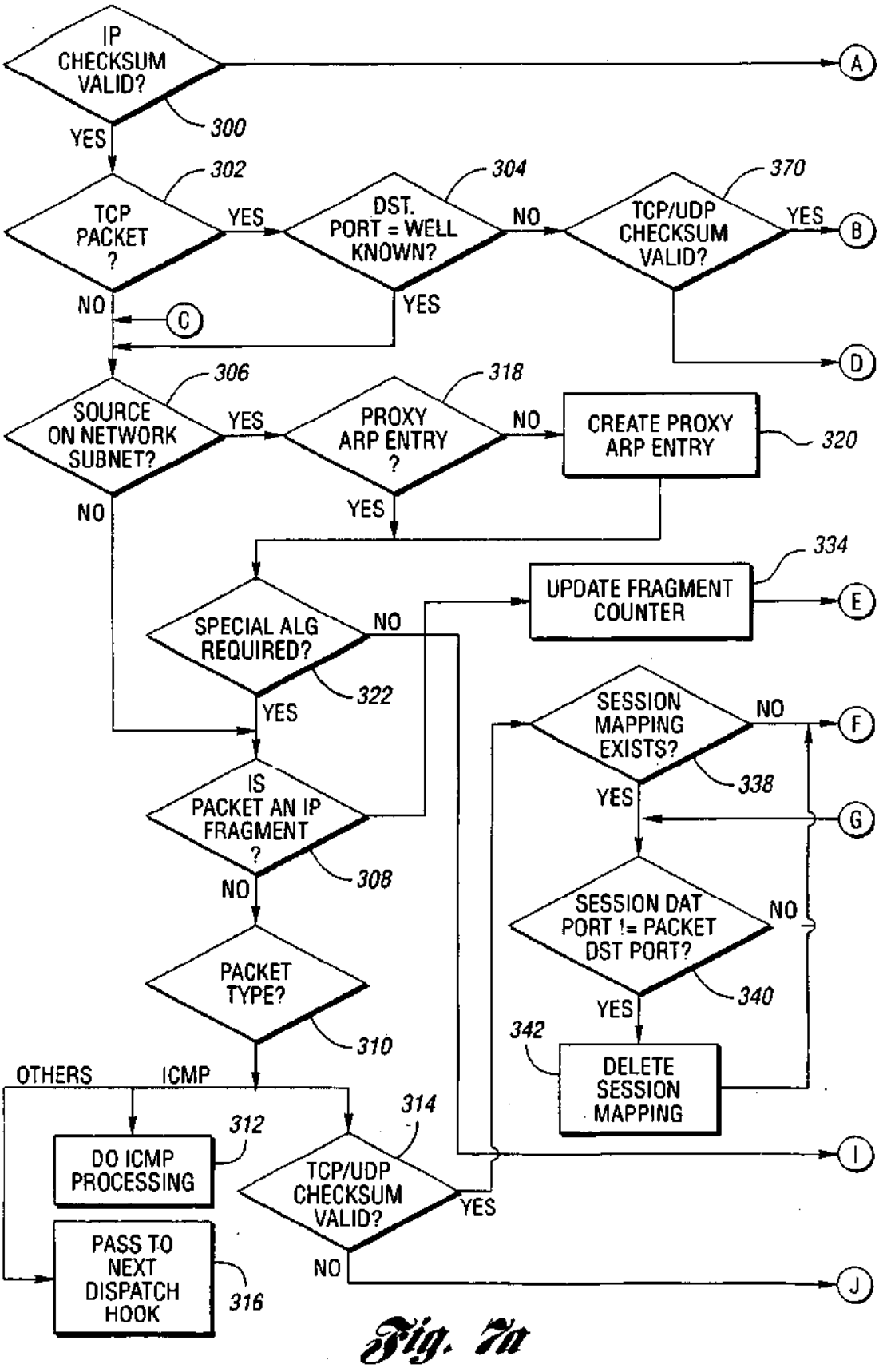

IP CHECKSUM VALID?
300
YES
A
TCP PACKET ?
302
YES
DST. PORT = WELL KNOWN?
304
NO
TCP/UDP CHECKSUM VALID?
370
YES
B
NO
C
YES
D
SOURCE ON NETWORK SUBNET?
306
YES
PROXY ARP ENTRY ?
318
NO
CREATE PROXY ARP ENTRY
320
NO
YES
SPECIAL ALG REQUIRED?
NO
UPDATE FRAGMENT COUNTER
334
E
322
YES
IS PACKET AN IP FRAGMENT ?
308
NO
PACKET TYPE?
310
OTHERS
ICMP
DO ICMP PROCESSING
312
PASS TO NEXT DISPATCH HOOK
316
TCP/UDP CHECKSUM VALID?
314
YES
NO
I
J
SESSION MAPPING EXISTS?
NO
F
338
YES
G
SESSION DAT PORT != PACKET DST PORT?
NO
340
YES
342
DELETE SESSION MAPPING

Fig. 7a

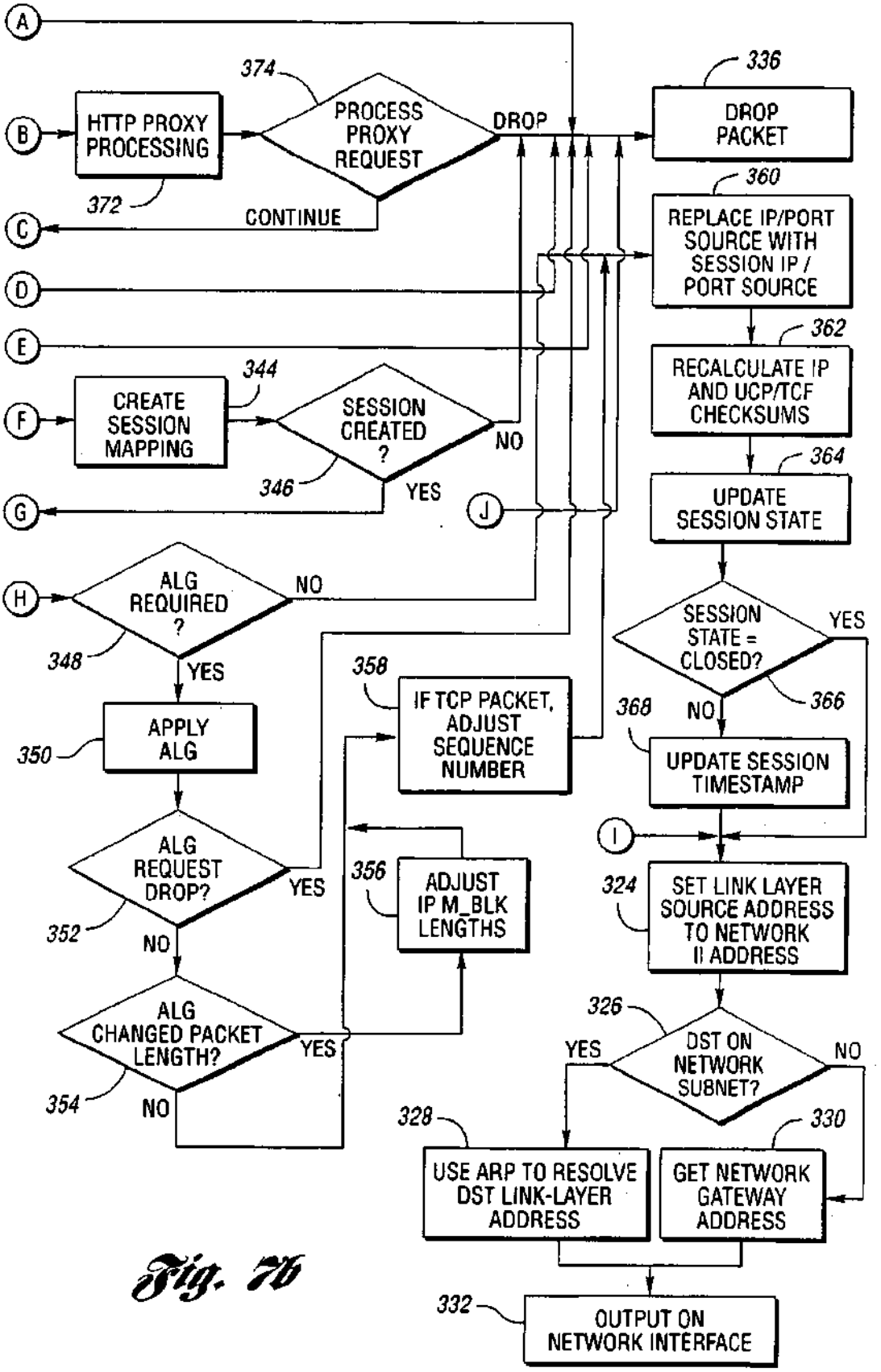

A
B
C
D
E
F
G
H
I
J
HTTP PROXY PROCESSING
372
374
PROCESS PROXY REQUEST
DROP
CONTINUE
336
DROP PACKET
360
REPLACE IP/PORT SOURCE WITH SESSION IP / PORT SOURCE
362
RECALCULATE IP AND UCP/TCF CHECKSUMS
364
UPDATE SESSION STATE
CREATE SESSION MAPPING
344
SESSION CREATED ?
346
NO
YES
ALG REQUIRED ?
348
NO
YES
APPLY ALG
350
ALG REQUEST DROP?
352
YES
NO
ALG CHANGED PACKET LENGTH?
354
YES
NO
358
IF TCP PACKET, ADJUST SEQUENCE NUMBER
356
ADJUST IP M_BLK LENGTHS
SESSION STATE = CLOSED?
366
YES
NO
368
UPDATE SESSION TIMESTAMP
324
SET LINK LAYER SOURCE ADDRESS TO NETWORK II ADDRESS
326
DST ON NETWORK SUBNET?
YES
NO
328
USE ARP TO RESOLVE DST LINK-LAYER ADDRESS
330
GET NETWORK GATEWAY ADDRESS
332
OUTPUT ON NETWORK INTERFACE

Fig. 7b

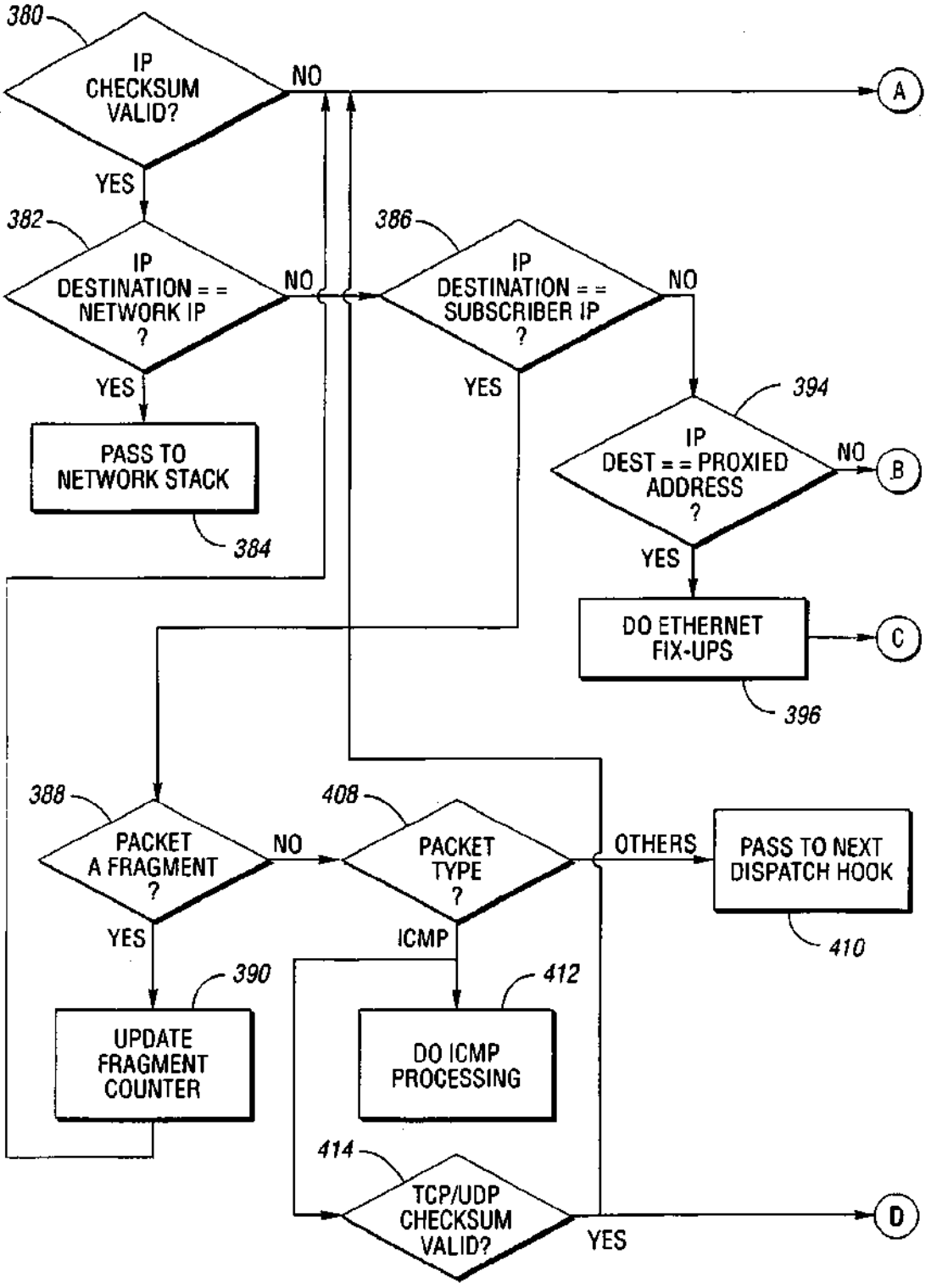

380
IP CHECKSUM VALID?
NO
A
YES
382
IP DESTINATION = = NETWORK IP ?
NO
386
IP DESTINATION = = SUBSCRIBER IP ?
NO
YES
YES
PASS TO NETWORK STACK
384
394
IP DEST = = PROXIED ADDRESS ?
NO
B
YES
DO ETHERNET FIX-UPS
C
396
388
PACKET A FRAGMENT ?
NO
408
PACKET TYPE ?
OTHERS
PASS TO NEXT DISPATCH HOOK
410
YES
ICMP
390
UPDATE FRAGMENT COUNTER
412
DO ICMP PROCESSING
414
TCP/UDP CHECKSUM VALID?
YES
D

Fig. 8a

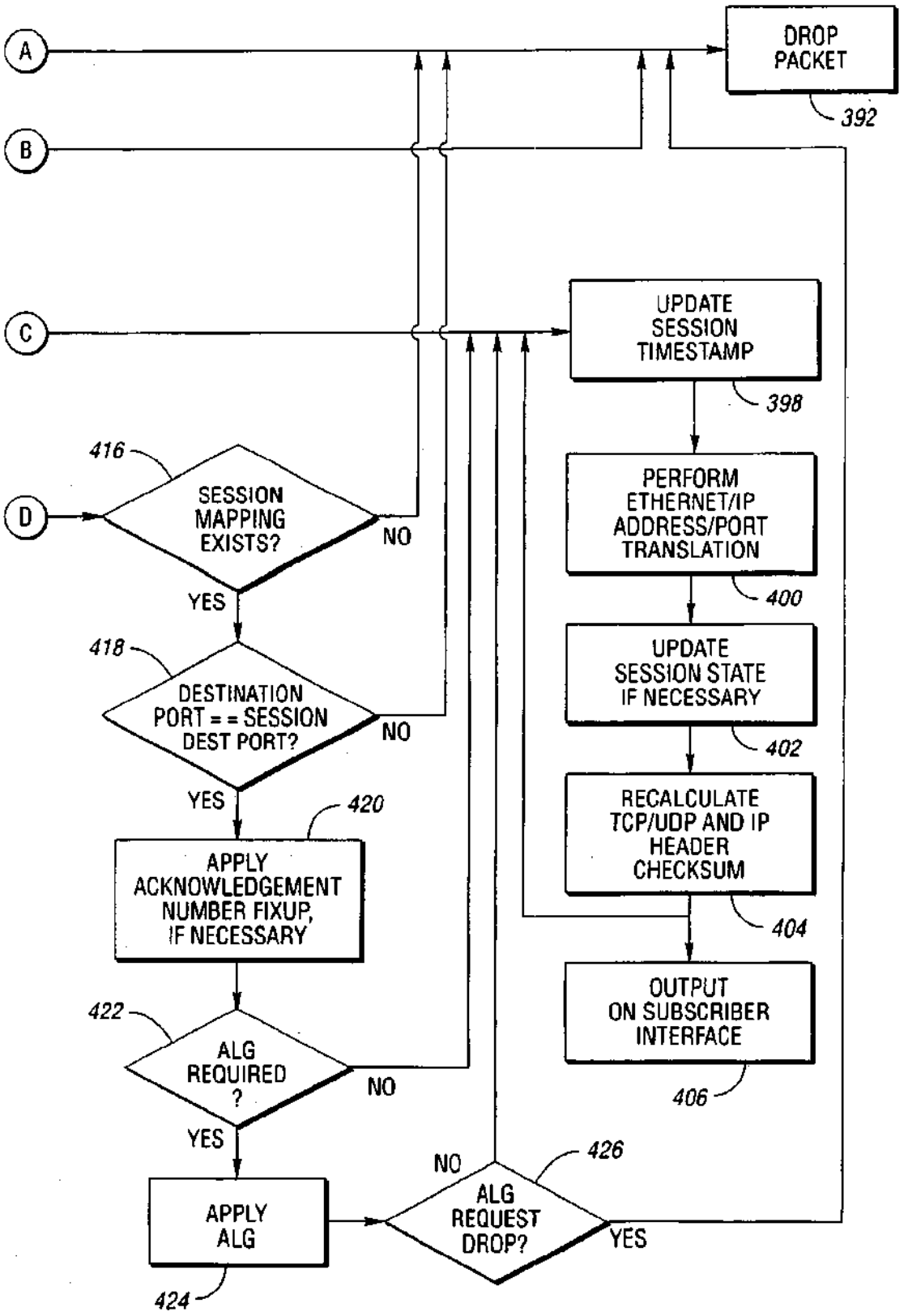

A
B
C
D
DROP PACKET
392
UPDATE SESSION TIMESTAMP
398
PERFORM ETHERNET/IP ADDRESS/PORT TRANSLATION
400
UPDATE SESSION STATE IF NECESSARY
402
RECALCULATE TCP/UDP AND IP HEADER CHECKSUM
404
OUTPUT ON SUBSCRIBER INTERFACE
406
416
SESSION MAPPING EXISTS?
NO
YES
418
DESTINATION PORT = = SESSION DEST PORT?
NO
YES
420
APPLY ACKNOWLEDGEMENT NUMBER FIXUP, IF NECESSARY
422
ALG REQUIRED ?
NO
YES
APPLY ALG
424
NO
426
ALG REQUEST DROP?
YES

Fig. 8b

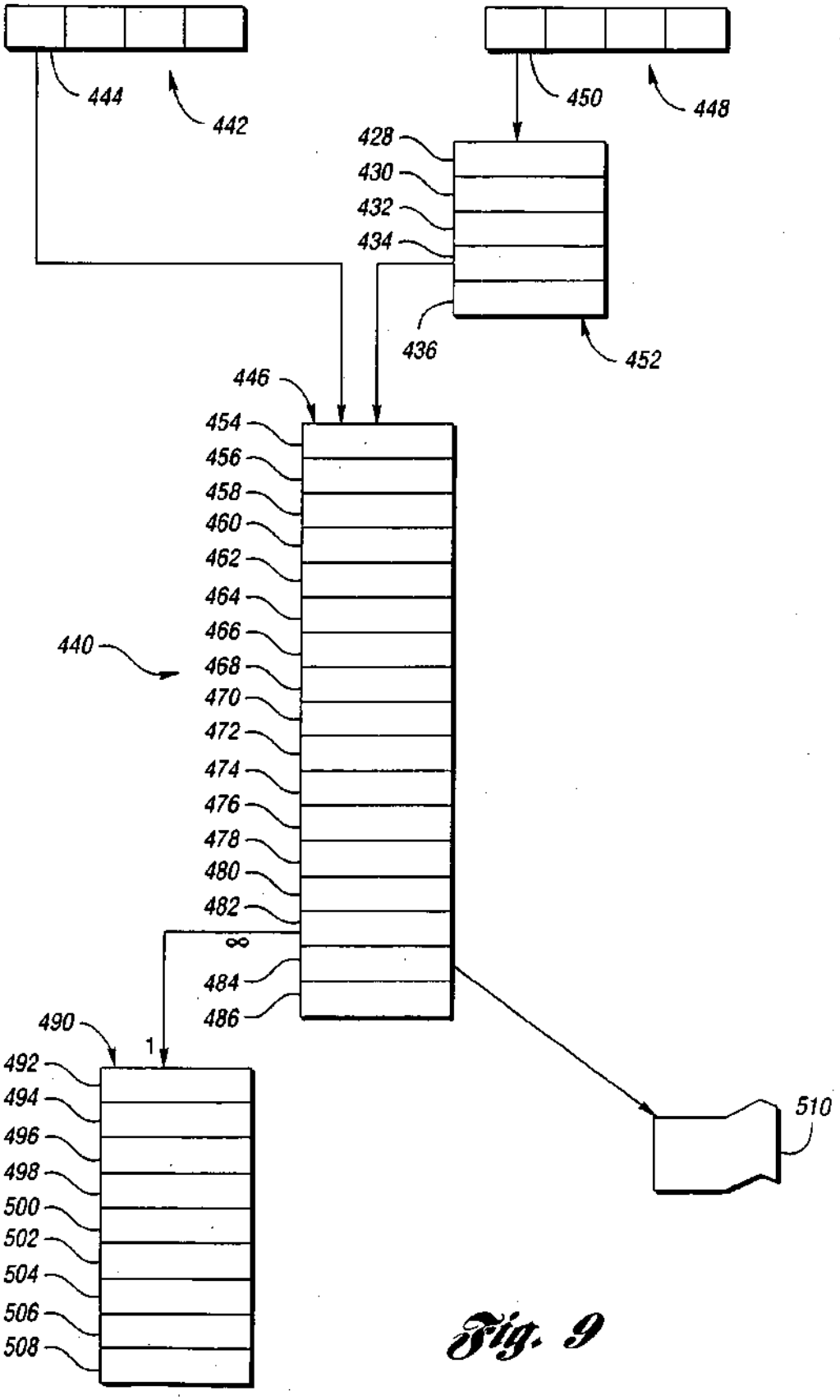

444
442
450
448
428
430
432
434
436
452
446
454
456
458
460
462
464
466
440
468
470
472
474
476
478
480
482
∞
484
486
490
1
492
494
496
498
500
502
504
506
508
510

Fig. 9

# SLOTS:	2048	4096	8192	16384	32768	65536	131072	PATRICIA
# SESSION	SLOT HASHED	SLOT HASHED	SLOT HASHED	SLOT HASHED	SLOT HASHED	SLOT HASHED	SLOT HASHED	TREE
256	1.125	1.0625	1.0313	1.016	1.0078	1.00391	1.002	8
512	1.25	1.125	1.0625	1.031	1.0156	1.00781	1.0039	9
1024	1.5	1.25	1.125	1.063	1.0313	1.01563	1.0078	10
2048	2	1.5	1.25	1.125	1.0625	1.03125	1.0156	11
4096	3	2	1.5	1.25	1.125	1.0625	1.0313	12
8192	5	3	2	1.5	1.25	1.125	1.0625	13
16384	9	5	3	2	1.5	1.25	1.125	14
32768	17	9	5	3	2	1.5	1.25	15
65536	33	17	9	5	3	2	1.5	16

Fig. 10

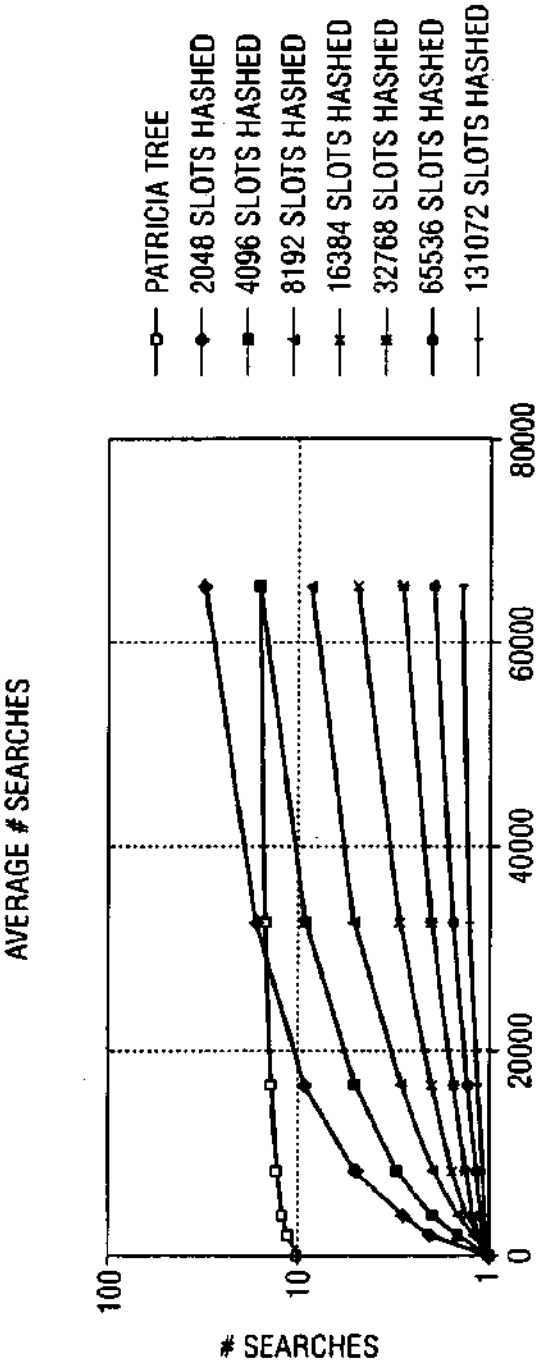


Fig. 11

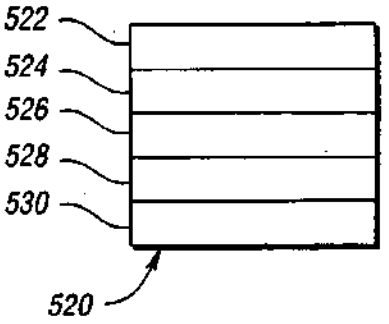

522
524
526
528
530
520

Fig. 12

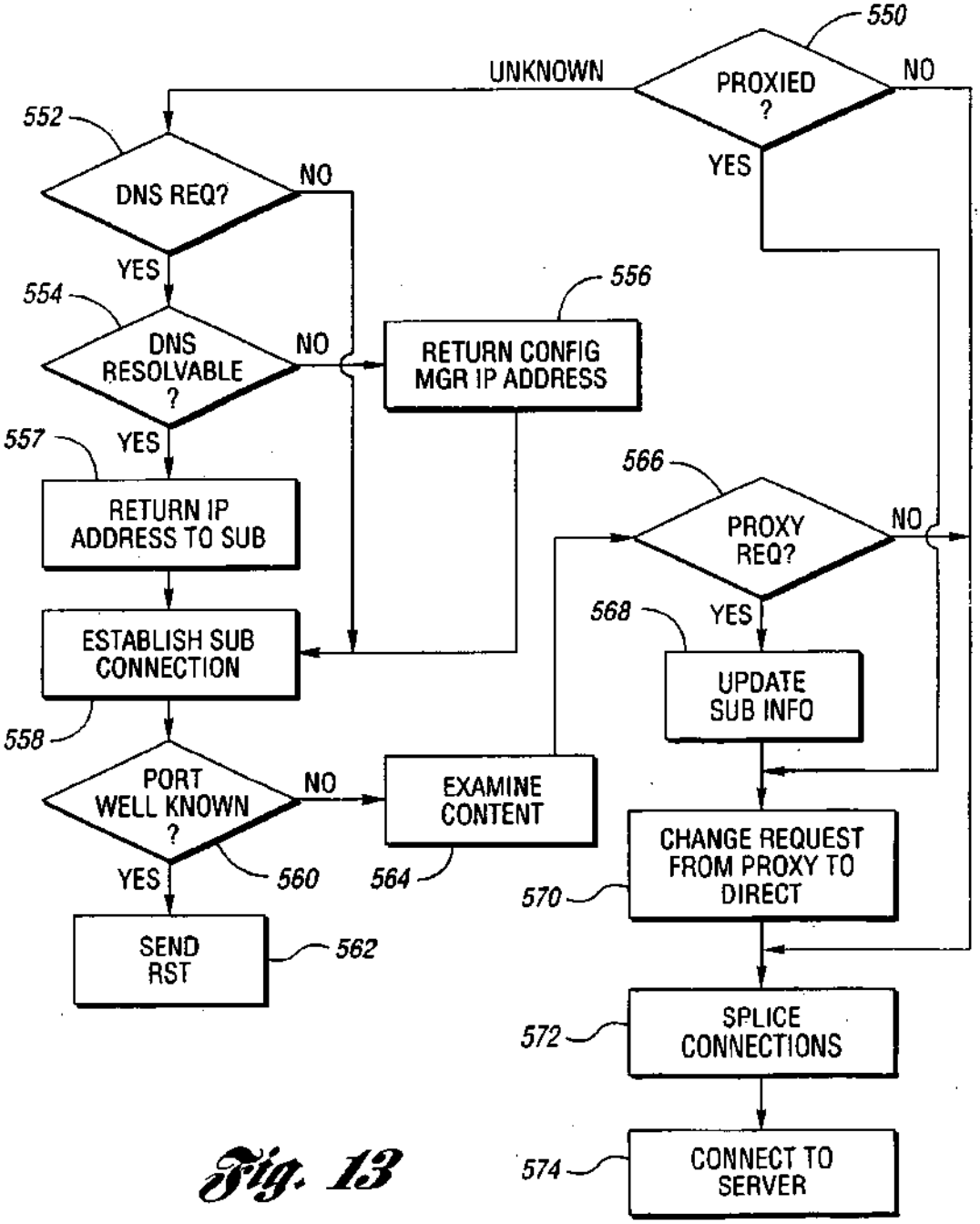

550
PROXIED ?
UNKNOWN
NO
YES
552
DNS REQ?
NO
YES
554
DNS RESOLVABLE ?
NO
556
RETURN CONFIG MGR IP ADDRESS
557
YES
RETURN IP ADDRESS TO SUB
ESTABLISH SUB CONNECTION
558
PORT WELL KNOWN ?
NO
560
YES
EXAMINE CONTENT
564
SEND RST
562
566
PROXY REQ?
NO
568
YES
UPDATE SUB INFO
CHANGE REQUEST FROM PROXY TO DIRECT
570
SPLICE CONNECTIONS
572
CONNECT TO SERVER
574

Fig. 13

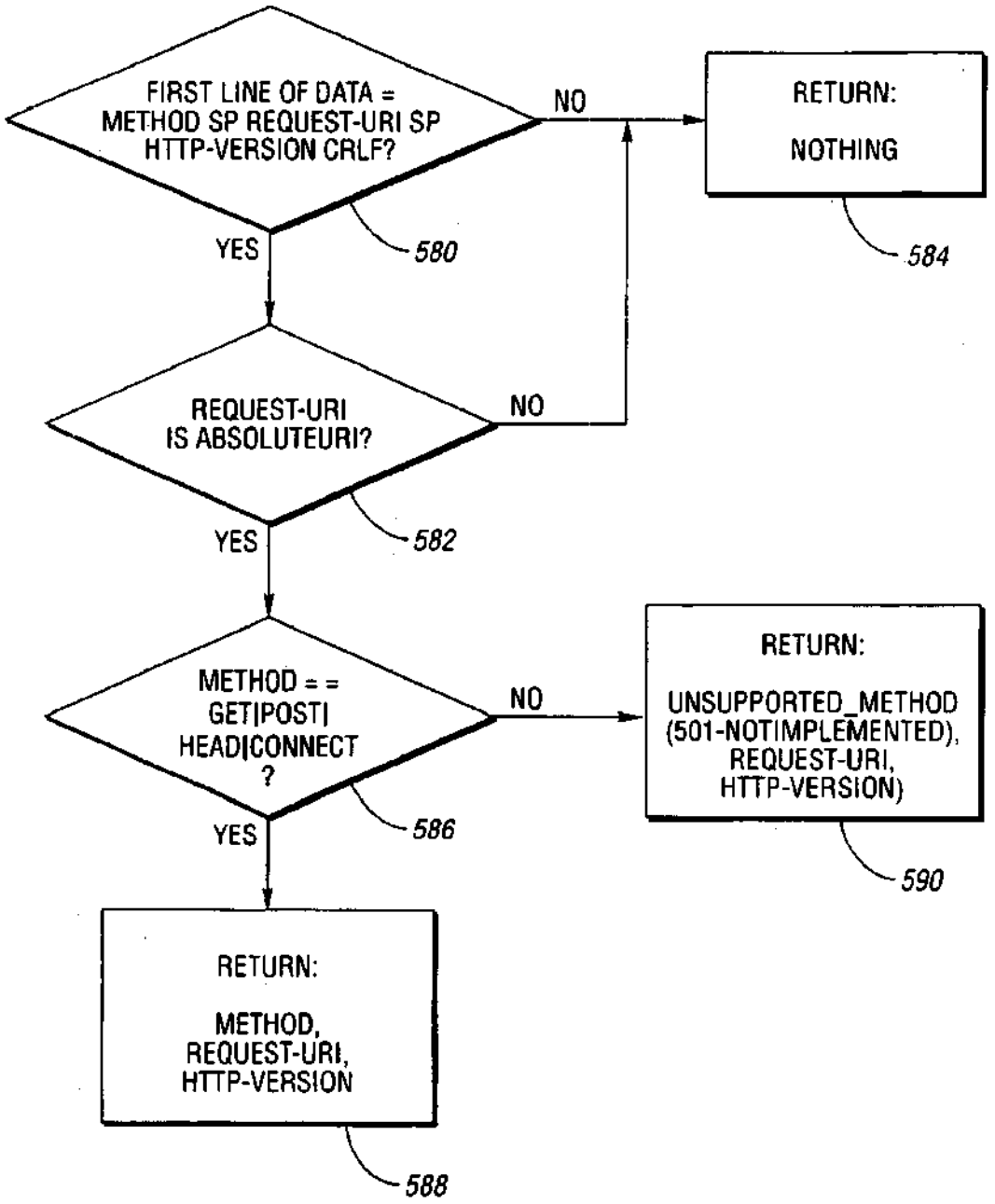

FIRST LINE OF DATA = METHOD SP REQUEST-URI SP HTTP-VERSION CRLF?
NO
RETURN: NOTHING
YES
580
584
REQUEST-URI IS ABSOLUTEURI?
NO
YES
582
METHOD = = GET|POST| HEAD|CONNECT ?
NO
RETURN: UNSUPPORTED_METHOD (501-NOTIMPLEMENTED), REQUEST-URI, HTTP-VERSION)
YES
586
590
RETURN: METHOD, REQUEST-URI, HTTP-VERSION
588

Fig. 14

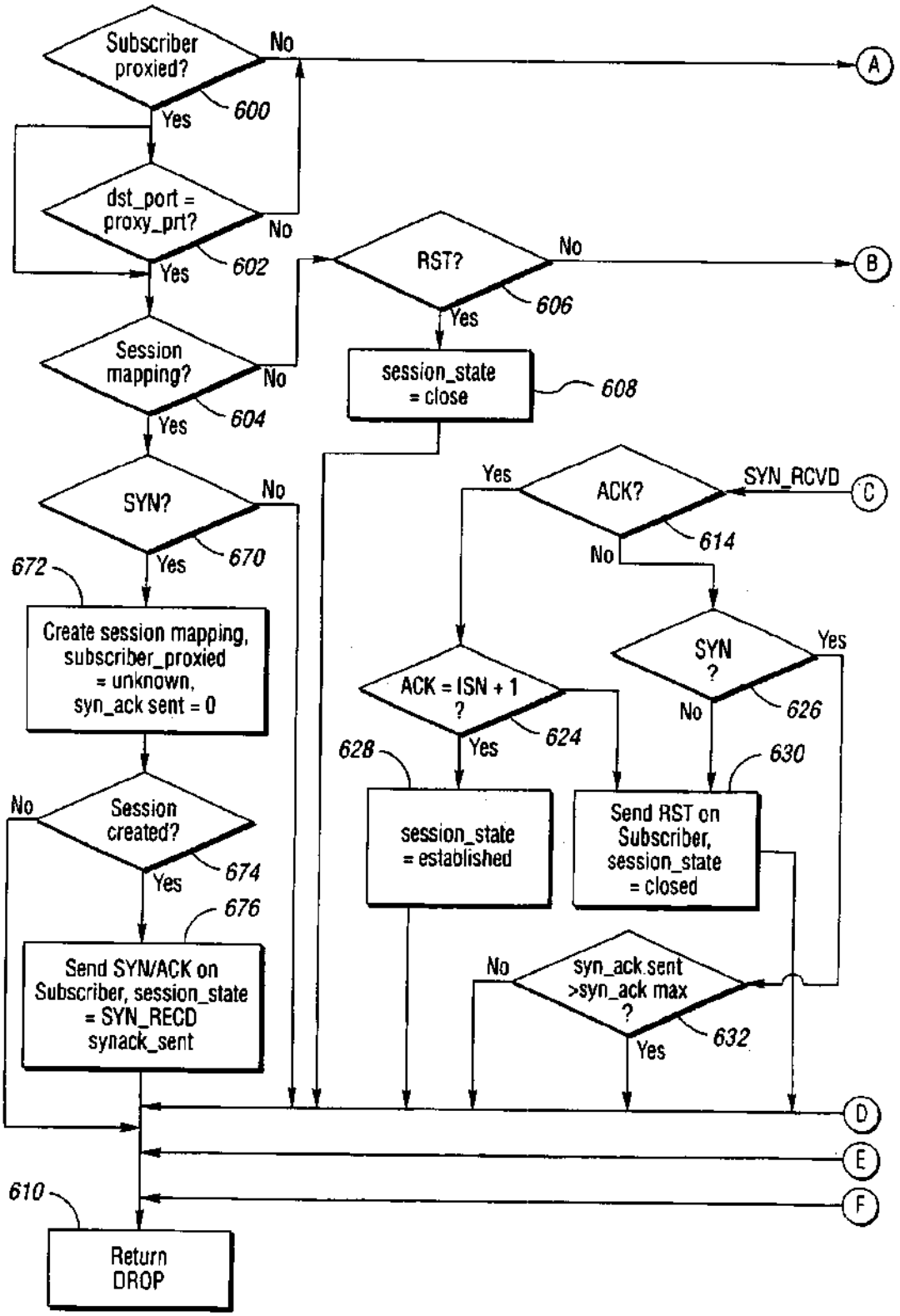

Subscriber proxied?
No
Yes
600
A
dst_port = proxy_prt?
No
Yes
602
RST?
No
Yes
606
B
Session mapping?
No
Yes
604
session_state = close
608
SYN?
No
Yes
670
672
Create session mapping, subscriber_proxied = unknown, syn_ack sent = 0
ACK?
Yes
SYN_RCVD
C
614
No
SYN ?
Yes
No
626
ACK = ISN + 1 ?
Yes
624
628
630
session_state = established
Send RST on Subscriber, session_state = closed
No
Session created?
Yes
674
676
Send SYN/ACK on Subscriber, session_state = SYN_RECD synack_sent
No
syn_ack sent >syn_ack max ?
Yes
632
D
E
F
610
Return DROP

Fig. 15a

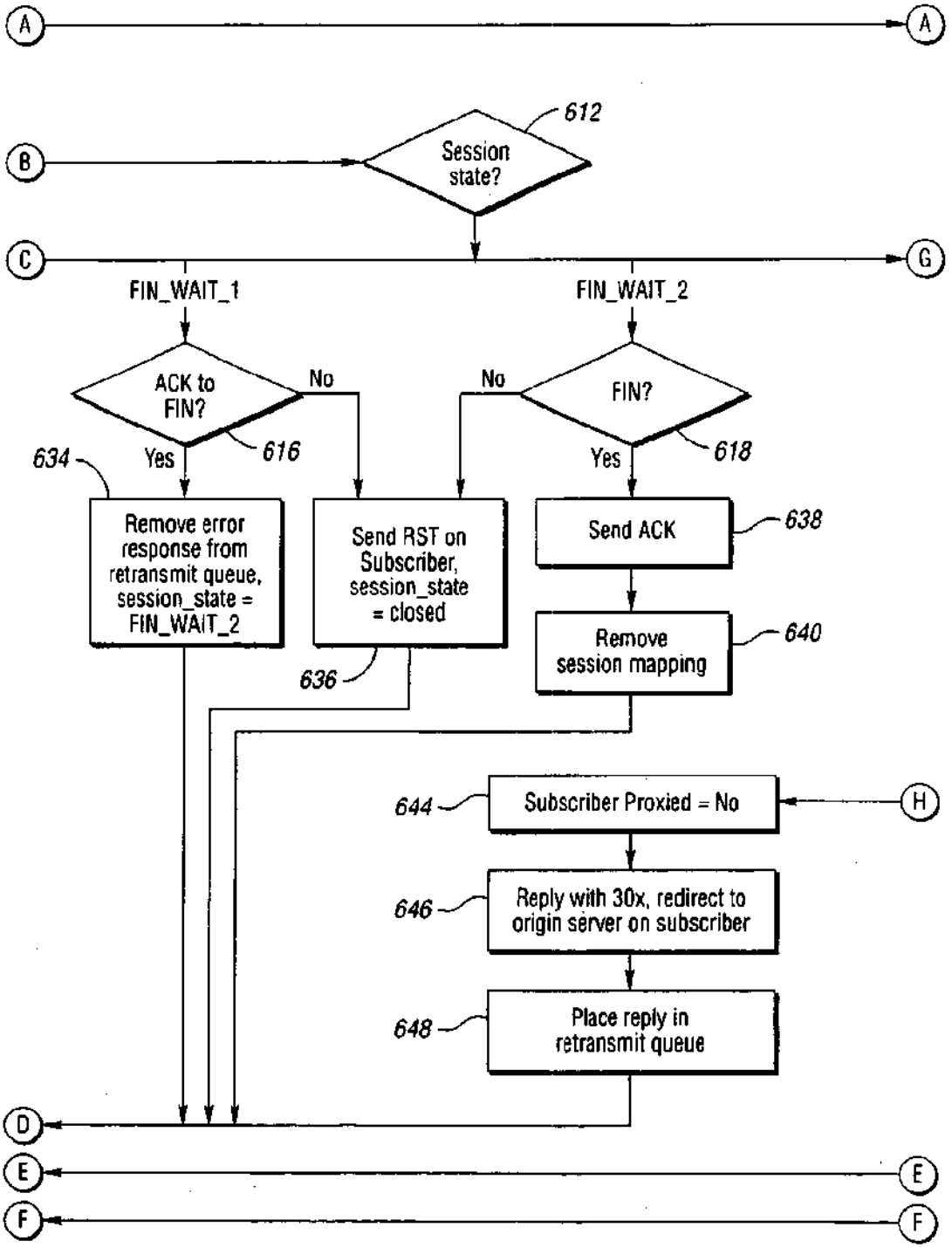

A
A
B
612
Session state?
C
G
FIN_WAIT_1
FIN_WAIT_2
ACK to FIN?
No
Yes
616
634
FIN?
No
Yes
618
Remove error response from retransmit queue, session_state = FIN_WAIT_2
Send RST on Subscriber, session_state = closed
636
Send ACK
638
Remove session mapping
640
644
Subscriber Proxied = No
H
646
Reply with 30x, redirect to origin server on subscriber
648
Place reply in retransmit queue
D
E
E
F
F

Fig. 15b

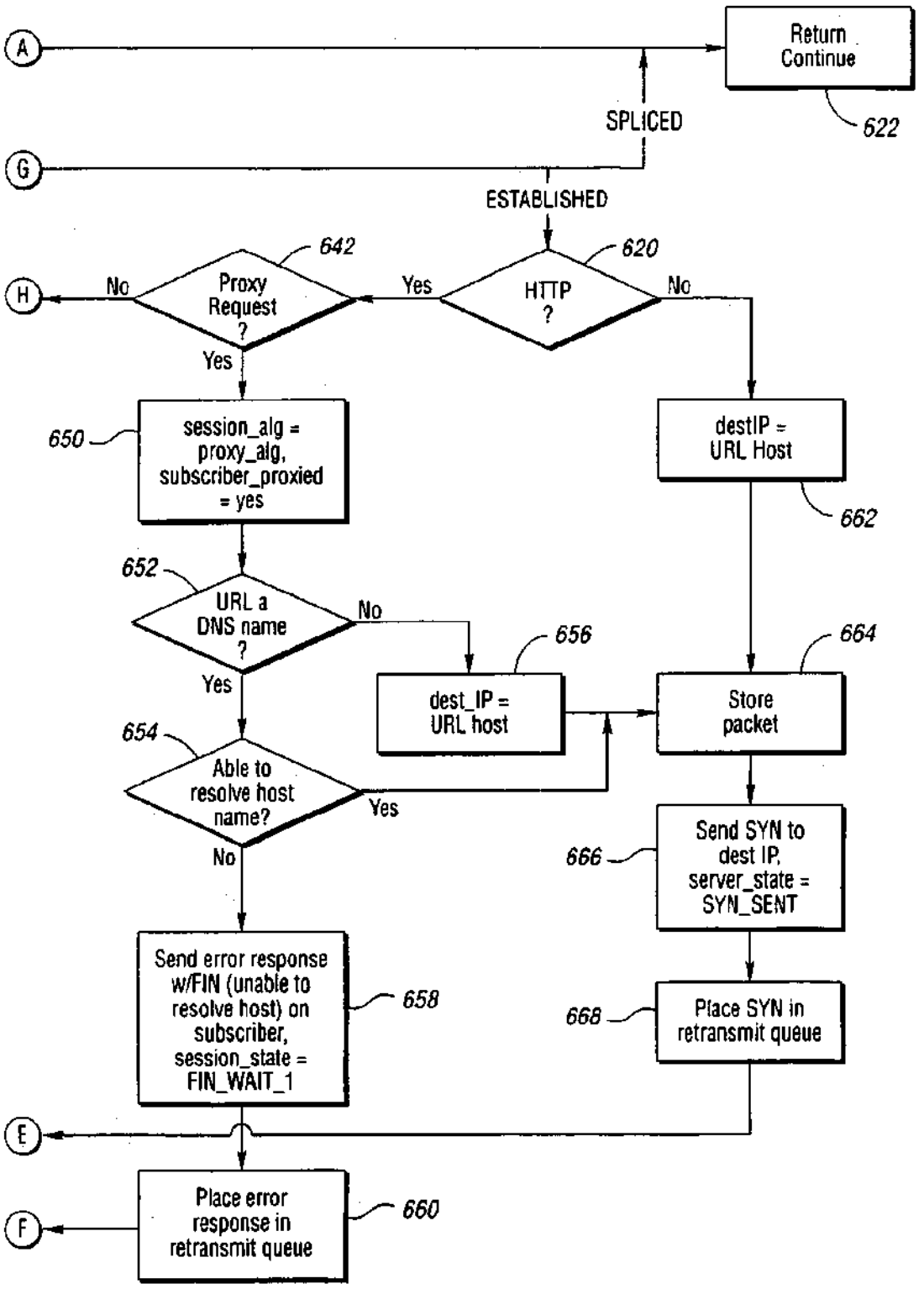

A
Return Continue
622
SPLICED
G
ESTABLISHED
642
620
H
No
Proxy Request ?
Yes
HTTP ?
No
Yes
650
session_alg = proxy_alg, subscriber_proxied = yes
destIP = URL Host
662
652
URL a DNS name ?
No
656
664
Yes
dest_IP = URL host
Store packet
654
Able to resolve host name?
Yes
No
Send SYN to dest IP, server_state = SYN_SENT
666
Send error response w/FIN (unable to resolve host) on subscriber, session_state = FIN_WAIT_1
658
668
Place SYN in retransmit queue
E
F
Place error response in retransmit queue
660

Fig. 15c

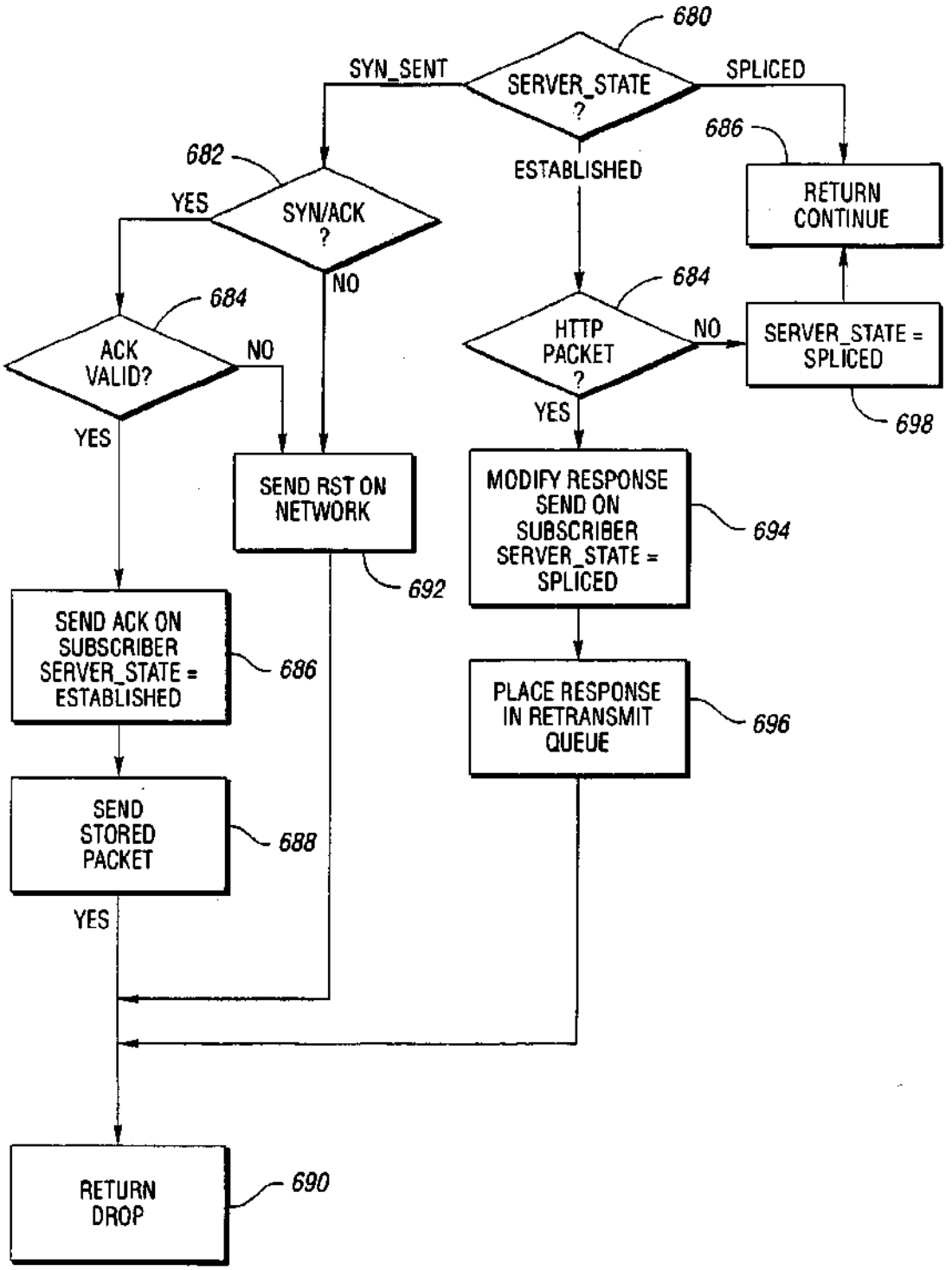

680
SERVER_STATE ?
SYN_SENT
SPLICED
ESTABLISHED
682
SYN/ACK ?
YES
NO
684
ACK VALID?
NO
YES
SEND RST ON NETWORK
692
SEND ACK ON SUBSCRIBER SERVER_STATE = ESTABLISHED
686
SEND STORED PACKET
688
YES
RETURN DROP
690
686
RETURN CONTINUE
684
HTTP PACKET ?
NO
SERVER_STATE = SPLICED
698
YES
MODIFY RESPONSE SEND ON SUBSCRIBER SERVER_STATE = SPLICED
694
PLACE RESPONSE IN RETRANSMIT QUEUE
696

Fig. 16

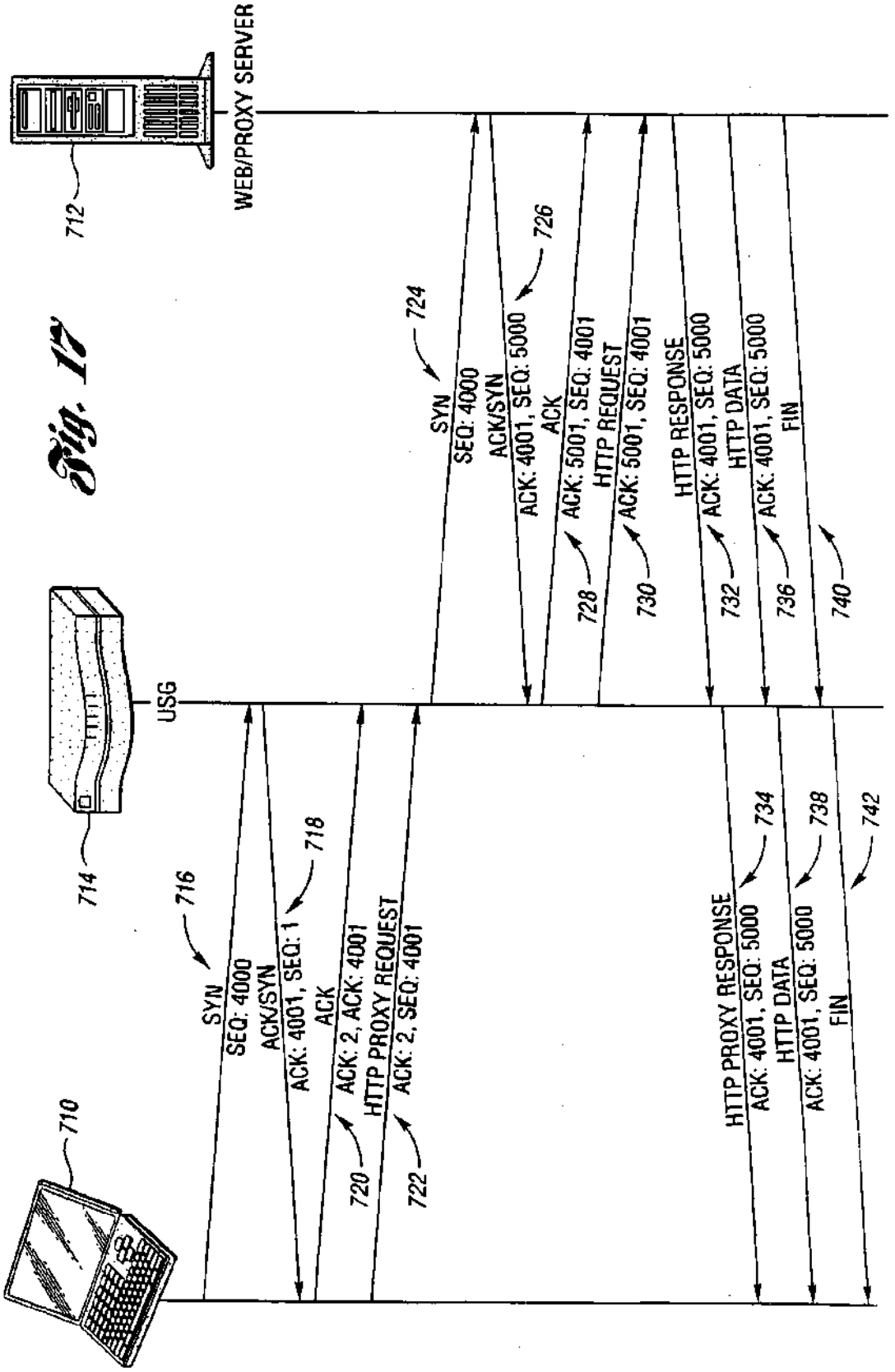

WEB/PROXY SERVER
712
USG
714
710
716
SYN
SEQ: 4000
718
ACK/SYN
ACK: 4001, SEQ: 1
ACK
720
ACK: 2, ACK: 4001
HTTP PROXY REQUEST
722
ACK: 2, SEQ: 4001
724
SYN
SEQ: 4000
726
ACK/SYN
ACK: 4001, SEQ: 5000
ACK
728
ACK: 5001, SEQ: 4001
HTTP REQUEST
730
ACK: 5001, SEQ: 4001
HTTP RESPONSE
732
ACK: 4001, SEQ: 5000
HTTP DATA
736
ACK: 4001, SEQ: 5000
FIN
740
734
HTTP PROXY RESPONSE
ACK: 4001, SEQ: 5000
738
HTTP DATA
ACK: 4001, SEQ: 5000
742
FIN

Fig. 17

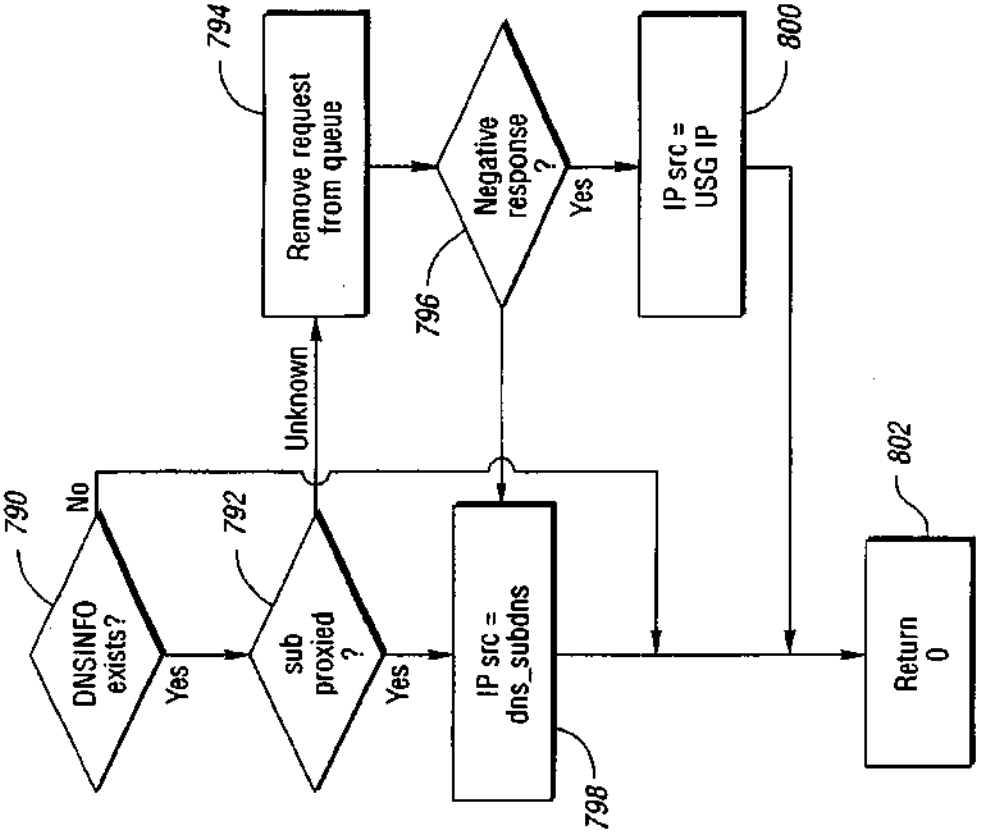

794
Remove request from queue
796
Negative response ?
Yes
800
IP src = USG IP
Unknown
790
No
DNSINFO exists?
Yes
792
sub proxied ?
Yes
IP src = dns_subdns
798
802
Return 0

Fig. 19

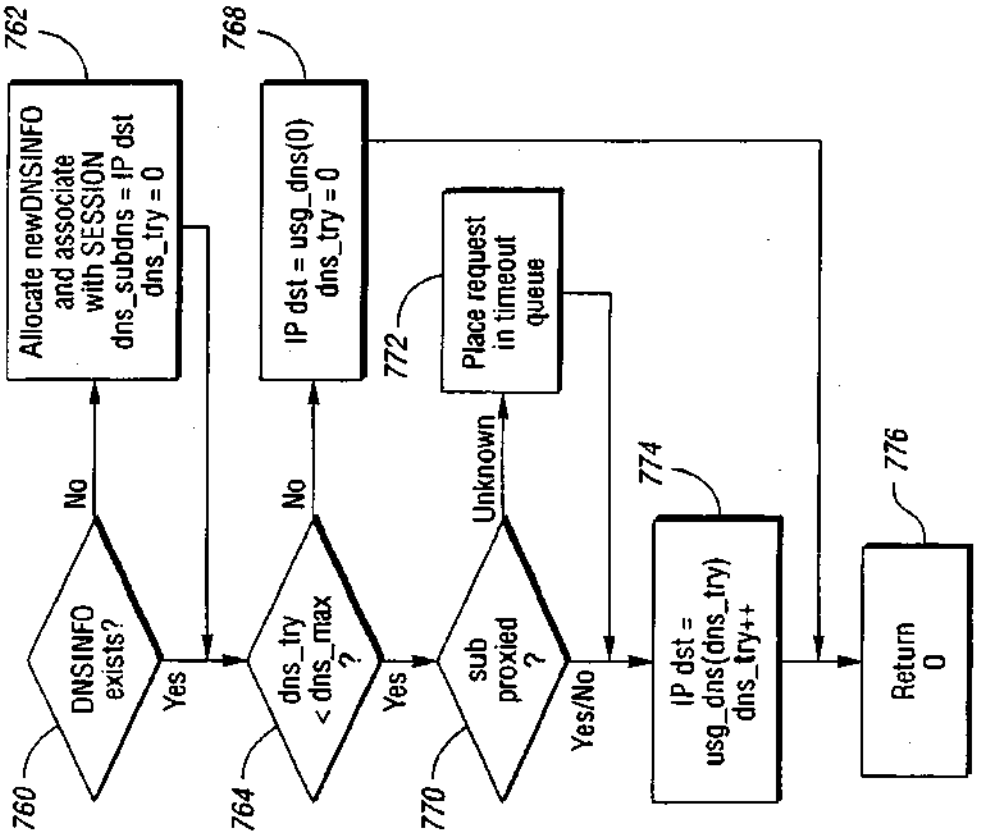
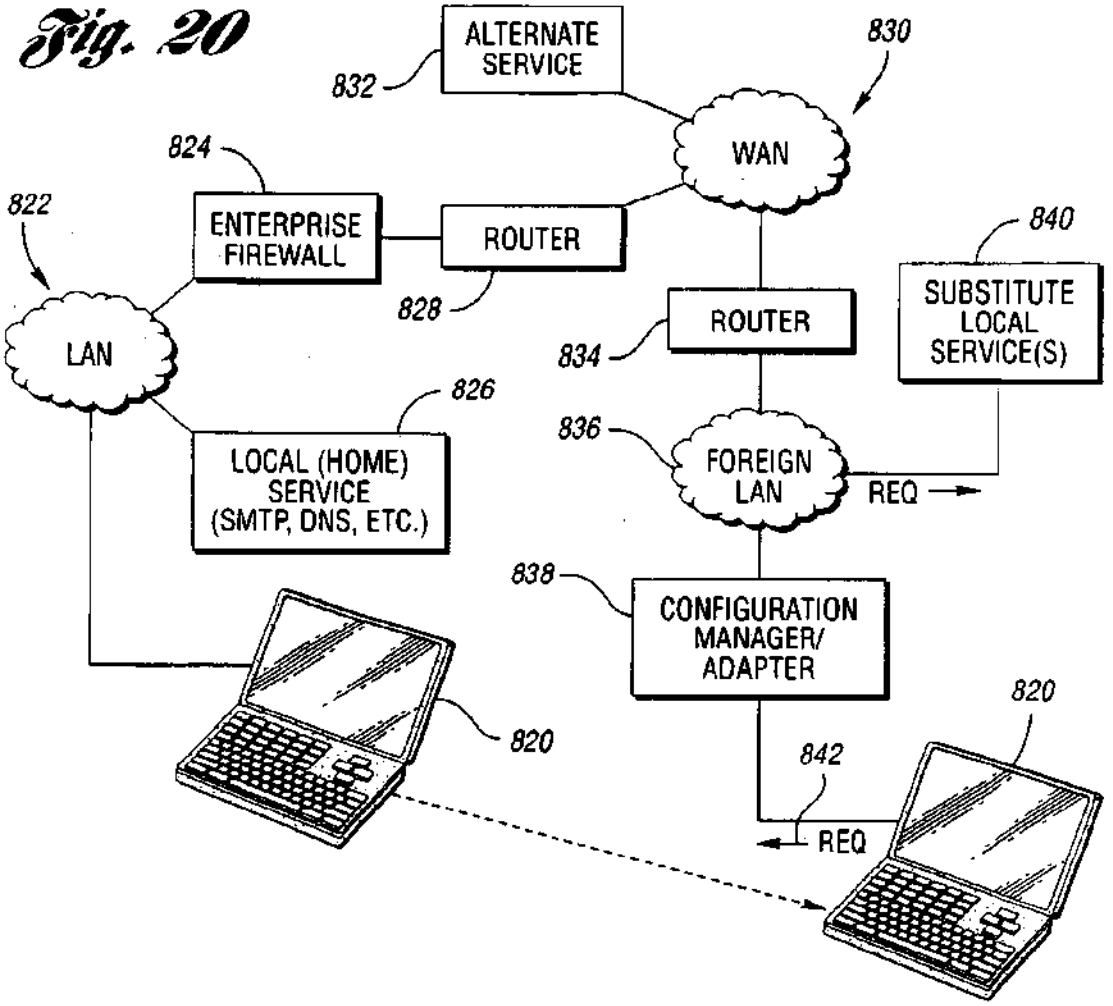

762
Allocate newDNSINFO and associate with SESSION dns_subdns = IP dst dns_try = 0
768
IP dst = usg_dns(0) dns_try = 0
772
Place request in timeout queue
No
No
Unknown
774
776
760
DNSINFO exists?
Yes
764
dns_try < dns_max ?
Yes
770
sub proxied ?
Yes/No
IP dst = usg_dns(dns_try) dns_try++
Return 0

Fig. 18

Fig. 20


ALTERNATE SERVICE
832
830
WAN
824
822
ENTERPRISE FIREWALL
ROUTER
828
840
SUBSTITUTE LOCAL SERVICE(S)
LAN
834
ROUTER
826
836
LOCAL (HOME) SERVICE (SMTP, DNS, ETC.)
FOREIGN LAN
REQ
838
CONFIGURATION MANAGER/ ADAPTER
820
820
842
REQ

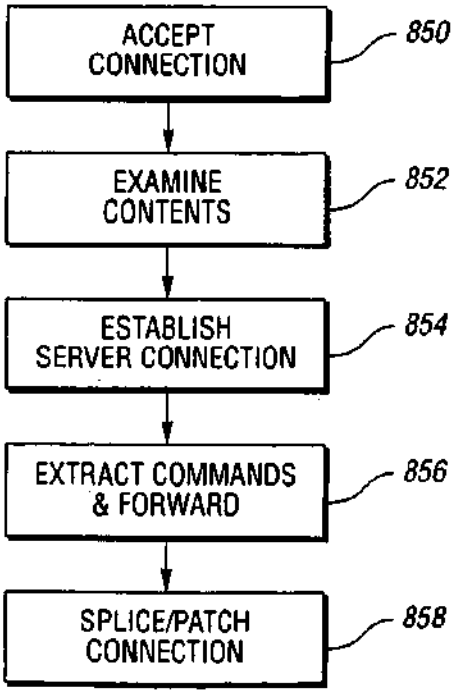

ACCEPT CONNECTION
850
EXAMINE CONTENTS
852
ESTABLISH SERVER CONNECTION
854
EXTRACT COMMANDS & FORWARD
856
SPLICE/PATCH CONNECTION
858

Fig. 21

SYSTEM AND METHOD FOR NETWORK ACCESS WITHOUT RECONFIGURATION

CROSS-REFERENCE TO RELATED APPLICATION

The present application claims priority to U.S. Provisional Patent Application Ser. No. 60/161,138 filed Oct. 22, 1999, the disclosure of which is hereby incorporated by reference in its entirety.

FIELD OF THE INVENTION

The present invention relates to a system and method for providing local and wide area network communications for devices without reconfiguration of communication parameters of the devices.

BACKGROUND OF THE INVENTION

Large corporate or enterprise networks typically require significant resources to deploy and maintain. To lessen the burden of supporting countless users, network administrators often mandate computer hardware, software, and network configuration choices based on a user's needs for access to a local or wide area network, such as a corporate intra-net or the Internet, respectively. Once a computer is configured in accordance with the corporate standard, any changes made by the user to connect to a different (foreign) network, such as may be available while traveling, at a remote corporate site, or at home, may result in his inability to reconnect to the network(s) upon returning to his normal (sometimes referred to as "home") location absent additional administrator intervention.

Widespread deployment of high-speed access technologies has reduced associated costs such that many users have high-speed access to their Network Service Provider (NSP) or Network Access Provider (NAP) from their residences. While high-speed residential access is becoming increasingly more affordable, an incentive remains to share the access among two or more computers, such as a desktop which may belong to the user and a laptop which is often owned by her employer. To establish a connection to the NSP, the user's computing device (desktop, laptop, PDA, etc.) must be appropriately configured. For most users, this task requires additional support from the NSP via telephone in the best case scenario or via an on-site visit for many provisioning tasks which may include hardware installation (cable modem, ISDN modem, NIC, etc.) in addition to application and communication parameter configuration (IP address, gateway, subnet mask, DNS, proxy selections).

Configuration issues present a formidable challenge for truly mobile computing. Wireless modems and cellular telephones are now capable of establishing a network connection within a particular service area. Typically, a user establishes a connection using a remote-access server communicating via point-to-point protocol (PPP) to avoid some of the configuration issues described above. However, this type of connection provides only limited access and functionality. As computing devices become smaller and more powerful, and wireless technologies support increasingly greater bandwidth, traveling "power users" will demand a seamless connection from network to network as they traverse a variety of disparate networks or access areas. User intervention for configuration changes is simply not an acceptable alternative.

A number of strategies have been utilized to reduce the time and effort required for provisioning and/or configuration to connect a new or returning user to a particular network. Dynamic Host Configuration Protocol (DHCP) was developed to allow network administrators to assign TCP/IP configuration parameters to various client computers on their networks. However, some of the functional characteristics of DHCP are not well suited for deploying residential or mobile network access. In particular, DHCP must be selected in the user's configuration to automatically obtain various communication parameters from an appropriate DHCP server. As such, this solution is not viable for any users configured with a static IP address.

In addition to communication parameters which may be set by a DHCP server if appropriately configured, the widespread use of the Internet and world wide web present additional challenges in terms of application configuration settings. For example, many browser applications may be configured to use proxy services for one or more protocols, including HTTP, FTP, Socks, etc. These proxy services are often used in enterprise networks to provide caching and additional security to users. However, the proxy settings must be manually reconfigured by the user to accommodate connection to a foreign network.

One approach to automating application settings uses a strategy similar to a DHCP server. A provisioning server on the foreign network may be used to communicate appropriate proxy settings to a new user using another application program, applet, or script, such as a Java script. However, this approach may require the user (or user's application) to actively request reconfiguration from the provisioning server, i.e. manual intervention from the user. In addition, the applet downloaded from the provisioning server modifies the user's settings which may prevent the user from using that browser on the enterprise network without additional manual intervention and proxy configuration changes.

SUMMARY OF THE INVENTION

Thus, it is an object of the present invention to provide a configuration manager which provides network access to a user without modifying the user's network communication parameters.

Another object of the present invention is to provide a transparent proxy service for users having browsers configured to use a protocol proxy.

A further object of the present invention is to provide a system and method for providing transparent access for a user to a network without requiring manual intervention from the user.

Yet another object of the present invention is to provide transparent HTTP and FTP proxy services to users having a browser configured to use a proxy.

An additional object of the present invention is to provide a system and method for selectively providing proxy service to only those users who are configured to use a proxy.

Another object of the present invention is to provide a system and method for determining whether a particular user is configured to use a proxy service.

A further object of the present invention is to provide a system and method for splicing a connection from a user to the configuration manager with a corresponding connection from the configuration manager to an origin server after determining the subscriber proxy settings.

In carrying out the above objects and other objects, features, and advantages of the present invention, a method for providing client access to a network without changing client network settings includes determining whether the

client is configured to use a proxy service and selectively acting as the proxy service when the client is so configured. In one embodiment, determining whether the client is configured to use a proxy service includes establishing a connection between the client and a configuration manager and monitoring the connection for messages containing a proxy request.

The present invention monitors domain name requests to detect clients configured to use a particular proxy based on a domain name, and provides domain name resolution to a network address to allow a connection to be established. The present invention detects failed domain name lookup requests originating from the client and generates a reply to the client with the network address of the configuration manager. Once the proxy configuration of the client is determined, an appropriate status indicator is preferably stored in a database for future requests from a particular client or subscriber. For clients which are not configured to use a proxy service, no additional processing overhead is incurred. As such, the present invention is capable of selectively processing requests and providing proxy services only when necessary for compatibility between the client settings and a foreign network.

Once it is determined that the client is not configured for proxy service, a connection between the origin server and the configuration manager is established to service the request.

For clients which are configured to use a proxy service, the proxy service is preferably provided by the configuration manager. However, in applications where the client specified proxy server is publicly available, the proxy request may be forwarded to the specified proxy server if desired. Alternatively, all requests (proxy or direct) may be redirected to a proxy server of the NSP, NAP, or a third-party portal, for example, to provide caching, security, and/or network-specific content.

Whether or not the client is configured to use a proxy service, a connection is established between the client and the configuration manager, and between the configuration manager and the origin server. Rather than copying data between these two sessions, the present invention transfers the session flow control functions to the endpoints to effectively splice the connections together while maintaining the end-to-end semantics. To splice the connections, the configuration manager modifies the message header and retransmits the message so there is no need for application buffering. This enhances throughput and reduces processing time. Preferably, the connection splice is performed below the conventional TCP/IP stack using a scaled down TCP implementation with minimal functionality including the three-way TCP connection establishment protocol.

Various other services may also be transparently provided to the subscriber/client including Domain Name Service (DNS) redirection and Simple Mail Transport Protocol (SMTP) over the foreign network. Redirection may be provided independent of the proxy settings where the client-specified server (SMTP or DNS) is unavailable or behind a firewall (which results in slow response times). DNS redirection according to the present invention intercepts a domain name request and redirects the request from the client-specified server to a local domain name server which may be internal or external to the configuration manager. Likewise, the present invention provides SMTP redirection to a local SMTP server which may be internal or external to the configuration manager. Unlike the DNS redirection, the SMTP redirection keeps the source/reply address but directs messages to their final destination via the local SMTP server.

In one embodiment of the present invention, the configuration manager includes an extendible architecture implemented as a cooperative multiplexing protocol dispatcher below the network and transport layers of the protocol stack. The dispatcher actively monitors all packets and uses various hooks to dynamically select which packets to act on rather than blindly sending packets up the stack. The dispatcher distributes packets not only based on frame type but also by protocol. The dispatcher is preferably implemented in software so various modules can be more easily added, deleted, selected, or unselected and may include event driven and/or condition dependent modules. The architecture of the present invention facilitates various hardware/software implementations including embedded systems having one or more microprocessors, application specific integrated circuits (ASICs) and the like.

The present invention provides a number of advantages relative to prior art approaches to the subscriber/client configuration problem. The present invention provides proxy service independent of whether a pre-configured proxy host is reachable from the foreign network, including cases wherein a domain name is not resolvable to a network address. The present invention provides proxy services for pre-configured users where the user's proxy host is located behind an enterprise network firewall. In addition, the present invention provides a system and method which does not require a proxy request as the first service request of a new subscriber.

The above advantages and other advantages, objects, and features of the present invention, will be readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating one application for a configuration manager according to one embodiment of the present invention;

FIG. **2** is a block diagram illustrating an alternative application for a network configuration adapter/manager according to one embodiment of the present invention;

FIG. **3** is a block diagram illustrating system components for a configuration manager/adapter according to one embodiment of the present invention;

FIG. **4** is a block diagram illustrating an application specific integrated circuit implementation of the configuration manager/adapter of the present invention;

FIG. **5** is a block diagram illustrating an extendible architecture of a configuration manager/adapter according to one embodiment of the present invention;

FIG. **6** is a flowchart illustrating operation of a system or method for initialization of a subscriber session for a configuration manager/adapter according to one embodiment of the present invention;

FIGS. **7***a* and **7***b* are flowcharts illustrating dynamic address translation processing of packets received on the subscriber side of a configuration manager/adapter according to one embodiment of the present invention;

FIGS. **8***a* and **8***b* are block diagrams illustrating dynamic address translation processing of packets received on the network side of a configuration manager/adapter according to one embodiment of the present invention;

FIG. **9** is a flowchart illustrating a data structure used for IP session mapping according to one embodiment of the present invention;

FIG. **10** is a table illustrating searching efficiency of a hashing algorithm relative to a Patricia tree algorithm according to one embodiment of the present invention;

FIG. **11** is a graph illustrating the number of searches as a function of the number of sessions for the data illustrated in FIG. **10**;

FIG. **12** illustrates a data structure which may be used to implement a timeout queue according to one embodiment of the present invention;

FIG. **13** is a flowchart illustrating operation of a system or method for adapting a protocol proxy configuration according to one embodiment of the present invention;

FIG. **14** is a flowchart illustrating operation of a system or method for protocol proxy determination according to one embodiment of the present invention;

FIGS. **15***a*–**15***c* provide a detailed flowchart representing operation of a system or method for subscriber HTTP proxy processing according to one embodiment of the present invention;

FIG. **16** is a flowchart illustrating operation of an HTTP proxy application level (layer) gateway (ALG) for the network side of a configuration manager/adapter according to one embodiment of the present invention;

FIG. **17** is a transaction diagram illustrating operation of an HTTP proxy request using a configuration manager/adapter according to one embodiment of the present invention;

FIG. **18** is a flowchart illustrating domain name service (DNS) processing for subscriber side packets according to one embodiment of the present invention;

FIG. **19** is a flowchart illustrating domain name service (DNS) processing for network side packets according to one embodiment of the present invention;

FIG. **20** is a block diagram illustrating operation of a system or method for service redirection according to one embodiment of the present invention; and

FIG. **21** is a flowchart illustrating operation of a method for protocol proxy processing of a file transfer protocol (FTP) request according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

As used throughout this description, the terms client and server refer to the role being performed by a program for a particular connection rather than to the program characteristics in general. As one of ordinary skill in the art will appreciate, any given program may be capable of acting both as a client and a server. Likewise, any server may act as an origin server, proxy, gateway, or tunnel based on the nature of a particular request. Likewise, the terms user and subscriber are used interchangeably.

FIG. **1** provides a block diagram for one possible application of a configuration manager/adapter according to one embodiment of the present invention. As one of ordinary skill in the art will appreciate, the configuration manager of the present invention may include various other features which may be integrated with the automatic configuration features. For example, various subscriber functions such as authentication, authorization, and accounting may also be provided. To communicate over a wide area network **32**, such as the Internet for example, various communication parameters must be appropriately configured. Enterprise networks, represented generally by reference numeral **34**, are typically managed by organizations with resources to provision and maintain computers such as laptop computer **36**. A variety of communication or network configuration parameters, represented generally by reference numeral **38**, must be appropriately configured for computer **36** to communicate with the local and wide area networks. Network configuration parameters **38** may include an IP address **40**, a gateway address **42**, a subnet mask **34**, a DNS address **46**, and various protocol proxies **48**. Protocol proxies may include HTTP, Socks, FTP, Gopher, and the like. The use of one or more web proxy servers is typically specified in the user's browser. Proxies may be specified using an IP address as illustrated, or via a domain name as known by those of skill in the art.

When laptop computer **36** is relocated to a subscriber's home, hotel, airport, etc., configuration settings **38** may be incompatible with the remote or foreign network configuration parameters, represented generally by reference numeral **52**. According to one embodiment of the present invention, a configuration manager/adapter **50** is utilized to detect configuration parameters **38** and translate or map these parameters to appropriate network parameters **52** for communication with the foreign network. The various configuration adaptation functions performed by manager/adapter **50** do not alter the settings of laptop computer **36** so no additional changes are required when attempting to reconnect to the home network. Configuration manager/adapter **50** may be physically located near laptop computer **36** or may be remotely located at the network access provider or network service provider, indicated generally by reference numeral **56**. The present invention is independent of the particular location of the configuration manager. Likewise, the present invention is independent of the particular communication parameters or protocols utilized.

Referring now to FIG. **2**, an alternative arrangement for use of a configuration manager/adapter **50** according to one embodiment of the present invention is shown. This arrangement may be utilized in a residential broadband cable application. Devices **70** may communicate via a local area network **72** with appropriate traffic routed through cable modem **74** to access a wide area network. Cable modems from various locations **74** communicate with a cable modem termination system (CMTS) which acts as a concentrator or multiplexor and performs various standardized processing functions. The configuration manager **50** is placed between CMTS **76** and the network service provider (NSP) **78** to provide subscriber management and automatic configuration adaptation. Depending upon the particular application and implementation, configuration manager **50** may be positioned at various locations throughout the networks. Various other implementations are described in U.S. provisional application Ser. No. 60/111,497 filed on Dec. 8, 1998, and U.S. application Ser. No. 09/041,534 filed Mar. 12, 1999, the disclosures of which are hereby incorporated by reference in their entirety.

FIG. **3** provides a system block diagram of a configuration manager according to one embodiment of the present invention. In this embodiment, system **90** includes a microprocessor or microcontroller **92** in communication with various computer-readable storage media, such as non-volatile memory **94** and random access memory (RAM) **96** via a communications bus **98**. Computer-readable storage media **94** and **96** include control logic **100** in the form of stored data representing instructions executable by microcontroller **92** to perform various processing steps as described in greater detail herein. Control logic **100** may include a real-time operating system (RTOS) **102** which may be extended with various software programs or algorithms **104** to provide the

various features of the present invention. Non-volatile memory **94** may also include configuration information **106** which is used to store configuration settings for particular subscribers once determined by the configuration manager/adapter for subsequent look-up.

Non-volatile memory **94** may be implemented by various known memory devices including PROM, EPROM, EEPROM, flash memory, and the like. Preferably, various components stored in non-volatile memory **94** are transferred or copied to random access memory **96** to improve processing speed. For example, RTOS **102** and one or more algorithms **104** may be copied to RAM **96**. Random access memory **96** may also be used to store various other temporary information. For example, RAM **96** may include a cache **108** to store data which is repeatedly requested by subscribers. RAM **96** preferably includes a session database **110** which is used to store various communication and processing parameters associated with a particular session so that it may be quickly accessed as described in greater detail below.

A host (subscriber or client) communicates with the configuration manager via one of a plurality of host/subscriber interfaces **112**. Communication packets are routed through RAM **96** and stored in appropriate packet buffers **114** for processing. Packets are then communicated to the foreign network via one or more network interfaces **116**. Similarly, messages originating on the foreign network pass through network interfaces **116** before being temporarily stored in packet buffers **114**, processed, and transmitted through subscriber interfaces **112** to the appropriate subscriber (unless dropped as explained below). As illustrated in FIGS. **3** and **4**, the processing features provided by the present application are "in-line" with the data being transmitted from the host to the foreign network. This allows direct modification or manipulation of various packet information without passing the packet up through the full protocol stack.

An alternative system implementation for a configuration manager/adapter according to one embodiment of the present invention is illustrated in FIG. **4**. System **118** may include an application specific integrated circuit (ASIC) **120** for providing control logic to implement various features of the present invention. ASIC **120** preferably includes storage media **122** to provide non-volatile storage **124** and random access or temporary storage **126**. Configuration information **128** may be stored in non-volatile memory **124**. Configuration information may include information associated with a particular subscriber so it does not have to be relearned the next time the subscriber attempts to communicate over the foreign network. Preferably, RAM **126** includes various packet buffers **130** for temporary storage of packets being communicated between host interfaces **132** and network interfaces **134**.

A block diagram illustrating system software architecture for one embodiment of a configuration manager/adapter according to the present invention is illustrated in FIG. **5**. In one preferred embodiment of the present invention, system **150** is implemented primarily in software. However, one of ordinary skill in the art will recognize that various functions may be implemented in software, hardware, or a combination of software and hardware without departing from the spirit or scope of the present invention. Likewise, various functions may be performed concurrently by one or more processors to accomplish the objects and features of the present invention using one or more processing strategies including event-driven and condition-driven processing. As will be appreciated by one of ordinary skill in the art, the sequence or order of processing may be different from that illustrated depending upon the particular application and the particular conditions existing at the time of execution.

System **150** may be used to extend the real-time operating system (RTOS) without significantly modifying the RTOS. In one embodiment, a commercially available RTOS, such as VxWorks is utilized in conjunction with the software architecture extensions illustrated in FIG. **5**. System **150** utilizes a cooperative multiplexing protocol dispatcher **152** implemented below the network and transport layers of the protocol stack. Packets transmitted by a client application of a subscriber over physical media **154** are received by one of the subscriber interfaces **156**. The device level processing of the received data signal is performed based on a particular signaling format, i.e. Ethernet, ATM, FDDI, and the like. Each packet is passed to block **160** which performs session mapping functions as illustrated and described in greater detail with reference to FIGS. **7–11**. Dispatcher **152** actively monitors all packets and uses various hooks to dynamically select which packet to act on, rather than forwarding all packets up through the RFC compliant TCP/IP protocol stack **162**. As such, a significant amount of the processing tasks are performed below the protocols stack **162**. Dispatcher **152** distributes packets based on frame type and protocol. The modular architecture illustrated in FIG. **5** facilitates the use of multiple processors for various processing tasks. For example, these processing tasks may include calculation of the cyclic redundancy check (CRC) **164**, dynamic address translation **166**, HTTP processing **168**, FTP processing **170**, DHCP processing **172**, and DNS processing **174**. These processing functions are explained in greater detail with reference to FIGS. **6–21**.

Dispatcher **152** includes various ALG hooks or callback functions to access various application level gateways **176**. This provides an extendable architecture with various pointers to functions depending on a particular session type. Because dispatcher **152** is implemented below the TCP/IP stack **162**, it is able to selectively process packets faster and more efficiently than implementations which perform such functions at the application level.

FIG. **6** is a flowchart illustrating operation of a system or method for dynamic address translation of packets received by the subscriber interface of a configuration manager according to one embodiment of the present invention. When an initialization packet is received as represented by block **200**, the media access control (MAC) hardware address associated with the packet is used to validate the subscriber based on a customer database **204** and a store of valid customer MAC addresses **203** as represented by block **202**. For a valid address as indicated by block **205**, user activity is logged to provide accounting information as represented by block **206**. The packet is analyzed to determine whether it contains a DHCP request as represented by block **208**. Subscribers previously configured to utilize a DHCP server receive appropriate configuration information as represented by block **210**. Such information may include the IP address, gateway address, subnet mask, etc. as illustrated and described with reference to FIG. **1**. This information is assigned to the subscriber or user device as represented by block **212**. Normal processing of the packet is then performed by block **214** and the process is completed as represented by block **216**. Although various communication configuration parameters are assigned to the subscriber and may actually be stored on the subscriber's computer, the present invention has not actually modified the controlling configuration parameter, i.e. whether to use a DHCP server or not. As such, when the subscriber returns to her home

network, the subscriber accesses the home DHCP server to obtain the appropriate configuration parameters. Any configuration changes are transparent to the subscriber and do not require manual intervention.

For users which have a static IP address, i.e. messages which do not contain a DHCP request as indicated by block **208**, appropriate address translation or redirection is performed as indicated by block **218**. For example, the static IP address contained in the subscriber packets is mapped to a network IP address compatible with the particular subnet of the configuration manager/adapter. To achieve this functionality, the configuration manager must monitor all packets to determine when to selectively perform address translation, i.e. when the subscriber is mis-configured for the foreign network. Processing then continues as illustrated through blocks **214** and **216**.

For initialization packets which do not have a valid MAC address as represented by block **205**, temporary configuration information is provided as represented by block **220**. A subscription log-in page may be provided as represented by block **222**. A new user as indicated by block **224** is prompted to create a user account as indicated by block **226**. The configuration information is then stored for future reference as indicated by block **228**. Processing then continues through blocks **210**, **212**, **214** and **216** as described above. For established users as determined by block **224**, blocks **230** and **232** determine whether a valid log-in ID has been entered. Then block **234** stores the MAC address for validated subscribers as represented by block **203** for subsequent connections to the foreign network. Processing then continues with block **218** which performs any necessary address translation or redirection as illustrated and described in greater detail below.

FIGS. **7***a* and **7***b* provide a block diagram illustrating dynamic address translation for packets received from the subscriber interface of a configuration manager according to one embodiment of the present invention. The received packet is examined to determine if it contains a valid IP checksum at **300**. For packets containing a valid checksum, block **302** determines whether it is a TCP packet. Block **304** then determines whether the destination port is a "well-known" destination port. As recognized by those of skill in the art, well-known ports may include those defined in RFC1060 for SMTP, POP-3, Telnet, and the like. If the port is recognized, block **306** determines whether the source address is on the same subnet as the foreign network and would therefore not necessarily require address translation. As such, the present invention selectively performs address translation on only those subscribers which require it.

Processing continues with block **308** which determines whether the packet is an IP fragment. If not, block **310** attempts to determine the type of packet. Internet control message protocol (ICMP) packets are processed as represented by block **312**. TCP/UDP packets are examined at block **314** to determine whether they include a valid checksum. Packets with an invalid checksum are dropped as represented by block **336**. If the packet type is not recognized, the packet is passed to the next hook of the dispatcher as represented by block **316**.

If the source address of the packet is on the same subnet as the foreign network as indicated by block **306**, block **318** determines whether the packet has a proxy ARP (address resolution protocol) entry. If not, an appropriate proxy ARP entry is created as represented by block **320**. Block **322** determines whether an application level gateway (ALG) is required for additional processing. If required, the processing continues with block **308**. If no special ALG processing is required, the processing continues with block **324** which sets the link layer source address to the network address. As such, the present invention selectively translates those addresses which are not appropriately configured for the foreign network. Block **324** changes the source address such that the packet appears to originate at the configuration manager.

Block **326** examines the destination address to determine whether it is on the same subnet as the foreign network. Block **328** uses ARP to resolve the destination link layer address for destinations on the same subnet. Block **330** obtains the appropriate network gateway address for destinations which are on a different subnet than the configuration manager processing the request. The packet is then output on the network interface as represented by block **332**.

For packets which are determined to be fragmented by block **308**, a fragment counter is updated as represented at block **334** prior to the packet being dropped at **336**. For packets which are not fragmented and recognized as TCP/UDP packets with a valid checksum indicated by block **314**, block **338** determines whether a session mapping exists. If an entry exists in the session mapping table, block **340** determines whether the destination port of the session matches the destination port of the packet. If the packet and session destination ports do not match, the session mapping is deleted at block **342** before creating a new session mapping as indicated by block **344**. As such, the present invention utilizes a destination port as part of the session mapping. Likewise, if the block **338** determines that session mapping does not yet exist, a new session mapping is created as represented by block **344**. Once the session is created as determined by block **346**, processing continues with block **340**. If a session cannot be established, the packet is dropped as indicated by block **336**. For newly created sessions, the session destination port is set equal to the packet destination port and processing continues through block **348** which determines whether an application level gateway is required for additional processing.

Block **350** applies appropriate ALG processing when required. Block **352** determines whether a request has been received from the ALG to drop the current packet. When such a request is received, the packet is dropped as indicated by block **336**. Otherwise, block **354** determines whether the ALG changed the packet length. If the packet length is modified by the ALG as indicated by block **354**, the M block lengths must be adjusted at block **356** prior to adjusting the sequence number (for TCP packets) at block **358**. If the ALG does not modify the packet length, no additional IP modifications are required and block **358** adjusts the sequence number prior to processing by block **360**. The message source port is replaced with the session source port as represented by block **360**. As such, the IP session mapping of the present invention preforms address and port translation. The port is utilized for messages received from the network interface to map back through the session mapping and be delivered to the appropriate subscriber as explained in greater detail below.

After modification of the source address and source port, the IP and UDP/TCP checksums must be recalculated as represented by block **362**. The status or state of the session is then updated as represented by block **364**. Preferably, the session status is stored within a data structure in RAM as illustrated in greater detail with reference to FIG. **9**.

Block **366** examines the status parameter for the current session to determine whether the session has been closed. If

not closed, block **368** updates the session time stamp. The present invention utilizes the time stamp to determine which ports may be reused. If a TCP FIN (close) is received, the port may be released immediately. Otherwise, a timeout queue is utilized, such as illustrated and described with reference to FIG. **12**, for example. The link layer source address is then changed from the subscriber's address to the configuration manager's address at block **324**. Block **326** determines whether the destination of the packet is on the same subnet as the configuration manager. If so, block **328** uses ARP to resolve the destination link layer address. Otherwise, the network gateway address is used as indicated by block **330** prior to outputting the packet on the network interface as indicated by block **332**.

A detailed block diagram illustrating operation of a system or method for performing dynamic address translation of packets received from the network interface of a configuration manager according to one embodiment of the present invention is illustrated in FIGS. **8***a* and **8***b*. Block **380** determines whether a valid IP checksum is contained within the packet received from the network interface. For valid checksums, block **382** determines whether the IP destination address matches the network IP address for the configuration manager. Block **384** then passes the packet to the network stack if the destination address matches the network address. Otherwise, block **386** determines whether the IP destination address corresponds to a subscriber IP address. For appropriately addressed packets, block **388** determines whether the packet is a fragment. If so, a fragment counter is updated as indicated by block **390** prior to dropping the packet as represented by block **392**.

If the destination address of the received packet does not correspond to the subscriber address, block **394** determines whether the destination address is a proxied address. If not, the packet is dropped as represented by block **392**. For proxied addresses, block **396** modifies the packet to comply with the appropriate frame type, e.g. Ethernet. Block **398** updates the session time stamp which is used to determine when the particular port can be reused by another session as explained in greater detail with reference to FIGS. **9**–**12**. Block **400** performs an appropriate address and port translation, i.e. translates the destination address received from the network interface to an appropriate subscriber destination address based on the session mapping. Likewise, the port address is translated based on the session mapping.

The session state indicator is updated if necessary as represented by block **402**. The TCP/UDP and IP header checksums are recalculated at block **404** because of the modification to the packet which occurred at block **400**. The packet is then output on the subscriber interface as represented by block **406**.

For packets having a destination IP address which matches a subscriber IP address and which are not fragments as determined by blocks **386** and **388**, the packet type is determined by block **408**. The packet is passed to the next hook of the dispatcher as indicated by block **410** unless the packet type is identified as an ICMP or TCP/UDP packet. ICMP packets are processed as represented by block **412**. TCP/UDP packets are examined for a valid checksum at block **414**. Packets with invalid checksums are dropped as represented by block **392**. Block **416** determines whether a session mapping exists for valid TCP/UDP packets. If no session mapping exists, the packet is dropped as indicated by block **392**. Otherwise, the packet is examined to determine whether the destination port corresponds to the session destination port at block **418**. If the ports do not match, the packet is dropped as indicated by block **392**. Otherwise, an appropriate acknowledgment is returned to the source address as represented by block **420** to acknowledge receipt of the packet. The acknowledgment number may have to be adjusted based on information stored in the session mapping tables.

Block **422** determines whether ALG processing is required. If required, the appropriate ALG is called as represented by block **424**. The ALG determines whether the packet should be dropped as indicated by block **392**, or processed through blocks **398**–**406** where it is output on the subscriber interface. Likewise, if no ALG processing is required as indicated by block **422**, the packet is processed in accordance with blocks **398**–**406** as described above.

Thus, the present invention utilizes selective address and port translation to allow any IP address transmitted by a subscriber to become a valid internal IP address for the foreign network without manual user intervention. Multiple subscriber clients can communicate even though each IP address may correspond to a different subnet. Because the functions illustrated in FIGS. **7***a*–**7***b* and **8***a*–**8***b* are performed as an extension of the RTOS in-line with the data, the present invention provides a scalable approach which is capable of handling several thousand concurrent sessions originating from thousands of subscriber clients. The extended RTOS operates below a traditional RFC compliant protocol stack which further improves efficiency and throughput compared to a traditional socket-based approach.

FIG. **9** illustrates a data structure for tracking various parameters associated with a particular session. Because of the large number of concurrent sessions which may be active and the number of communication and processing parameters associated with each session, the present invention incorporates a search strategy which attempts to minimize the number of searches necessary to locate session parameters based on packets received from the subscriber interface or the network interface. The data structure, indicated generally by reference numeral **440**, is preferably accessed via a first table **442** from the subscriber side of the configuration manager/adapter and accessed from a second table or array **448** from the network side of the configuration manager/adapter. In one embodiment, table **442** is a hashed table keyed on the MAC address of the subscriber and the subscriber port.

The advantages of the present invention in terms of searching efficiencies are illustrated and described with reference to, FIGS. **10** and **11**. The present invention utilizes a hashed table to locate parameters associated with a particular session rather than a Patricia tree algorithm. As known by those of skill in the art, a Patricia tree is a well known searching strategy or algorithm commonly used in routing applications to determine the next hop based on a particular packet. The Patricia tree is particularly suited for large networks and has good scalability since the number of searches increases as a log function of the number of nodes. However, a hashed table with an appropriately selected hashing function provides a more efficient search algorithm for smaller scale implementations. In one embodiment of the present invention, hashed table **442** includes 131,072 (128K) slots. The hashed table **442** uses a linked list to access the session data structure indicated generally by reference numeral **446**. To provide a unique key, the present invention utilizes at least a portion of a link layer attribute, such as the MAC address of the subscriber. Various portions of the MAC address which are common to many network interface cards (NICs) are excluded from the hashing function to increase the uniqueness of the key. For example, the MAC address is specified to include various fields associated with

the manufacturer, product line, type, and serial number of the NIC card. As such, it is more desirable to use a unique portion, such as the serial number, than a common portion, such as the manufacturer code, in the hashing function. In one embodiment, the hashing function utilizes a portion of the MAC address, the protocol (TCP or IP) and the source port number to generate a key. In addition to the serial number, a randomized vendor code (part of the MAC address) may also be utilized. The uniqueness of the key generated by the hashing function directly affects the efficiency of the search. As such, it is desirable to devise a hashing function which generates unique keys such as accomplished by the present invention.

As also illustrated in FIG. **9**, an indexed array or linear list **448** is used to access the session data structure for packets originating on the network side of the configuration manager. In one embodiment of the present invention, linear list **448** includes 65,536 (64K) possible slots or entries. Each entry **450** of the indexed array includes fields **428**, **430** for pointers indicating the next and previous locations of the list, respectively. Field **432** is used to store the network port for port translation. A pointer to the session, represented by reference numeral **434**, is used to index into the session data structure **446**. Field **436** indicates that the net port is free or available for use.

Each session data structure **446** includes a number of fields or entries represented by reference numerals **454–486**. Each session data structure includes links to the next **454** and previous **456** entries in the session linked list. In addition, the transport protocol, MAC address, IP address and port of the subscriber are stored as represented by blocks **458–464**. The original subscriber's destination port which corresponds to the port prior to translation is stored in entry **466**. The mapped IP address **468** and mapped network port **470** are used to adapt the subscriber's configuration (IP address and port) to an appropriate address and port for communication over the foreign network. The current session state is also stored as indicated by reference numeral **472**.

The sequence number and acknowledgment number for the subscriber are entered in fields **474** and **476**, respectively. A sequence number delta or modification value is stored in field **478**. The sequence number delta is used to modify the TCP sequence information between the subscriber and the foreign network to maintain appropriate end-to-end connection semantics as explained in greater detail below. Slot **480** is used to store the previous value for the subscriber sequence number delta. An ALG pointer is provided to link an ALG information list **490** to a particular session. As indicated, ALG linked list **490** exists in a one-to-many relationship with respect to the ALG pointer **482**, i.e. many sessions may be linked to the same ALG data structure **490**. Session specific ALG data **510** is associated with a particular session via slot **484**. A time stamp slot **486** records an absolute time indicating the last time the session was active, i.e. used to transmit or receive any packets. The time stamp may be used to identify the oldest session so that the associated port may be reused. Any sessions which are closed can be used to immediately release the associated port. Thus, the present invention preferably does not expend overhead to proactively clean the tables or data structures. Rather, ports are reused based on the oldest absolute time, or based on ports which are explicitly released as a result of a closed session, for example when a TCP FIN packet is received.

An ALG information list **490** is associated with one or more sessions as described above. Each ALG data structure may include various fields represented by entries **492–508**. In particular, structure **490** preferably includes pointers linking the next **492** and previous **494** entries in the ALG list. Entry **496** provides for storage of the ALG identifier or name. The ALG protocol and application are stored in entries **498** and **500**, respectively. Preferably, data structure **490** includes separate packet hooks **502** and **504** for packets received via the subscriber interface and network interface, respectively. Entry **506** provides an additional hook which may be used to link the ALG to various other applications. A shut down hook **508** is used to terminate execution of the ALG if required.

FIG. **10** provides a table of the average number of searches required for various combinations of sessions and slots in a hashed table with an appropriate hashing function as described above. The last column indicates the average number of searches which would be required for a Patricia tree search algorithm. This information is presented graphically in FIG. **11**. As can be seen from FIGS. **10** and **11**, the hashed table and hashing function in accordance with the present invention provide a more efficient search algorithm for smaller scale implementations than the more traditional Patricia tree which is commonly used with routing applications. Of course, various other implementations of hashing functions and/or searching algorithms may be utilized with various other aspects of the present invention.

FIG. **12** illustrates a data structure which can be used in accordance with the present invention as a timeout queue. Data structure **520** includes fields or entries **522–530** which are used to track the time **522** that a particular job was added to the queue, the number of ticks or time units beyond the initial time available to process the current job **524**, and the number of times to process this job **526**. In addition, a pointer **528** indicates location of the function to process a particular job while entry **530** stores the data to be passed to the function processing the job. Timeout queue **520** may be used by a variety of processing functions of the present invention. For example, the timeout queue is preferably used to reduce overhead otherwise associated with maintaining the session mapping table. Rather than actively cleaning up the table to eliminate inactive sessions to accommodate new session mappings, the oldest sessions (based on time stamp) are reused as necessary.

Referring now to FIG. **13**, a flowchart illustrating operation of a system or method for protocol proxy processing in a configuration manager/adapter according to one embodiment of the present invention is shown. Block **550** in FIG. **13** determines whether the subscriber is proxied, i.e. whether the client browser or other application is configured to use a proxy server. Block **550** accesses the subscriber database to determine whether the proxy status of a particular subscriber was previously determined and stored. If the proxy status is unknown, block **552** examines the packet to determine whether it is a DNS request. This is necessary to automatically accommodate browsers which are preconfigured with a proxy host name rather than an IP address. If the browser is configured to connect to a proxy server by name, the first request from the browser when trying to connect to an HTTP server will be a DNS request for the proxy server name to determine the associated IP address. Block **554** attempts to resolve the DNS request. If the preconfigured proxy server name is not publicly available, the DNS server will return an error, or nothing will be returned and the process will timeout. In this case, the DNS request is not resolvable. Until the subscriber's proxy configuration is known, all DNS responses should be examined to detect a failure or timeout. Either condition results in the configuration manager returning its own IP address as represented

by block **556**. Thus, the configuration manager has resolved the DNS request using its own IP address and is therefore acting as the otherwise unreachable preconfigured proxy server. For proper operation, any timeout failure for the configuration manager should be less than the corresponding timeout of the client browser and should be configured to allow for slow links. If the configuration manager times-out but then subsequently receives a reply to the DNS request which resolves the address, the connection can be reset and the actual IP address passed to the subscriber.

The configuration manager returns its own IP address to resolve the DNS request for a proxy server only until the proxy status can be established. Once the proxy configuration of the browser or other application program is determined and stored in the subscriber database, additional DNS requests are not resolved by the configuration manager (unless employing redirection as described below). The DNS request which is resolved as represented by block **556** is returned with a duration of zero such that any subsequent HTTP requests by the client browser will also be preceded by a DNS request to again resolve the proxy address. These subsequent DNS requests will not be resolved by the configuration manager because the proxy configuration has been previously determined and stored. Rather, these DNS requests are relayed by the configuration manager/adapter to the server which responded to the previous DNS request.

If the DNS request is resolvable to the actual preconfigured proxy server, then the actual DNS result may be relayed back to the browser as represented by block **557**. Once the IP address has been resolved, a connection is established between the subscriber and the configuration manager as represented by block **558**. The packet is then examined to determine if a well-known destination port is being used as represented by block **560**. If a well-known port is being used, a connection reset request is sent as indicated by block **562**. Otherwise, the packet contents or payload must be examined to determine if the HTTP request is a proxy request as indicated by blocks **564** and **566**. If a proxy request is detected, the proxy status of the subscriber is updated in the subscriber database as represented by block **568**. The configuration manager then acts as the proxy and modifies the packet to change the proxy request to a standard unproxied or direct request with an appropriate IP address as represented by block **570**. The configuration manager then establishes a connection with the origin server, and splices the connection from the subscriber to the origin server as represented by block **572** and explained below.

Rather than maintain two separate connections between the subscriber and configuration manager, and between the configuration manager and the origin server, the connections are spliced to form a single end-to-end connection. Rather than utilizing a known splicing technique which essentially short circuits TCP sockets without going through the application buffer, the present invention operates below the protocol stack on top of the link layer between the routing and network layers to directly manipulate the packets and forward them between the subscriber and the origin server. That is, the present invention directly manipulates the packet headers to modify or adjust the sequencing, checksums, and CRC data while essentially transferring additional transport layer semantics to the end-points, i.e. the subscriber and the origin server. By avoiding the use of socket connections, the present invention requires fewer resources for the file system, buffers, etc. and is capable of operating with a resource-limited operating system.

If the proxy configuration has been previously determined and stored in the subscriber information database, block **550** proceeds to block **570** or block **572**. For users configured to use a proxy server, the proxy request is modified by block **570** prior to connecting to the origin server and splicing the connections as described above. Likewise, if the subscriber is not configured to use a proxy server, no manipulation of the packet is required. However, proxy use may be required by the access provider as a means to improve security or performance. In this case, a direct request from the subscriber will be modified to use the proxy server specified by the access provider. For subscribers configured to use a proxy server, proxy requests may be directed to the proxy server specified by the access provider whether or not the originally specified proxy server is available or not. A connection to the origin server is then established and the connections are spliced as indicated by blocks **572** and **574**.

Referring now to FIG. **14**, an alternative representation of a proxy determination algorithm for use in a configuration manager/adapter according to one embodiment of the present invention is shown. After establishing a connection between the subscriber and the configuration manager, the configuration manager must examine the contents or payload of the packet to determine whether an HTTP proxy request (or other proxy request) is contained therein. Block **580** examines the first line of data to determine whether it contains a method, request, and HTTP version information. If not, nothing is returned as represented by block **584**. Otherwise, block **582** examines the request URI to determine whether it is an absolute URI. If not, nothing is returned as indicated by block **584**. Otherwise, the method information is examined as represented by block **586**. If the method information is not recognized, an appropriate message is returned as represented by block **590**. Otherwise, the method, absolute URI, and HTTP version are returned as indicated by block **588**.

A more detailed representation of HTTP proxy processing for packets received through the subscriber interface is provided by FIGS. **15***a*–**11***c*. FIGS. **15***a*–**15***c* provide a more detailed illustration and description of the operations performed by block **372** of FIG. **7***b* and provide an alternate representation of the functions illustrated in FIG. **13**.

Block **600** determines whether the subscriber has previously been determined to be using a proxy server. If the proxy status for the subscriber is unknown or determined to be yes, block **602** examines the destination port to determine whether it is a proxy port. If the result is negative, processing continues as represented by block **622**. Otherwise, or if the proxy status is unknown, block **604** determines whether any session mapping has been established. If yes, block **606** determines whether to reset the connection, in which case the session state is set to close as represented by block **608** and the packet is caused to be dropped as represented by block **610**. Otherwise, the session state is examined at **612** to determine subsequent processing as represented by blocks **614**, **616**, **618**, **620**, and **622**. If a SYN (synchronization request) has been received as reflected by the session state, block **614** determines whether an acknowledgment (ACK) has been received. The acknowledgment is then examined for a proper value as represented by block **624**. If an appropriate acknowledgment is received, the session state is changed to "established" as represented by block **628**. Otherwise, a connection reset is sent to the subscriber and the session state is changed to "closed" as represented by block **630**. Similarly, if no acknowledgment and no synchronization have been received as indicated by blocks **614** and **626**, respectively, the connection is reset and the session state is closed. Otherwise, block **632** determines whether the acknowledgment is greater than a maximum value, in which

case a packet drop is requested as represented by block **610**. If the maximum is not exceeded, block **676** sends a SYN/ACK to the subscriber and updates the session state appropriately.

Session state FIN_WAIT1 is used to accommodate slow links in resolving DNS requests. Block **616** detects the state transition to the first wait state. Any errors are removed from the retransmit queue and the session state is changed to the second wait state (FIN_WAIT2) as represented by block **634**. Otherwise, a connection reset is sent to the subscriber and the session is closed as represented by block **636**.

Likewise, in the second wait state as determined by block **618**, if a FIN is not received, a subscriber reset is generated as indicated by block **636**. If a FIN is received, an appropriate acknowledgment as represented by block **638** is sent. The session mapping is subsequently removed as represented by block **640**.

For an established HTTP connection as indicated by block **620** (FIG. **15***c*), block **642** determines whether the packet includes a proxy request as explained in greater detail with reference to FIGS. **13** and **14**. If not, the subscriber database entry is updated to indicate that the HTTP proxy is not being used as represented by block **644** (FIG. **15***b*). A reply is generated to redirect the subscriber to the origin server with an appropriate reply in the retransmit queue as represented by blocks **646** and **648**.

If a proxy request is detected by block **642** (FIG. **15***c*), a session ALG is called to process the proxy request and the subscriber database is updated for this subscriber. If the packet contains a DNS name as represented by block **652**, an attempt to resolve the host name is performed as indicated by block **654**. Otherwise, the destination IP address is set to the URL and the packet is stored as represented by blocks **656** and **664**, respectively. Likewise, if block **654** is able to resolve the host name, a packet is stored with the destination IP address as resolved by the DNS and the package is stored as represented by block **664**. Otherwise, an error response is generated and the session state is updated with an appropriate error response placed in the retransmission queue as represented by blocks **658** and **660**. Once the packet is stored, blocks **666** and **668** attempt to establish a connection with the origin server using the resolved destination IP address.

If a session mapping has not been created as determined by block **604** (FIG. **15***a*), and a SYN has been received as indicated by block **670**, a session mapping is created with the proxy status set to "unknown" as represented by block **672**. Once the session has been created as indicated by block **674**, an appropriate SYN/ACK is sent over the subscriber interface and the session state is appropriately updated as indicated by blocks **674** and **676**. For established sessions which are not HTTP sessions as indicated by block **620** (FIG. **15***c*), block **662** changes the destination IP address to the packet destination IP address. The packet is then stored as indicated by block **664**. A connection with the origin server is then established as indicated by blocks **666** and **668**.

A block diagram illustrating a HTTP proxy ALG for packets received from the network interface is illustrated in FIG. **16**. This diagram represents a state transition diagram for the server state as indicated by block **680**. Depending upon the particular state, processing proceeds via blocks **682**, **684**, and **686**. For the SYN_SENT state, block **682** determines whether a SYN/ACK packet has been received. If such packet has not been received, or the acknowledgment is not valid as indicated by block **684**, then the connection between the origin server and the configuration manager is reset as indicated by block **692**. A drop request is then returned by block **690**. If a valid acknowledgment is received, block **686** forwards the acknowledgment to the subscriber side via the subscriber interface and updates the server state to "established." The stored packet is then sent as represented by block **688**.

For the "established" state, block **684** determines whether an HTTP packet has been received. If so, the response received from the origin server is appropriately modified prior to sending to the subscriber via the subscriber interface as indicated by block **694**. The server state is then updated to "spliced." The appropriate response is then placed in the retransmit queue as indicated by block **696** prior to returning a drop request at block **690**.

If a packet is not an HTTP packet, the server state is updated to "spliced" as indicated by block **698** and the ALG returns a "continue" as indicated by block **686**. Once the connection is spliced, the server state is set accordingly and additional requests are not processed by the ALG.

FIG. **17** provides a transaction diagram to illustrate a typical HTTP proxy request processed by a configuration manager/adapter according to one embodiment of the present invention. The HTTP proxy request originates from an appropriate application, such as a browser running on subscriber **710**. A synchronization (SYN) request is generated by subscriber **710** and passed to configuration manager **714** via the subscriber interface (not specifically illustrated). The SYN packet includes the subscriber's sequence number which is 4000 in this example as represented by reference numeral **716**. Configuration manager **714** replies with an ACK/SYN packet with an acknowledgment of 4001 and its sequence number which is 1 in this example as represented by reference numeral **718**. The reply is generated by configuration manager **714** and passed to subscriber **710** via the subscriber interface of configuration manager **714**.

Subscriber **710** then responds with an ACK packet **720** and an HTTP proxy request **722** having an ACK value of 2 and sequence value of 4001. Configuration manager **714** then attempts to establish a connection with the web/proxy server **712** over the foreign network via the network interface of the configuration manager **714**. The original sequence number generated by subscriber **710** is used in the synchronization request to the web/proxy server **712** as represented by reference numeral **724**. Server **712** responds with an ACK/SYN packet having its sequence number (5000 in this example) and an acknowledgment number corresponding to the sequence number of the synchronization request as indicated at **726**. Configuration manager **714** generates an appropriate ACK packet to reply to server **712** as indicated at **728** to establish the connection. Configuration manager **714** then modifies the HTTP proxy request **722** to an HTTP request with the established acknowledgment and sequence numbers as represented by reference numeral **730**. Server **712** replies to configuration manager **714** with an HTTP response **732** which is forwarded as an HTTP proxy response from configuration manager **714** to subscriber **710** as indicated at **734**. This is followed by HTTP data **736** which is forwarded at **738** to subscriber **710**. The connection between proxy server **712** and configuration manager **714** is closed by the request **740**. The connection between the configuration manager **714** and subscriber **710** is then closed via an appropriate request **742**.

The separate connections between subscriber **710** and configuration manager **714**, and between configuration manager **714** and server **712** may be spliced to reduce or

eliminate processing by configuration manager **714**. According to the present invention, the connection is preferably spliced by directly manipulating the packet without having to copy its contents or payload. For example, the sequence numbers, SYNs and ACKs, may be manipulated with corresponding adjustments (and padding if necessary) to the checksum and CRC so subscriber **710** maintains a single connection with server **712**.

FIGS. **18** and **19** provide more detailed representations of a DNS ALG for use with a configuration manager according to one embodiment of the present invention. The DNS ALG may be used to determine the proxy configuration settings as described above. Alternatively, or in combination, the DNS ALG illustrated in FIGS. **18** and **19** may be used for DNS redirection. For example, subscribers may be configured to utilize a DNS server having a private IP address and/or located behind an enterprise firewall. Alternatively, the requested domain name server may be a significant number of hops from the foreign network resulting in a slow response time when network traffic is high. The DNS redirection of the present invention receives a DNS request from the subscriber and changes the request to a local DNS server to attempt to resolve the domain name rather than the requested, possibly (likely) unavailable server. This differs slightly from the proxy detection method which may resolve the DNS request to the configuration manager's own IP address to determine the proxy configuration of the subscriber. In particular, if DNS redirection is enabled, all DNS requests are redirected to DNS servers which are local to the foreign network.

FIG. **18** illustrates processing of a packet received via the subscriber interface of the configuration manager. Block **760** determines whether there is DNS information in the session table for the current session. If not, block **762** allocates new DNS information and associates it with the current session. The requested DNS IP address is stored and a counter is initialized. Block **764** examines the counter to determine if it has exceeded a maximum value. If not, the IP address is changed to a first local DNS server address as indicated by block **768**. The packet is then sent out over the network interface as represented by block **776**. If all local DNS servers have been exhausted, i.e. the DNS counter exceeds the maximum, block **770** determines whether the subscriber is using a proxy server based on information stored in the subscriber database. If unknown, the DNS request is placed in a timeout queue as indicated by block **772**. If the request is not answered, or answered in the negative, the DNS request may be resolved with the IP address of the configuration manager to determine the proxy settings as described above.

Once the proxy status has been determined and stored in the subscriber database, block **774** attempts to resolve the address using a local server. The IP destination address is changed to the address for the current attempt and the counter is incremented. The packet is then sent over the network interface as represented by block **776**.

Referring now to FIG. **19**, packets received via the network interface are examined to determine whether DNS information for the current session exists at block **790**. If not, no action is taken and the process completes as indicated by block **802**. If DNS information exists for the current session, block **792** determines whether the subscriber proxy settings are known by examining a corresponding entry in the subscriber database. If the status is unknown, block **794** removes the DNS request from the timeout queue and block **796** determines whether a negative response to the DNS request has been received. If a negative response is received, or if the request times out, the IP source address is changed to the IP address of the configuration manager of block **800**. Otherwise, the local DNS request was successful and the IP source address is changed to the local DNS server as indicated at **798**. The processing then continues via block **802**.

FIG. **20** provides a block diagram illustrating operation of a generic service redirector according to one embodiment of the present invention. Redirection may be provided for a variety of services including DNS, SMTP, and the like. Subscriber **820** is connected to a first network, such as home LAN **822**. Subscriber **820** communicates with one or more servers to provide local (home) services as represented by block **826**. Such services may include SMTP for email transactions, DNS, and the like. As illustrated in FIG. **20**, the servers providing local service may be located on home LAN **822** which is protected by an enterprise firewall **824**. Alternatively, service may be provided by servers located at the NSP, or available over a wide area network, such as the Internet, as represented by block **832**. In either case, subscriber **820** is preconfigured to access a particular service by IP address or domain name. To access alternate service **832**, subscriber **820** may communicate across home LAN **822**, through firewall **824** and router **828**.

When subscriber **820** moves to a remote location which is serviced by foreign LAN **836**, the preconfigured service or servers may be unavailable or provide poor response due to the network traffic and location of the servers. In addition, various network service providers may prevent access to services from a foreign network. For example, many ISPs prevent access to the SMTP server from an unregistered network address because SMTP does not have built-in authentication and authorization features. This may be enforced to prevent, or at least hinder, spoofing, for example. As such, when subscriber **820** relocates to foreign LAN **836**, SMTP service may not be available even though the home SMTP server is publicly addressable.

To provide complete transparency to the subscriber **820** while interfacing with the foreign LAN **836**, the present invention may redirect various service requests to a substitute local service as represented by **840**. As such, configuration manager/adapter **838** receives a request for a preconfigured service as represented by **842**. Configuration manager **838** redirects the request to a local server which can service the request. In the case of an SMTP request, the source address of the subscriber **820** is preferably maintained such that any replies are routed back to the home LAN **822** of subscriber **820**. However, outbound traffic is redirected to a local substitute service **840** which then directs the messages to their final destination as specified by subscriber **820**. Depending upon the particular application, the substitute local service **840** may be integrated within configuration manager/adapter **838**.

FIG. **21** illustrates an FTP proxy ALG according to one embodiment of the present invention. The FTP proxy ALG functions in a similar manner to the HTTP proxy processing as described in detail above. FTP commands proxied through an HTTP browser are sent as HTTP requests. As such, to determine whether a particular packet contains an FTP proxy request, a connection must first be established between the configuration manager/adapter and the subscriber. An additional complicating feature of the FTP proxy is that FTP provides for an active mode transfer in which the host opens a new connection to the user or subscriber for each FTP file request. As such, multiple sessions are created for data channels which must be processed by the FTP ALG. A passive FTP mode is also provided in which the control

channel is also used to transfer data. As such, it is necessary only to modify the header of any packets and not the content.

As illustrated in FIG. **21**, a connection between the subscriber and configuration manager/adapter is established as indicated by block **850**. The content of the data is examined to determine whether the request is a FTP proxy request as represented by block **852**. The configuration manager/adapter attempts to establish a connection with the requested FTP server as represented by block **854**. Once established, FTP commands contained within the packet are extracted and forwarded to the FTP server as represented by block **856**. Rather than incur the additional overhead to maintain two separate connections between the subscriber and the configuration manager, and between the configuration manager and the FTP server, the connection is preferably patched or spliced as represented by block **858** to improve throughput. As described above, this requires direct manipulation or modification of the header information, including the sequencing, and forwarding the packet to the intended destination.

Thus, the present invention provides a subscriber transparent access to a foreign network using a configuration manager/adapter which adapts the subscriber to the foreign network without making any changes to the subscriber's settings which would require user intervention to reconnect to a home network. The configuration manager/adapter of the present invention selectively determines whether a particular communication parameter or service request needs to be adapted and may only process those requests which are mis-configured to minimize processing overhead. By operating below the protocol stack, the present invention provides improved processing efficiency and greater throughput in a scalable architecture capable of multiple thousands of concurrent sessions.

While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention.

What is claimed is:

1. A method for providing connectivity to a foreign network for a device having network settings configured for communication over a home network without reconfiguring the network settings of the device, the method comprising:

intercepting packets transmitted by the device;

selectively modifying intercepted packets which are incompatible with network settings configured for communication over the foreign network to be compatible with the network settings configured for communication over the foreign network, wherein the network settings configured for communication over the home and foreign networks include respective IP addresses, gateway addresses, subnet masks, DNS addresses, and protocol proxies; and

selectively providing network services for the device corresponding to network services available on the home network to reduce delay associated with accessing the network services from the foreign network, or to provide network services otherwise inaccessible from the foreign networks wherein selectively providing network services comprises providing a proxy service which includes resolving a domain name to an address;

wherein resolving a domain name to an address includes;

establishing a connection between the device and a configuration adapter in order for the configuration adapter to intercept packets transmitted by the device;

examining contents of the intercepted packets to identify a domain name;

resolving the domain name to an address;

establishing a connection between the configuration adapter and a computer at the address corresponding to the domain name; and

splicing the connections between the device and the configuration adapter, and between the configuration adapter and the computer, to form a single connection between the device and the computer such that the device and the computer communicate packets with each other over the single connection without the network settings of the device being reconfigured.

2. The method of claim **1** wherein the proxy service comprises a hypertext transfer protocol proxy service.

3. The method of claim **1** wherein the proxy service comprises a file transfer protocol proxy service.

4. The method of claim **1** wherein resolving a domain name to an address comprises:

attempting to resolve the domain name to an address using a domain name server accessible from the foreign network; and

resolving the domain name to an address corresponding to a configuration adapter after a predetermined timeout period expires, or if domain name servers accessible from the foreign network can not resolve the domain name.

5. The method of claim **1** wherein splicing the connections comprises directly modifying subsequently intercepted packets without copying the packet payload.

6. The method of claim **1** wherein resolving the domain name to an address comprises using a domain name server accessible from the foreign network.

7. The method of claim **1** wherein resolving the domain name to an address comprises:

resolving the domain name to an address using a domain name server;

attempting to establish a connection with the computer at the address corresponding to the domain name;

resolving the domain name to an address corresponding to the configuration adapter after expiration of a predetermined timeout period;

wherein the step of splicing is performed after receiving a delayed response from the computer at the address corresponding to the domain name.

8. The method of claim **1** wherein selectively providing network services comprises providing an outgoing email service.

9. The method of claim **8** wherein providing an outgoing email service comprises modifying intercepted simple mail transport protocol (SMTP) packets to redirect the intercepted SMTP packets to an SMTP server on the foreign network.

10. The method of claim **8** wherein providing an outgoing email service comprises modifying intercepted simple mail transport protocol (SMTP) packets to redirect the intercepted SMTP packets to an SMTP server on the foreign network without modifying the source address of the SMTP packet packets.

11. The method of claim **1** wherein selectively providing network services comprises redirecting domain name service requests to a local domain name server for the foreign network.

12. Apparatus for providing connectivity to a foreign network for a device having network settings configured for communication over a home network without reconfiguring the network settings of the device, the apparatus comprising:

means for intercepting packets transmitted by the device;

means for selectively modifying intercepted packets which are incompatible with network settings configured for communication over the foreign network to be compatible with the network settings of configured for communication over the foreign network, wherein the network settings configured for communication over the home and foreign networks include respective IP addresses, gateway addresses, subnet masks, DNS addresses, and protocol proxies; and

means for selectively providing network services for the device corresponding to network services available on the home network to reduce delay associated with accessing the network services from the foreign network, or to provide network services otherwise inaccessible from the foreign network;

wherein the means for selectively providing network services comprises means for providing a proxy service;

wherein the means for providing a proxy service comprises means for resolving a domain name to an address;

wherein the means for resolving a domain name to an address includes;

means for establishing a connection between the device and a configuration adapter in order for the configuration adapter to intercept packets transmitted by the device;

means for examining contents of the intercepted packets to identify a domain name;

means for resolving the domain name to an address;

means for establishing a connection between the configuration adapter and a computer at the address corresponding to the domain name; and

means for splicing the connections between the device and the configuration adapter, and between the configuration adapter and the computer, to form a single connection between the device and the computer such that the device and the computer communicate packets with each other over the single connection without the network settings of the device being reconfigured.

13. The apparatus of claim 12 wherein the proxy service comprises a hypertext transfer protocol proxy service.

14. The apparatus of claim 12 wherein the proxy service comprises a file transfer protocol proxy service.

15. The apparatus of claim 12 wherein the means for resolving a domain name to an address comprises:

means for attempting to resolve the domain name to an address using a domain name server accessible from the foreign network; and

means for resolving the domain name to an address corresponding to the configuration adapter after a predetermined timeout period expires, or if the domain name servers accessible from the foreign network can not resolve the domain name.

16. The apparatus of claim 12 wherein the means for splicing the connections comprises means for directly modifying subsequently intercepted packets without copying the packet payload.

17. The apparatus of claims 12 wherein the means for resolving the domain name to an address comprises means for using a domain name server accessible from the foreign network.

18. The apparatus of claim 12 wherein the means for resolving the domain name to an address comprises:

means for resolving the domain name to an address using a domain name server;

means for attempting to establish a connection with the computer at the address corresponding to the domain name;

means for resolving the domain name to an address corresponding to the configuration adapter after expiration of a predetermined timeout period;

wherein the means for splicing performs the splicing only after receiving a delayed response from the computer at the address corresponding to the domain name.

19. The apparatus of claim 12 wherein the means for selectively providing network services comprises means for providing an outgoing email service.

20. The apparatus of claim 19 wherein the means for providing an outgoing email service comprises means for modifying intercepted simple mail transport protocol (SMTP) packets to redirect the intercepted SMTP packets to an SMTP server on the foreign network.

21. The apparatus of claim 19 wherein the means for providing an outgoing email service comprises means for modifying intercepted simple mail transport protocol (SMTP) packets to redirect the intercepted SMTP packets to an SMTP server on the foreign network without modifying the source address of the SMTP packets.

22. The apparatus of claim 12 wherein the means for selectively providing network services comprises means for redirecting domain name service requests to a local domain name server for the foreign network to improve response time.

23. A configuration adapter for providing connectivity to a foreign network for a device having network settings configured for communication over a home network without reconfiguring the network settings of the device, the configuration adapter comprising:

at least one network interface for connecting to the foreign network; and

a processor in communication with the network interface, the processor intercepting packets transmitted by the device, selectively modifying intercepted packets which are incompatible with network settings configured for communication over the foreign network to be compatible with the network settings of configured for communication over the foreign network, and selectively providing network services for the device corresponding to network services available on the home network to reduce delay associated with accessing the network services from the foreign network, or to provide network services otherwise inaccessible from the foreign network;

wherein the network settings configured for communication over the home and foreign networks include respective IP addresses, gateway addresses, subnet masks, DNS addresses, and protocol proxies;

wherein the processor selectively provides a proxy service for the device which includes resolving a domain name to an address;

wherein the processor resolves a domain name to an address by establishing a connection between the device and the configuration adapter, examining contents of the intercepted packets to identify a domain name, resolving the domain name to an address, establishing a connection between the configuration adapter and a computer at the address corresponding to the

domain name, and splicing the connections between the device and the configuration adapter, and between the configuration adapter and the computer, to form a single connection between the device and the computer such that the device and the computer communicate packets with each other over the single connection without the network settings of the device being reconfigured.

24. The configuration adapter of claim **23** wherein the proxy service comprises a hypertext transfer protocol proxy service.

25. The configuration adapter of claim **23** wherein the proxy service comprises a file transfer protocol proxy service.

26. The configuration adapter of claim **23** wherein the processor attempts to resolve the domain name to an address using a domain name server accessible from the foreign network, and resolves the domain name to an address corresponding to the configuration adapter after a predetermined timeout period expires, or if the domain name servers accessible from the foreign network can not resolve the domain name.

27. The configuration adapter of claim **23** wherein the processor splices the connections by directly modifying subsequently intercepted packets without copying the packet payload.

28. The configuration adapter of claim **23** wherein the processor resolves the domain name to an address using a domain name server accessible from the foreign network.

29. The configuration adapter of claim **23** wherein the processor resolves the domain name to an address by:

resolving the domain name to an address using a domain name server;

attempting to establish a connection with the computer at the address corresponding to the domain name;

resolving the domain name to an address corresponding to the configuration adapter after expiration of a predetermined timeout period; and

splicing the connections after receiving a delayed response from the computer at the address corresponding to the domain name.

30. The configuration adapter of claim **23** wherein the processor selectively provides an outgoing email service.

31. The configuration adapter of claim **30** wherein the processor provides an outgoing email service by redirecting intercepted simple mail transport protocol (SMTP) packets to an SMTP server configured to process mail from addresses on the foreign network.

32. The configuration adapter of claim **30** wherein the processor redirects intercepted simple mail transport protocol (SMTP) packets without modifying the source address of the SMTP packets.

33. The configuration adapter of claim **30** wherein the processor redirects domain name service requests to a local domain name server for the foreign network.

34. A method for providing access to a second local area network for a device configured to communicate over a first local area network having incompatible network settings with network settings of the second local area network, the method comprising:

determining whether an application running on the device is requesting a proxy service;

wherein the step of determining comprises:

establishing a transmission control protocol (TCP) connection between a configuration adapter and the device to examine contents of a packet transmitted by the device;

establishing a TCP connection between the configuration adapter and the proxy server requested by the application; and

splicing the connection such that end-to-end semantics are maintained by the application and the requested proxy server, and

modifying packets containing proxy requests to direct requests if the requested proxy service is inaccessible from the foreign network without modifying the network settings of the device.

35. The method of claim **34** wherein the step of splicing comprises:

implementing a subset of network protocol functionality to intercept each packet from the application without passing the packet through an RFC-compliant protocol stack.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,857,009 B1
DATED : February 15, 2005
INVENTOR(S) : Manuel Ferreria et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 21,
Line 63, delete "networks" and insert therefor -- networks; --
Line 67, delete "includes;" and insert therefor -- includes: --.

Column 22,
Line 63, delete "packet".

Column 23,
Line 9, delete "of".

Signed and Sealed this

Twenty-fourth Day of May, 2005

JON W. DUDAS
Director of the United States Patent and Trademark Office

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge A. Howard Matz and the assigned discovery Magistrate Judge is Carla Woehrle.

The case number on all documents filed with the Court should read as follows:

CV10- 381 AHM (CWx)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

==========

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

[X] **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

[ ] **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

[ ] **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.