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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2002 (28.02.2002)

PCT

(10) International Publication Number
WO 02/17035 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/KR01/01419

(22) International Filing Date: 22 August 2001 (22.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/227,569 23 August 2000 (23.08.2000) US
09/756,979 9 January 2001 (09.01.2001) US

(71) Applicant: **GREAT HUMAN SOFTWARE CO., LTD.** [KR/KR]; 85-3, 10F Allianzfirstlife-Building, Seosomun-Dong, Jung-Gu, Seoul 100-110 (KR).

(72) Inventors: **LEE, Ken, Young-sang**; 226 Airport Parkway, Suite 240, San Jose, CA 95110 (US). **LEE, Jong-woo**; 226 Airport Parkway, Suite 240, San Jose, CA 95110 (US).

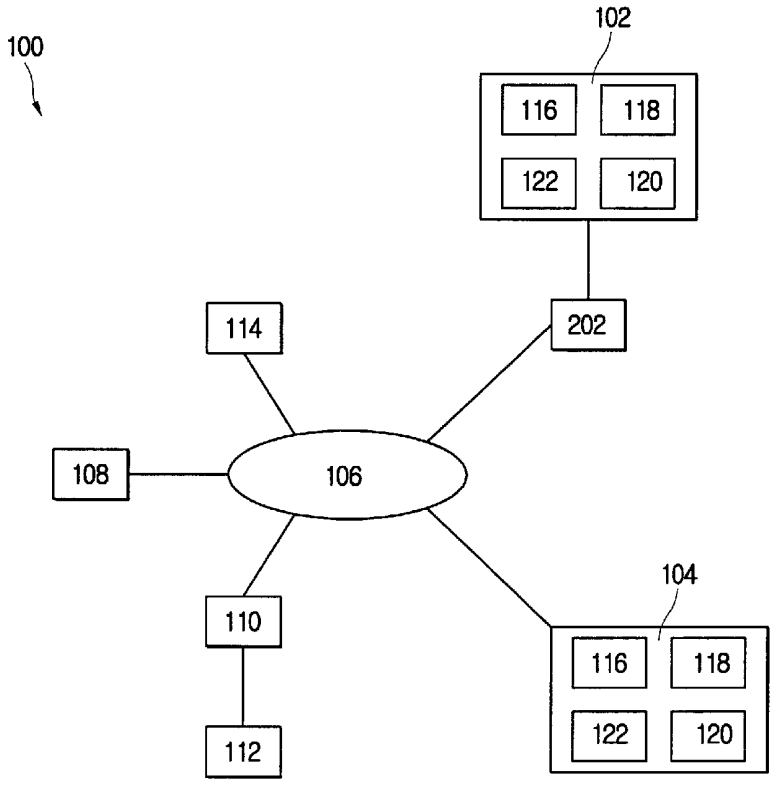
(74) Agent: **L & K PATENT FIRM**; 701, Daekun Building, 822-5, Yeoksam-Dong, Kangnam-Gu, Seoul 135-080 (KR).

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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR ESTABLISHING CONNECTIONS BETWEEN TERMINALS CONNECTED TO NETWORK ENVIRONMENTS HAVING DIFFERENT IP-ADDRESSING SCHEMES



(57) Abstract: A method and system is provided for establishing a connection between a first terminal connected to a router in a first-network environment and a second terminal in a second-network environment. In one embodiment, a connection is established from the first terminal to a server that lies outside of the first-network environment. The first terminal then transmits a packet to the server through the router. The server then determines the IP address and port number utilized by the router to transmit the packet to the server. This IP address and port number is then transmitted to the second terminal, which then establishes a connection to the first terminal.

WO 02/17035 A2

Published:

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

— *entirely in electronic form (except for this front page) and available upon request from the International Bureau*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR ESTABLISHING CONNECTIONS BETWEEN TERMINALS CONNECTED TO NETWORK ENVIRONMENTS HAVING DIFFERENT IP-ADDRESSING SCHEMES

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to establishing connections between terminals, and more particularly to establishing connections between terminals connected to network environments having different Internet Protocol (IP) addressing schemes.

2. Description of the Related Art

In general, routers are utilized to connect network environments that utilize different IP-addressing scheme. For example, a Virtual Private Network (VPN) router can be utilized to connect terminals behind the router to the Internet. The terminals behind the router are assigned virtual-IP addresses rather than standard-IP addresses, such as those assigned by InterNIC. As such, when a terminal behind the router sends a packet to a terminal outside of the VPN router, the virtual-IP address of the terminal behind the router is replaced by the real-IP address of the VPN router.

One disadvantage of utilizing routers is that terminals outside of the router generally cannot initiate connections with terminals behind the router. For example, in the VPN-network environment described above, the terminal behind the VPN router only has a virtual-IP address. Accordingly, a terminal outside of the VPN router cannot initiate a connection with the terminal behind the VPN router.

SUMMARY OF THE INVENTION

The present invention relates to a method and system for establishing a connection between a first terminal in a first-network environment and a second terminal in a second-network environment. In accordance with one aspect of the present invention, the first-network environment and the second-network environment utilize different Internet Protocol (IP) addressing schemes. As such, the first terminal is connected to a router. In one embodiment, a connection is established from the first terminal to a server that lies outside of the first-network environment. The first terminal then transmits a packet to the server through the router. The server then determines the IP address and port number utilized by the router to transmit the packet to the server. This IP address and port number is then transmitted to the second terminal, which then establishes a connection to the first terminal.

DESCRIPTION OF THE DRAWING FIGURES

The present invention can be best understood by reference to the following description taken in conjunction with the accompanying drawing figures, in which like parts may be referred to by like numerals:

Fig. 1 is a block diagram of one embodiment of the present invention;

Fig. 2 is a block diagram of another embodiment of the present invention;

Fig. 3 is a block diagram of still another embodiment of the present invention;

Fig. 4 is a block diagram of yet another embodiment of the present invention; and

Fig. 5 is a flow diagram

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

In order to provide a more thorough understanding of the present invention, the following description sets forth numerous specific configurations, parameters, and the like. It should be recognized, however, that such description is not intended as a limitation on the scope of the present invention, but is instead provided to provide a better description of exemplary embodiments.

With reference to Fig. 1, in one exemplary embodiment of the present invention, an IP telephony system 100 includes terminals 102 and 104 connected to a computer network 106. In the present exemplary embodiment, terminals 102 and 104 are configured to conduct IP-based telephony through computer network 106. More particularly, as will be described in greater detail below, terminals 102 and 104 are configured to transmit and receive data through computer network 106 in accordance with the H.323 standard established by the International Telecommunications Union (ITU).

Although the H.323 standard provides for audio, video, and data communication, the portions of this standard that relates to audio communication is becoming heavily used in IP-based telephony. More particularly, in accordance with the H.323 standard, terminals 102 and 104 are configured to support H.245 for negotiating channel usage and capabilities. Terminals 102 and 104 are also configured to support Q.931 for call signaling and setup.

In the present exemplary embodiment, each terminal 102 and 104 includes a microphone 118 and speaker 120 configured to capture and reproduce audio signals, respectively. It should be recognized that microphones 118 and speakers 120 can be integrated into terminals 102 and 104. Alternatively, they can be accessories that connect to terminals 102 and 104. Furthermore, they can be configured as a headset unit.

Each terminal 102 and 104 also includes a coder/decoder (CODEC) 122 configured to convert analog signals to digital signals and vice versa. Furthermore, in the present embodiment, CODEC 122 is configured to facilitate signal compression in accordance with the G.729 standard. It should be recognized, however, that any H.323 compliant signal compression routine can be used, such as G.711, G.723, and the like.

Each terminal 102 and 104 further includes an interface program 116. In the present embodiment, interface program 116 includes system-control routines for conducting communication in accordance with H.323 standards, including H.245 and Q.931. Interface program 116 is configured to support RTP/RTCP and RAS (Registration/Admission/Status) protocol. As will be described in greater detail, interface program 116 can also include various additional routines for conducting telephony through computer network 106.

In one embodiment, interface program 116 can be implemented as a computer software program written using the C programming language. But it should be recognized that interface program 116 can be implemented using any convenient programming language. For example, interface program 116 can be implemented using JAVA or PERL programming languages. These programming languages have the

advantage that programs written in them can operate independent of the operating system of the terminals on which the programs are executed.

In the present embodiment, interface program 116 can be installed on terminals 102 and 104 by down-loading it from a web site. It should be recognized, however that interface program 116 can be installed on terminals 102 and 104 using any convenient method. For example, interface program 116 can be distributed on any convenient storage medium, such as diskettes, compact disks, and the like.

Terminals 102 and 104 can include personal computers, such as desk-top computers, lap-top computers, workstations, and the like. It should be recognized, however, that terminals 102 and 104 can include any device configured to communicate with computer network 106, such as a teleconference system, a personal digital assistance (PDA), an internet appliance, and the like. It should also be recognized that terminals 102 and 104 need not be all the same type of devices. By way of example, terminal unit 102 can be a workstation running a Unix operating system. Terminal unit 104 can be an Intel-based computer running a Microsoft Windows operating system from Microsoft Corporation of Redmond Washington. Additionally, although terminals 102 and 104 are depicted, it should be recognized that IP telephony system 100 can include any number of terminals 102 and 104.

In the present exemplary embodiment, IP telephony system 100 can also include a gatekeeper 108, a gateway 110, and a Multipoint Control Unit (MCU) 114. As will be described in greater detail below, these additional components of IP telephony system 100 are also configured to facilitate IP-based telephony in accordance with the H.323 standard.

More particularly, gatekeeper 108 can be configured to provide call control services to terminals 102 and 104. Gatekeeper 108 can be configured to translate Local Area Network aliases to IP or IPX addresses. Gatekeeper 108 can also be configured to provide bandwidth management and to route calls.

Gateway 110 can be configured to provide translation functions between different terminal types. For example, gateway 110 can be connected to a telephone unit 112, which in turn is connected to the PSTN (Public Switched Telephone Network). As such, gateway 110 can translate between IP-based computer network 106 and the switched-circuit based PSTN. Gateway 110 can also perform call setup and clearing on both the LAN and the PSTN sides.

MCU 114 can be configured to support conferences between three or more terminals. Thus, MCU 114 can be configured to handle H.245 negotiations between terminals to determine common compatibility.

In accordance with one aspect of the present invention, interface program 116 registers terminals 102 and 104 when they connect to computer network 106. More particularly, in the present embodiment, when terminal 102 connects to computer network 106, interface program 116 installed on terminal 102 registers with gatekeeper108 by sending a GRQ (Gatekeeper Request) to gatekeeper 108. In response, gatekeeper 108 sends a GCF (Gatekeeper Confirm) message to terminal 102. Terminal 102 then sends a RPQ (Registration Request) message to gatekeeper 108. In response, gatekeeper 108 sends a RCF (Registration Confirm) message to terminal 102. In the present embodiment, all of these messages (i.e., GRQ, GCF, RPQ, and RCF messages) are sent using UDP (User Datagram Protocol). In a similar manner, interface program 116 installed on terminal 104 registers with gatekeeper 108.

In the present embodiment, the IP addresses of terminals 102 and 104 are registered with gatekeeper 108. It should be recognized that additional data can also be registered with gatekeeper 108. For example, in an alternative embodiment, a unique Personal Communication Number (PCN) is assigned to each terminal connected to IP telephony system 100.

Have thus described the manner in which terminals 102 and 104 registers with gatekeeper 108, assume for example that terminal 102 wants to call terminal 104. The description below provides an example of establishing a connection between terminals 102 and 104 using the H.323 standard for a call from terminal 102 to terminal 104.

In the present embodiment, terminal 102 first sends an ARQ (Admission Request) message to gatekeeper 108 requesting the IP address of terminal 104. In response, gatekeeper 108 sends an ACF (Admission Confirm) message to terminal 102 transmitting the IP address for terminal 104. Next, terminal 102 opens a signaling channel with terminal 104 using the H.225 standard. Terminal 102 then sends a call setup H.225/Q.931 setup message. In response, terminal 104 sends an Alert (Ringing) message H.225/Q.931 setup message to terminal 102. Terminal 104 then sends a connect message H.225/Q.931 setup message to terminal 102. Next, terminal 102 makes a TCP (Transmission Control Protocol) connection with terminal 104 by opening a signaling channel using H.245. Terminal 102 then sends a Terminal Capability Request message using H.245 to terminal 104. In response, terminal 104 sends a terminal capability ACK (Acknowledgement). Terminal 102 then sends a Master Slave Determination message using H.245 to terminal 104. In response, terminal 104 sends a Master Slave Determination ACK (Acknowledgement) using H.245. In the present

embodiment, the ARQ and ACF messages are sent using UDP and the remaining messages are sent using TCP.

In the example above, terminals 102 and 104 were presumed to have real IP addresses, meaning that each IP address is unique. When computer network 106 includes the Internet, a real IP address is assigned by InterNIC and is unique to each terminal connected to the Internet.

But in some applications of the present invention, terminal 102 and/or terminal 104 can have virtual IP addresses. More particularly, with reference to Fig. 2, in another embodiment of the present invention, terminal 102 can be connected to computer network 106 through a VPN (Virtual Private Network) router 202. As such, terminal 102 is assigned a virtual IP address rather than a real IP address. Thus, when terminal 102 sends data out to computer network 102, the data includes the real IP address of VPN router 202 rather than the virtual IP address of terminal 102. This can be problematic in conducting IP-based telephony between terminals 102 and 104.

To more clearly illustrate the problem described above, assume for example that terminal 102 has a virtual IP address of 10.10.10.20 and that VPN router 202 has a virtual IP address of 10.10.10.1 and a real IP address of 210.119.58.40. As alluded to above, when terminal 102 sends a packet, for example to gatekeeper 108 or terminal 104, the IP address associated with that packet will be the real IP address of VPN router 202 (i.e., 210.119.58.40) rather than the address of terminal 102. Thus, gatekeeper 108 and terminal 104 do not know the IP address of terminal 102. Moreover, terminal 102 does not know the real IP address of VPN router 202 that was used to send out the packet. This can interfere with the transmission of audio packets in accordance with the H.323 standard for conducting IP-based telephony.

Consequently, in one embodiment of the present invention, terminal 102 and gatekeeper 108 are configured to facilitate IP-based telephony using H.323 standard even when terminal 102 is behind VPN router 202. More particularly, interface program 116 installed in terminal 102 is configured to transmit a packet to gatekeeper 108. When this packet is received, gatekeeper 108 is configured to examine it to determine the port number and the IP address used to send the packet. Gatekeeper 108 then sends this information in another packet to the port number and the IP address used to send the received packet. This subsequent packet is relayed to terminal 102 by VPN router 202. After this packet is received, interface program 116 installed in terminal 102 is configured to examine it and to obtain the port number and the IP address used to send the original packet to gatekeeper 108. Using this information, terminal 102 can then communicate with terminal 104 or any other terminal connected to computer network 106 to conduct IP-based telephony using the H.323 standard.

To more clearly illustrate this aspect of the present invention, assume again that terminal 102 has a virtual IP address of 10.10.10.20 and that VPN router 202 has a virtual address of 10.10.10.1 and a real IP address of 210.119.58.40. Now also assume that gatekeeper 108 has a real IP address of 211.104.18.60.

In the present embodiment, terminal 102 sends a packet to gatekeeper 108 through VPN router 202. More particularly, a port is created at the virtual IP address of terminal 102 (i.e., 10.10.10.20) to send the packet (assume that this port is port number 1720). A port is also created at the virtual IP address of VPN router 202 (i.e., 10.10.10.1) to receive the packet from terminal 102 (assume that this port is port number 2500). A port is also created at the real IP address of VPN router 202 (i.e., 210.119.58.40) to send this packet to gatekeeper 102 (assume that his port is port

number 3000). A port is also created at the real IP address of gatekeeper 108 (i.e., 211.104.18.60) to receive this packet (assume that this port is port number 1720).

After receiving the packet, gatekeeper 108 examines the packet and determines that it was received from port number 3000 at IP address 210.119.58.40 (i.e., VPN router 202). Gatekeeper 108 then places this information into another packet and sends this packet to port number 3000 at IP address 210.119.58.40. Thus, this subsequent packet is received by VPN router 202 and routed to terminal 102 via port number 2500 at IP address 10.10.10.1. This packet is then received at port number 1720 at IP address 10.10.10.20. Interface program 116 at terminal 102 then examines this packet to obtain the port number and the IP address used to send the original packet to gatekeeper 108. Once this information is obtained, terminal 102 can conduct IP-based telephony with terminal 104 using the H.323 standard. It should be recognized that using the procedures described above terminal 102 can also connect with gateway 110 to conduct IP-based telephony with telephone unit 112 connected to the PSTN.

With reference now to Fig. 3, in another application of the present invention, terminal 102 can be connected to computer network 106 through a firewall 302. Typically firewall 302 is a router configured to perform packet filtering. In this regard, firewall 302 presents similar problems as VPN router 202 (Fig. 2) describe above. More particularly, firewall 302 can function as a VPN router in that it has a virtual IP address and a real IP address. In that case, when terminal 102, which again is assigned a virtual IP address rather than a real IP address, sends out a packet to computer network 106, the packet includes the real IP address of firewall 302 rather than terminal 102. Consequently, IP-based telephony can be conducted through firewall 302 using the same process described above for VPN router 202 (Fig. 2).

But in some firewalls, one port is created to send packets and a different port is created to receive packets. If this is the case, then the process describe above for VPN router 202 cannot be used for firewall 302. But in accordance with another aspect of the present invention, interface program 116 can be configured to use SOCKS protocol to enable IP-based telephony through firewall 302 when firewall 302 supports SOCKS protocol.

As before, assume for example that terminal 102 wants to call terminal 104. Also assume that terminal 102 has a virtual IP address of 10.10.10.20 and that firewall 302 has a virtual IP address of 10.10.10.1 and a real IP address of 210.119.58.40. When terminal 102 sends a packet to firewall 302, a port (assume port number 1720) is created at virtual IP address of terminal 102 (i.e., 10.10.10.20) to send the packet. Also, a port (assume port number 2500) is opened at the virtual IP address of firewall 302 (i.e., 10.10.10.1) to receive the packet. A port (assume port number 3000) is also opened at the real IP address of firewall 302 (i.e., 210.119.58.40). In accordance with SOCKS protocol, this port and IP address is transmitted by firewall 302 to terminal 102. Thus, terminal 102 can register this information with gatekeeper 108 and conduct IP-based telephony with terminal 104 using the H.323 standard. Moreover, terminal 102 can also conduct IP-based telephony with telephone unit 112 connected to the PSTN through gateway 110.

In the description above, it was assumed that a call was made from terminal 102, which is behind firewall 302, to terminal 104, which is outside firewall 302. The following description, however, assumes that a call is made from terminal 104 to terminal 102.

In the present embodiment, terminal 102 forms a TCP/IP connection with gatekeeper 108 through firewall 302 using the SOCKS protocol process described above. Additionally, this TCP/IP connection between terminal 102 and gatekeeper 108 is constantly maintained. Terminal 104 also forms a TCP/IP connection with gatekeeper 108 and maintains this connection constantly.

When terminal 104 wants to call terminal 102, using the TCP/IP connection between terminal 104 and gatekeeper 108, interface program 116 installed on terminal 104 informs gatekeeper 108 that terminal 104 wants to connect with terminal 102. When this message is received, using the TCP/IP connection formed between gatekeeper 108 and terminal 102, gatekeeper 108 informs terminal 102 that terminal 104 wants to connect with terminal 102. Gatekeeper 108 also transmits the IP address of terminal 104 to terminal 102. Interface program 116 installed on terminal 102 then notifies firewall 302 to wait for the pending connection from terminal 104 using SOCKS bind function. In response, firewall 302 creates the port to connect with terminal 104 and sends that port number and IP address to terminal 102. Using the TCP/IP connection between terminal 102 and gatekeeper 108, interface program 116 installed on terminal 102 notifies gatekeeper 108 to connect to terminal 102 using the port and IP address received from gatekeeper 108. In response, gatekeeper 108 notifies terminal 104 to connect to firewall 302 using the port and IP address received from terminal 102. Terminal 104 then opens this connection to firewall 302. Firewall 302 verifies that the IP address of terminal 104 and other information before authorizing the connection to terminal 104. When a connection is opened between firewall 302 and terminal 104, firewall 302 sends a notification to terminal 102. After receiving this

notification, terminal 102 uses this connection between firewall 302 and terminal 104 to communicate terminal 104 to conduct IP-based telephony.

In another embodiment of the present invention, interface program 116 and gatekeeper 108 can be configured to receive calls from a telephone unit connected to the PSTN. For example, assume that telephone unit 112 connected to the PSTN wants to call unit 102. Telephone unit 112 is also connected to gateway 110, which is configured to translate between IP-based computer network 106 and the PSTN.

As such in the present embodiment, gateway 110 registers with gatekeeper 108. More particularly, gateway 110 transmits a RRQ (Register Request) message to gatekeeper 108. In response, gatekeeper 110 transmits a RCF (Request Confirm) message to gateway 110. In the RRQ message, gateway 110 transmits, in part, its IP address.

Additionally, as described above, terminal 102 registers with gatekeeper 108. More particularly, terminal 102 also transmits a RRQ (Register Request) message to gatekeeper 108. In response, gatekeeper 110 transmits a RCF (Request Confirm) message to terminal 102. It should be noted that terminal 102 can transmit its IP address and port number to gatekeeper 108 through firewall 303 using any of the procedures described above.

When telephone unit 112 initiates a call, gateway 110 transmits an ARQ (Admission Request) to gatekeeper 108. In response, gatekeeper 108 transmits the ARQ message to terminal 102 using the port number and IP address that terminal 102 registered earlier. When the ARQ message is received, interface program 116 installed at terminal 102 binds a port to firewall 302 and sends the bound port information to gatekeeper 108. In response, gatekeeper 108 sends back a RCF (Registration Confirm)

message to terminal 102 and a ACF (Admission Confirm) message to gateway 110. Gatekeeper 108 also sends gateway 110 the port number and IP address that terminal 102 registered with gatekeeper 108. Consequently, terminal 10 and gateway 110 have the IP addresses needed to conduct IP-based telephony using the H.323 standard.

In one exemplary embodiment of the present invention, computer network 106 is the Internet. But it should be recognized that computer network 106 can include any network, either public, private, or any combination of public and private computer networks, that operate using an IP-based protocol. Additionally, the IP protocol alluded to above can include IPv4, IPv6, and the like.

Thus far the present invention has been described with regard to conducting IP-based telephony through a computer network. It should be recognized, however, that the present invention can be utilized in various applications in addition to IP-based telephony.

More particularly, with reference to Fig. 2, in conjunction with an exemplary embodiment of the present invention, a method and system was described above to facilitate IP-based telephony with terminal 102 that is connected to VPN router 202. In that exemplary embodiment, terminal 102 is assigned a virtual IP address. Thus, when terminal 102 transmits a packet, VPN router 202 (Fig. 2) replaces the virtual IP address of terminal 102 with VPN router 202's (Fig. 2) real IP address. To facilitate IP-based telephony with terminal 102, interface program 116 installed on terminal 102 can be configured to transmit a packet to gatekeeper 108 through router 202. When gatekeeper 108 receives this packet, gatekeeper 108 then determines the port number and the IP address utilized by router 202 to send the packet from terminal 102.

As stated above, although this method and system summarized above was earlier described in conjunction with IP-based telephony, it should be recognized that this method and system can be utilized in any number of applications. As such, in the following description, this scheme will be described in conjunction with a more general application of facilitating communication between two terminals in two different network environments that utilize two different IP-addressing schemes.

With reference now to Fig. 4, it should be recognized that gatekeeper 108 can be configured to facilitate communication between terminals 102 and 104 without necessarily performing the functions of a gatekeeper in accordance with the H.323 standard. Thus, in the following description, gatekeeper 108 will be referred to as server 108. It should be recognized that gatekeeper (server) 108 can be configured as any number of terminals, computers, processors, and the like.

In accordance with one exemplary embodiment of the present invention, terminal 102 can be connected to server 108 through a router 402. In the present example, router 402 can be configured to translate an IP address utilized within a first-network environment 406 to a different IP address utilized within a second-network environment 408. Accordingly, router 402 can be configured as a Virtual Private Network (VPN) router, a Network Address Translation (NAT) router, and the like. Additionally, router 402 can be configured to be a part of a firewall.

As depicted in Fig. 4, terminal 102 and router 402 lie within network environment 406, while server 108 lies outside of network environment 406. More particularly, in the present embodiment, server 108 and terminal 104 lie within network environment 408. It should be recognized, however, that network environment 406 and network environment 408 can include a VPN environment, a NAT environment, a

network behind a firewall, and the like. It should be further recognized, that server 108 can lie within a third network environment separate from network environments 406 and 408.

As described earlier, network environment 406 can utilize a different IP-addressing scheme than network environment 408. As also described earlier, router 402 can be configured to translate between the different IP addressing schemes utilized in network environments 406 and 408. As such, when terminal 102 wants to communicate with terminal 104, router 402 translates the IP-addressing scheme utilized in network environment 406 to the IP-addressing scheme utilized in network environment 408. However, terminal 104 cannot initiate communication with terminal 102 without having the IP address of terminal 102 within network environment 406.

Thus, the method and system described earlier in conjunction with facilitating IP-based telephony between terminals 102 and 104 can be utilized to permit terminal 104 to initiate communication with terminal 102. For the sake of clarity and convenience, only terminals 102 and 104 are described below and depicted in Fig. 4. It should be recognized, however, that the present invention can be utilized to facilitate communication between any number of terminals 102 and 104.

With reference to Fig. 4, in the present embodiment, terminal 102 can be configured to establish an initial connection with server 108 (block 502 in Fig. 5). As described earlier, terminal 102 can include interface program 116 configured to establish a connection with server 108. This initial connection can be established when interface program 116 is initially launched or activated on terminal 102. In one embodiment, this initial connection can be established using a TCP/IP protocol. One advantage of utilizing a TCP/IP protocol is that the connection between terminal 102

and server 108 is maintained. More particularly, in the present embodiment, router 402 opens a port to connect terminal 102 with server 108. When a TCP/IP protocol is utilized, router 402 keeps this port open. However, when a UDP protocol is utilized, router 402 closes this port within a short period of time, such as within a few minutes. As such, in another embodiment, when a UDP protocol is utilized to establish the initial connection between terminal 102 and server 108, interface program 116 can be configured to repeatedly send packets to server 108 to maintain this connection. More particularly, interface program 116 can be configured to repeatedly send packets to server 108 before router 402 closes the port opened to establish the initial connection between terminal 102 and server 108. For example, interface program 116 can be configured to send a packet to server 108 every minute. It should be recognized, that interface program 116 can be configured to send a packet within any convenient period of time, such as every few seconds, minutes, and the like. It should also be recognized that server 108 can also send packets to terminal 102 to maintain the connection between terminal 102 and server 108.

Having established a connection between terminal 102 and server 108, interface program 116 in terminal 102 can be configured to send a packet to server 108 through router 402 (block 504 in Fig. 5). More particularly, terminal 102 sends a packet to server 108 through router 402. When router 402 transmits the packet from terminal 102 to server 108, it translates from the IP-addressing scheme utilized in network environment 406 to the IP-addressing scheme utilized in network environment 408. Additionally, router 402 assigns a port to transmit the packet from terminal 102 to server 108.

Thus, when this packet is received, server 108 can be configured to examine it to determine the IP address and port number utilized by router 402 to transmit this packet sent from terminal 102 (block 506 in Fig. 5). It should be recognized that server 108 can include any convenient software and/or hardware to determine the IP address and port number utilized by router 402.

After determining this IP address and port number, server 108 can then transmit this information to terminal 104 (block 508 in Fig. 5). Utilizing this IP address and port number transmitted by server 108, terminal 104 can then establish a connection with terminal 102 behind router 402 (block 510 in Fig. 5). In this manner, terminal 104 within network environment 408 having one IP-addressing scheme can establish a connection and communicate with terminal 102 within network environment 406 having a different IP-addressing scheme.

Server 108 can also be configured to store the IP address and port number utilized by router 402 to transmit the packet from terminal 102. As such, when terminal 104 wants to communicate with terminal 102, it can send a request to server 108, which can then transmit the IP address and port number associated with terminal 102.

More particularly, in one embodiment of the present invention, users of terminals 102 and 104 can be assigned unique identification codes. When interface program 116 connects to server 108, it can transmit the unique identification code associated with the user of terminal 102 to server 108. Server 108 can then store this identification code with the IP address and port number associated with terminal 102. Thus, when the user of terminal 104 wants to communicate with the user of terminal 102, the identification code associated with the user of terminal 102 can be included in the request transmitted to server 108 from terminal 104. It should be recognized that

aliases can be associated with the identification codes assigned to users of terminals 102 and 104. Additionally, terminals 102 and 104 can be assigned the identification codes rather than the users. For a more thorough description of such an identification code system, see U.S. Patent Application Serial No. 09/557,746, filed on April 24, 2000, entitled METHOD AND APPARATUS FOR CONDUCTING COMPUTER TELEPHONY, the entire content of which is incorporated herein by reference.

As described above, in one embodiment of the present invention, server 108 can be configured to transmit the IP address and port number associated with terminal 102 to terminal 104 upon receipt of a request from terminal 104. In this embodiment, router 402 is configured to keep open the port utilized to send the packet from terminal 102 to server 108, such as when using a TCP/IP protocol. However, in some applications, router 402 can be configured to close this port shortly after sending the packet from terminal 102 to server 108, such as when using a UDP protocol. For example, when router 402 is a part of a firewall, the port utilized to send out the packet from terminal 102 to server 108 can be closed within a few minutes. In these applications, terminal 104 preferably establishes a connection with terminal 102 using the address and port number received from server 108 before the port closes.

More particularly, in one embodiment of the present invention, terminals 102 and 104 can be configured to establish initial connections with server 108. More particularly, as described earlier, terminals 102 and 104 can include interface programs 116 configured to connect terminals 102 and 104 with server 108. This initial connection can be established when interface programs 116 are initially launched or activated on terminals 102 and 104. In the present embodiment, this initial connection

is established using a TCP/IP protocol. As described above, in another embodiment, this initial connection can be established using a UDP protocol.

In the present embodiment, when terminal 104 wants to initiate communication with terminal 102, interface program 116 on terminal 104 can be configured to send a request to server 108. When terminal 104 sends this request to server 108, a port is opened on terminal 104 and server 108. When server 108 receives this request, it can be configured to determine the address and port number that terminal 104 utilized to send this request. Server 108 can be configured to store this address and port number.

After receiving the request from terminal 104, server 108 can be configured to transmit a request to interface program 116 on terminal 102. In the present embodiment, server 108 can transmit this request to terminal 102 through the initial connection established with terminal 102.

In response to this request from server 108, interface program 116 on terminal 102 can be configured to send a packet to server 108 through router 402. When terminal 102 sends this packet, router 402 opens a port to send the packet to server 108.

When server 108 receives this packet, it can be configured to determine the address and port number that router 402 utilized to send the packet. Server 108 then transmits this address and port number to terminal 104, and more particularly to interface program 116 in terminal 104. Server 108 can transmit this information to terminal 104 through the initial connection established with terminal 104.

Utilizing the IP address and port number received from server 108, terminal 104 can then establish a connects with terminal 102 behind router 402. In this manner, terminal 104 within network environment 408 having one IP-addressing scheme can

establish a connection with terminal 102 within network environment 406 having a different IP-addressing scheme.

It should be recognized that in the present embodiment, server 108 can be configured to store the IP address and port number associated with terminal 102. Additionally, the identification code scheme described earlier can also be utilized in the present embodiment.

Although the present invention has been described in conjunction with particular embodiments illustrated in the appended drawing figures, various modifications can be made without departing from the spirit and scope of the invention. Therefore, the present invention should not be construed as limited to the specific form shown in the drawings and described above.

We claim:

1. A method of establishing a connection between a first terminal in a first-network environment and a second terminal in a second-network environment, wherein the first-network environment and the second-network environment utilize different Internet Protocol (IP) addressing schemes, and wherein the first terminal is connected to a router, said method comprising:

establishing a connection from the first terminal to a server, wherein said server lies outside of the first-network environment;

transmitting a packet from the first terminal to said server through the router;

determining the IP address and port number utilized by the router to transmit the packet to said server;

transmitting the IP address and port number to the second terminal; and

establishing a connection from the second terminal to the first terminal utilizing the IP address and port number received from the server.

2. The method of claim 1 further comprising the steps of:

storing the IP address and port number on said server;

receiving a request from the second terminal to connect to the first terminal; and

transmitting the stored IP address and port number to the second terminal.

3. The method of claim 2, wherein the first terminal, the second terminal, and said server communicate utilizing a Transmission Control Protocol/Internet Protocol (TCP/IP) protocol.

4. The method of claim 1 further comprising the steps of:

establishing a connection from the second terminal to said server;

transmitting a request from the second terminal to said server utilizing said connection established between the second terminal and said server; and

transmitting a request from said server to the first terminal, wherein said request is transmitted utilizing the connection from the first terminal to said server, and wherein the packet transmitted from the first terminal to said server is transmitted in response to said request transmitted from said server to the first terminal.

5. The method of claim 4 further comprising the step of storing the IP address and port number on said server.

6. The method of claim 4, wherein the first terminal, the second terminal, and said server communicate utilizing a User Datagram Protocol (UDP) protocol.

7. The method of claim 1, wherein said connection established from the first terminal to said server is established utilizing a TCP/IP protocol.

8. The method of claim 1, wherein said connection established from the first terminal to said server is established utilizing a User Datagram Protocol (UDP).

9. The method of claim 8 further comprising the step of repeatedly transmitting a packet from the first terminal to said server.

10. The method of claim 1, wherein the first-network environment is a Virtual Private Network (VPN) environment.

11. The method of claim 1, wherein the first-network environment is a Network Address Translation (NAT) environment.

12. The method of claim 1, wherein the first-network environment is a firewall environment.

13. A method of establishing a connection between a first terminal in a first network environment having a first Internet Protocol (IP) addressing scheme and a second terminal in a second-network environment having a second IP-addressing scheme, wherein the first terminal is connected to a router configured to translate between the first and second IP addressing schemes, said method comprising:

establishing an initial connection between the first terminal and a server, wherein said server lies outside of said first network environment;

transmitting a request from the second terminal to said server;

transmitting a request from said server to the first terminal in response to said request transmitted from the second terminal, wherein said request is transmitted utilizing said initial connection established between the first terminal and said server;

transmitting a packet from the first terminal through the router to said server in response to said request transmitted from said server;

determining the IP address and port number utilized by the router to transmit said packet to said server;

transmitting the IP address and port number utilized by the router from the server to the second terminal; and

establishing a connection from the second terminal to the first terminal utilizing the IP address and port number transmitted from the server.

14. The method of claim 13 further comprising the step of storing the IP address and port number on said server.

15. The method of claim 13, wherein said request from the second terminal to said server is transmitted from an interface program installed on the second terminal, and wherein said request from said server to the first terminal is transmitted to an interface program installed on the first terminal.

16. The method of claim 13 further comprising the step of establishing an initial connection between the second terminal and said server, and wherein the IP address and port number transmitted from the server to the second terminal is transmitted utilizing said initial connection between the second terminal and said server.

17. The method of claim 16, where said initial connections established between the first terminal, the second terminal, and said server are established using a Transmission Control Protocol/Internet Protocol (TCP/IP) protocol.

18. The method of claim 17, wherein said request transmitted from the second terminal to said server, said request transmitted from said server to the first terminal,

and said packet transmitted from the first terminal to said server are transmitted using a User Datagram Protocol (UDP) protocol.

19. The method of claim 13, wherein said initial connection established between the first terminal and said server is established utilizing a TCP/IP protocol.

20. The method of claim 13, wherein said initial connection established between the first terminal and said server is established utilizing a UDP protocol.

21. The method of claim 20 further comprising the step of repeatedly transmitting a packet from said first terminal to said server.

22. The method of claim 13, wherein the first-network environment is a Virtual Private Network (VPN) environment.

23. The method of claim 13, wherein the first-network environment is a Network Address Translation (NAT) environment.

24. The method of claim 13, wherein the first-network environment is a firewall environment.

25. A system configured to establish a connected between a first terminal in a first-network environment and a second terminal in a second-network environment, wherein the first-network environment and the second-network environment utilize different

Internet Protocol (IP) addressing schemes, and wherein the first terminal is connected to a router; said system comprising:

a server located outside of the first-network environment;

a first-interface program installed on the first terminal, wherein said first-interface program is configured to establish a connection with said server and to transmit a packet to said server through the router, and wherein said server is configured to determine the IP address and port number utilized by the router to send the packet to said server; and

a second-interface program installed on the second terminal, wherein said server is configured to transmit the IP address and the port number to said second-interface program, and wherein said second-interface program is configured to establish a connection with said first-interface program utilizing the IP address and port number received from said server.

26. The system of claim 25, wherein said server is configured to store the IP address and port number.

27. The system of claim 26, wherein said second-interface program is configured to transmit a request to said server to connect to said first-interface program, and wherein said server is configured to transmit the stored IP address and port number to said second-interface program in response to said request.

28. The system of claim 25, wherein said second-interface program is configured to establish a connection with said server and to transmit a request to said server utilizing

said connection established with said server, wherein said server is configured to transmit a request to said first-interface program in response to said request from said first-interface program, and wherein said second-interface program is configured to transmit said packet to said server in response to said request from said server.

29. The system of claim 28, wherein said server is configured to store the IP address and port number.

30. The system of claim 25, wherein said first-interface program is configured to establish the connection with said server utilizing a Transmission Control Protocol/Internet Protocol (TCP/IP) protocol.

31. The system of claim 25, wherein said first-interface program is configured to establish the connection with said server utilizing a User Datagram Protocol (UDP) protocol.

32. The system of claim 31, wherein said first-interface program is configured to repeatedly transmit a packet to said server to maintain the connection with said server.

33. The method of claim 25, wherein the router is configured as a Virtual Private Network (VPN) router.

34. The method of claim 25, wherein the router is configured as a Network Address Translation (NAT) router.

35. The method of claim 25, wherein the router is configured to be a part of a firewall.

Fig.1

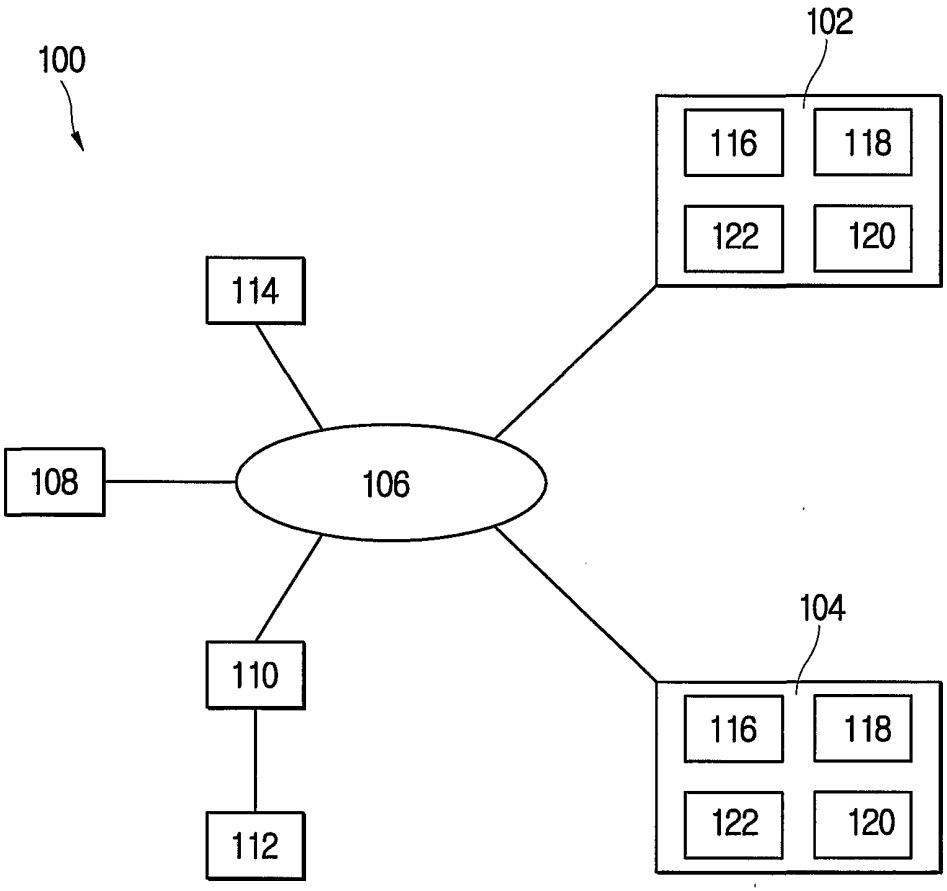


Fig.2

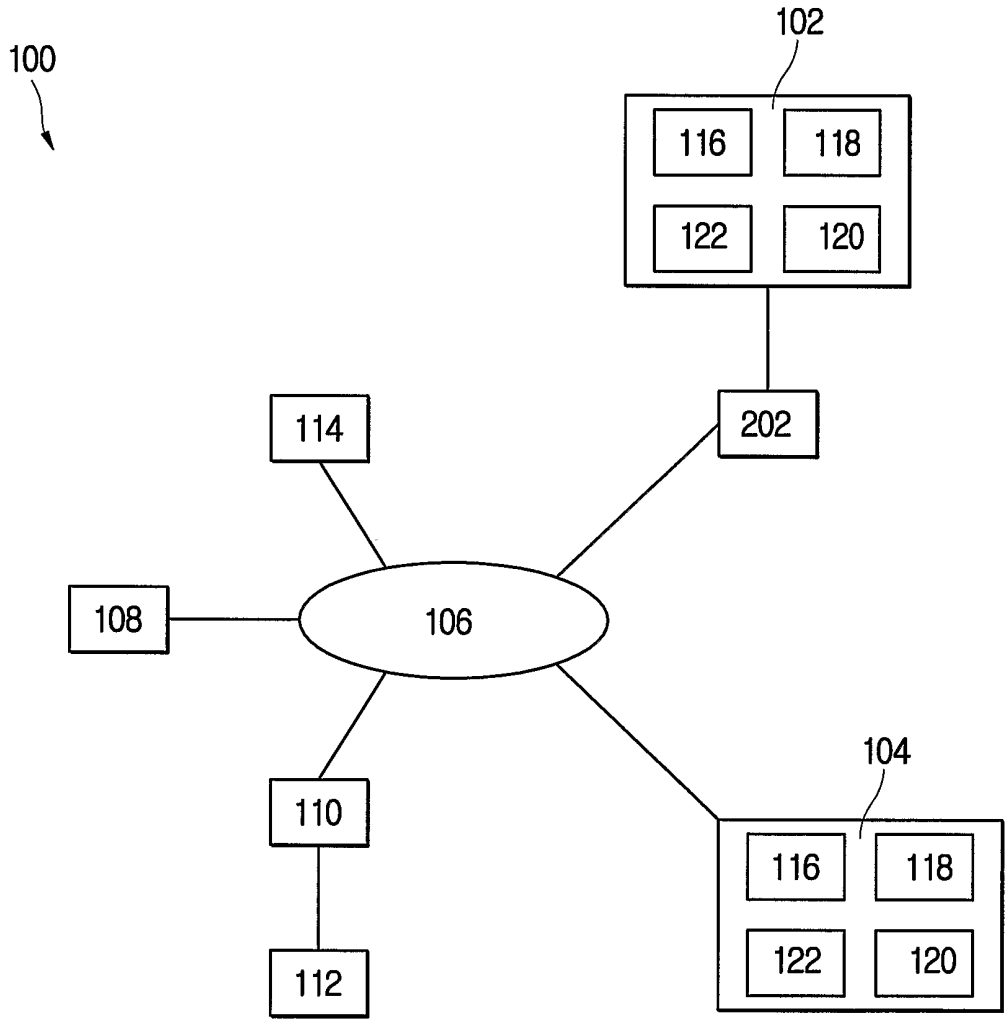

100
102
116
118
122
120
202
114
108
106
110
112
104
116
118
122
120

Fig.3

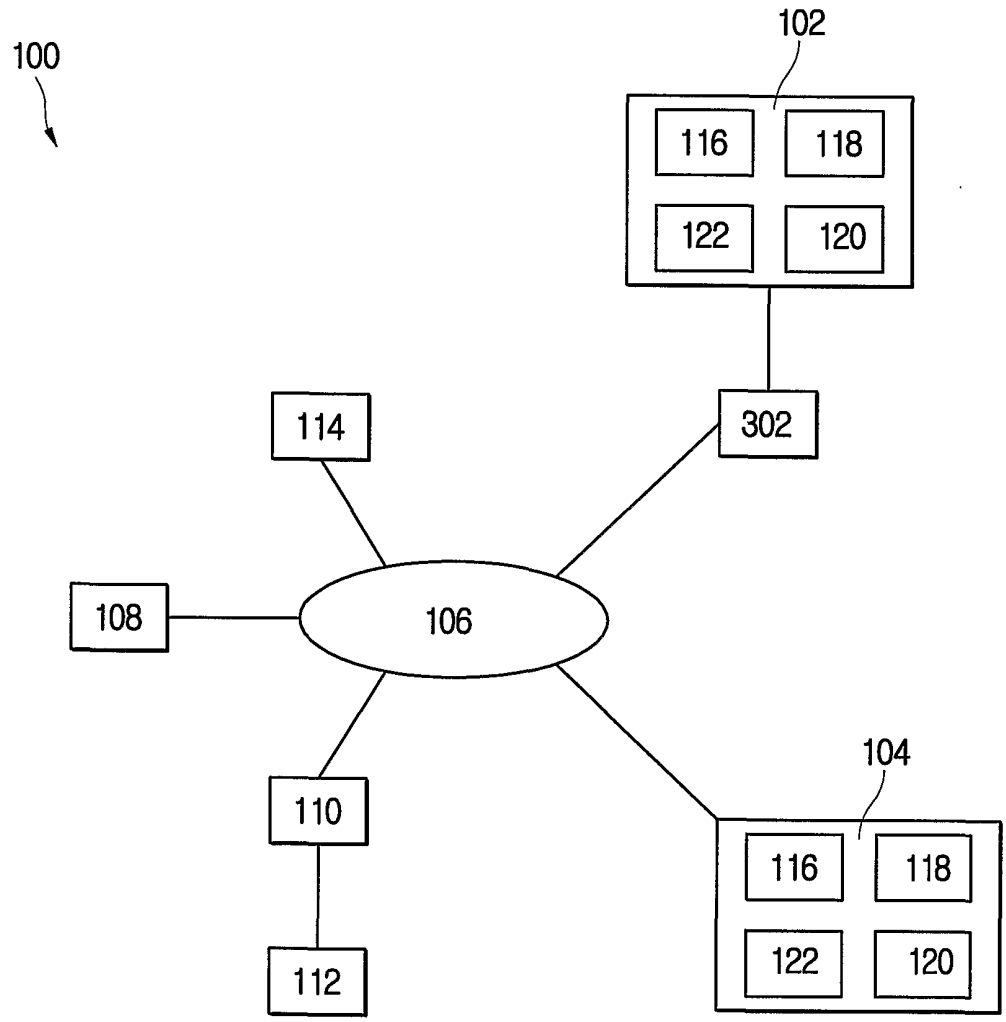

100
102
116
118
122
120
302
114
108
106
110
112
104
116
118
122
120

Fig.4

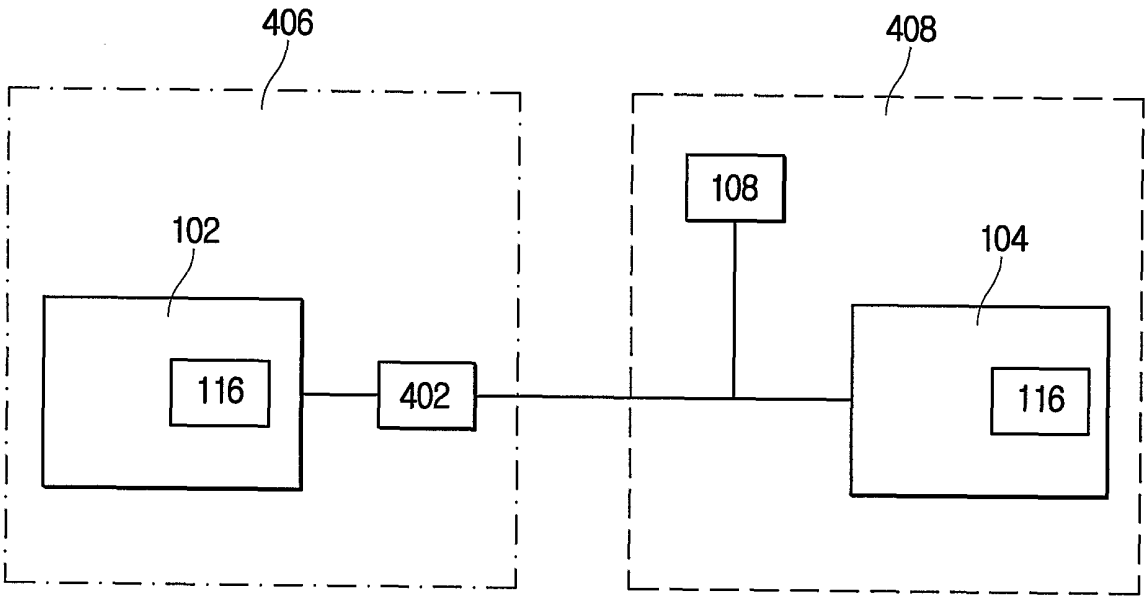
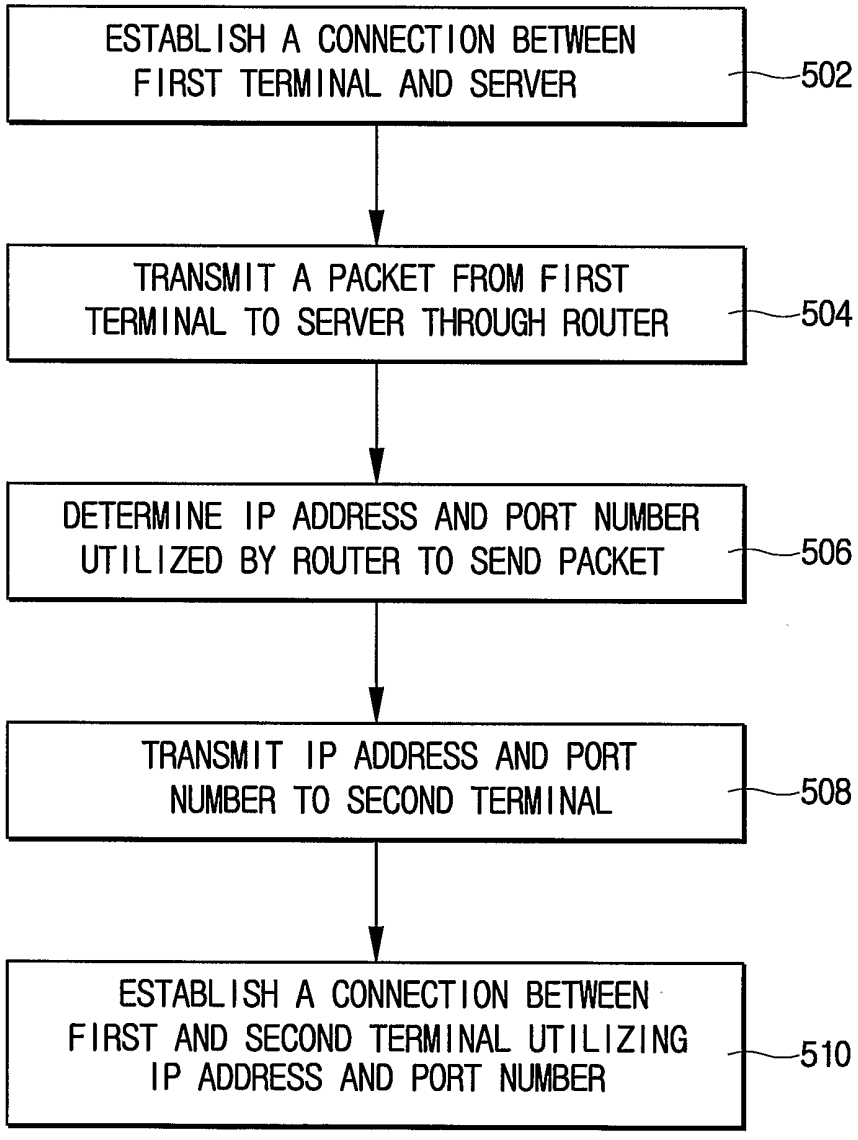


Fig.5


ESTABLISH A CONNECTION BETWEEN FIRST TERMINAL AND SERVER
502
TRANSMIT A PACKET FROM FIRST TERMINAL TO SERVER THROUGH ROUTER
504
DETERMINE IP ADDRESS AND PORT NUMBER UTILIZED BY ROUTER TO SEND PACKET
506
TRANSMIT IP ADDRESS AND PORT NUMBER TO SECOND TERMINAL
508
ESTABLISH A CONNECTION BETWEEN FIRST AND SECOND TERMINAL UTILIZING IP ADDRESS AND PORT NUMBER
510