08/721316

PATENT
September 25, 1996
N0003/7002

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

NEW APPLICATION TRANSMITTAL LETTER

Sir:

Transmitted herewith for filing is the Patent Application of

1 - 00 Inventor(s): Shane D. Mattaway, Glenn W. Hutton, and Craig B. Strickland et. al.

For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

This application is a continuation-in-part of U.S. Patent Application Serial No. 08/533,115, entitled, Point-to-Point Internet Protocol, by Glenn W. Hutton, filed September 25, 1995.

Enclosed are the following papers required to obtain a filing date under 37 C.F.R. §1.53(b):

27 Sheets of Informal Drawings
80 Pages of Specification, Including Claims and Abstract
6 Claims

The following papers, if indicated by an X, are also enclosed:

____ A Declaration and Power of Attorney
____ An Assignment of the invention
____ An Information-Disclosure Statement, Form PTO-1449 and a copy of each cited reference
____ A Small-Entity Declaration
X A Certificate of Express Mailing, Express Mail Label No. EM316008331US

FEE CALCULATION:

Total Claims:	6 - 20 = 0 X $22.00 =	$00.00
Independent Claims:	1 - 3 = 0 X $78.00 =	$00.00
Basic Fee:		$750.00

Total of Above Calculations: $750.00

__X__ A check in the amount of $750.00 is enclosed to cover the Filing Fee.

_____ A check in the amount of $40.00 is enclosed to cover the Recording Fee for the Assignment. A duplicate copy of this transmittal letter is enclosed.

The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §1.16 and 1.17 that may be required by this paper or any paper filed in connection with this Patent Application, or credit any overpayment, to our Deposit Account No. 02-3038.

Please address all communications and telephone calls to the undersigned.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse
Reg. No. 33,518
BOOKSTEIN & KUDIRKA, P.C.
One Beacon Street
Boston, MA 02108
(617) 367-4600

Express Mail mailing label number EM316008331US

Date of Deposit 9/25/96

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: The Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Bruce D. Jobse
(Typed or printed name of person mailing paper or fee)

Bruce D. Jobse
(Signature of person mailing paper or fee)

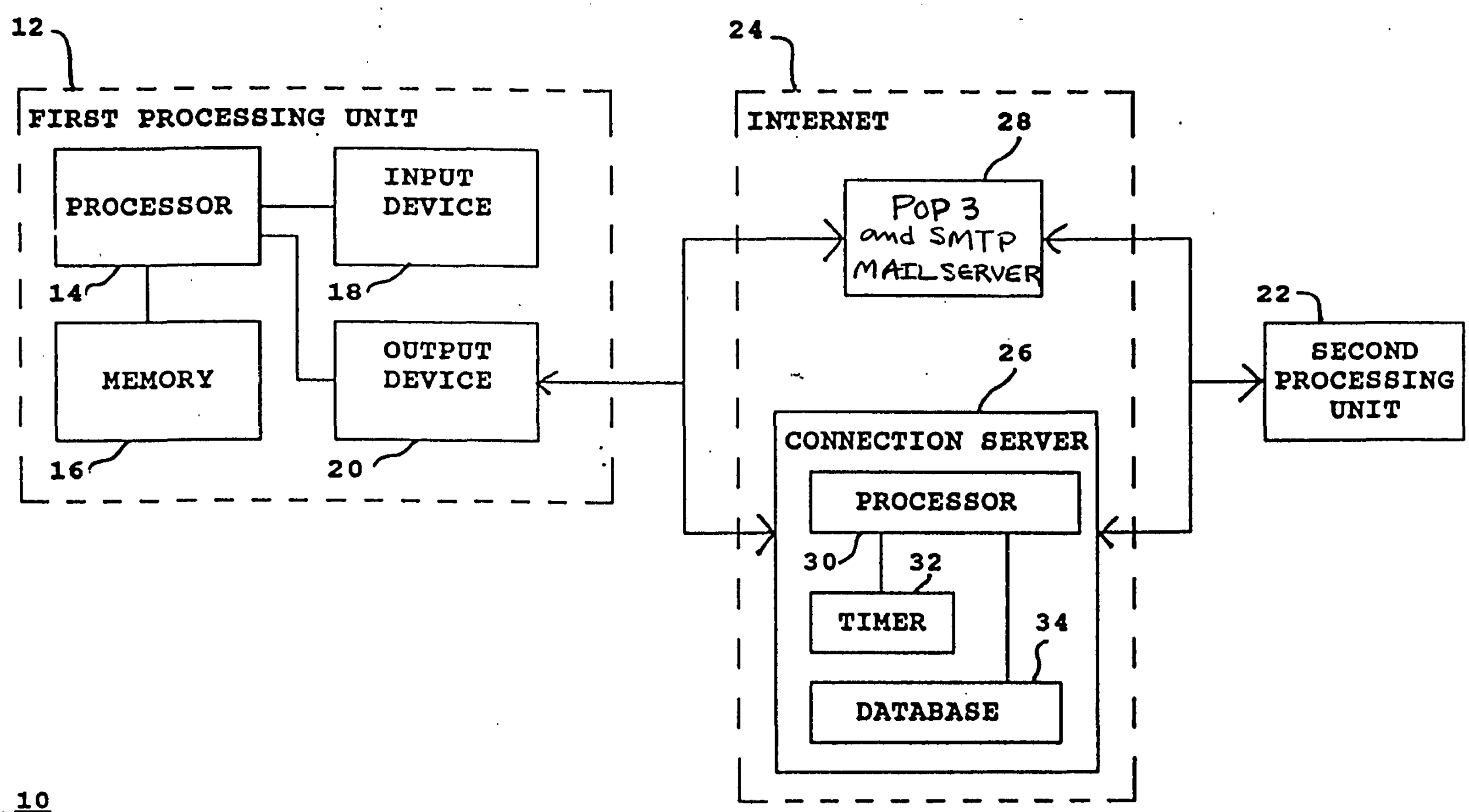


FIG. 1

08/721316

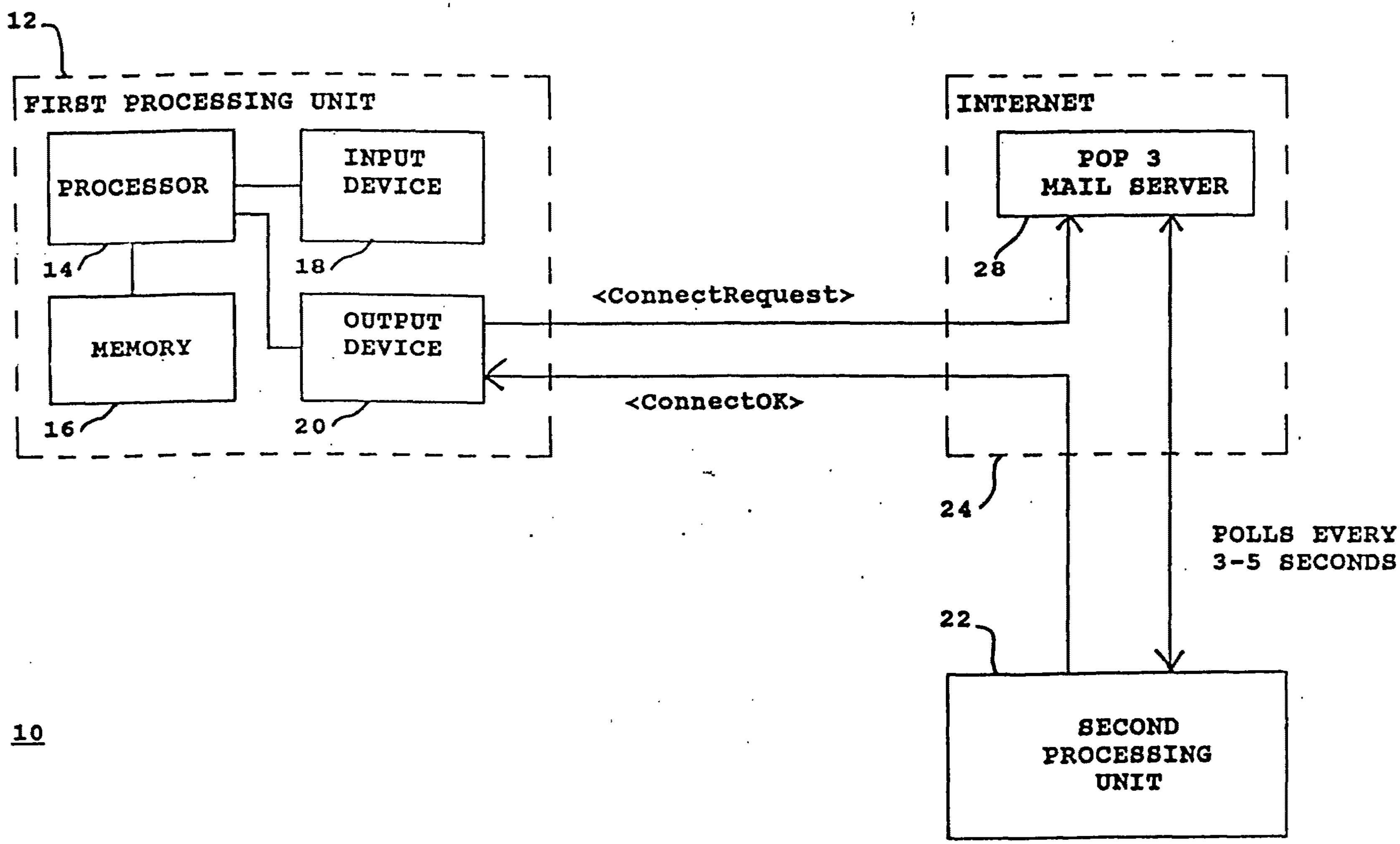


FIG. 2

08/721316

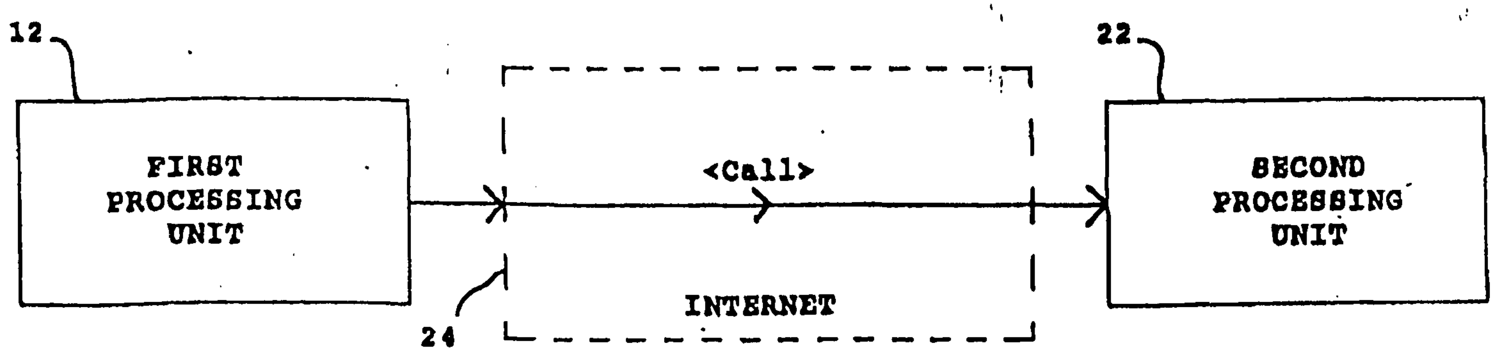


FIG. 3

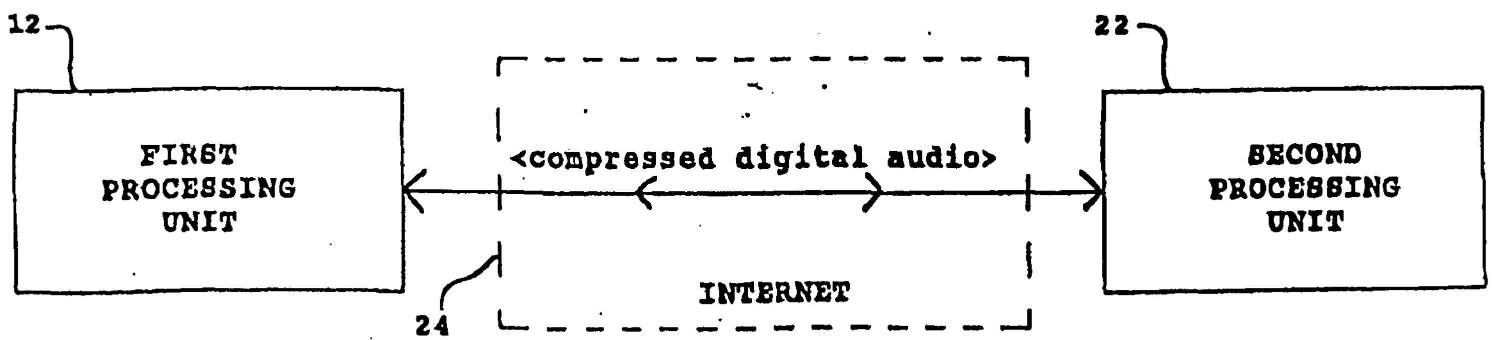


FIG. 4

08/721316

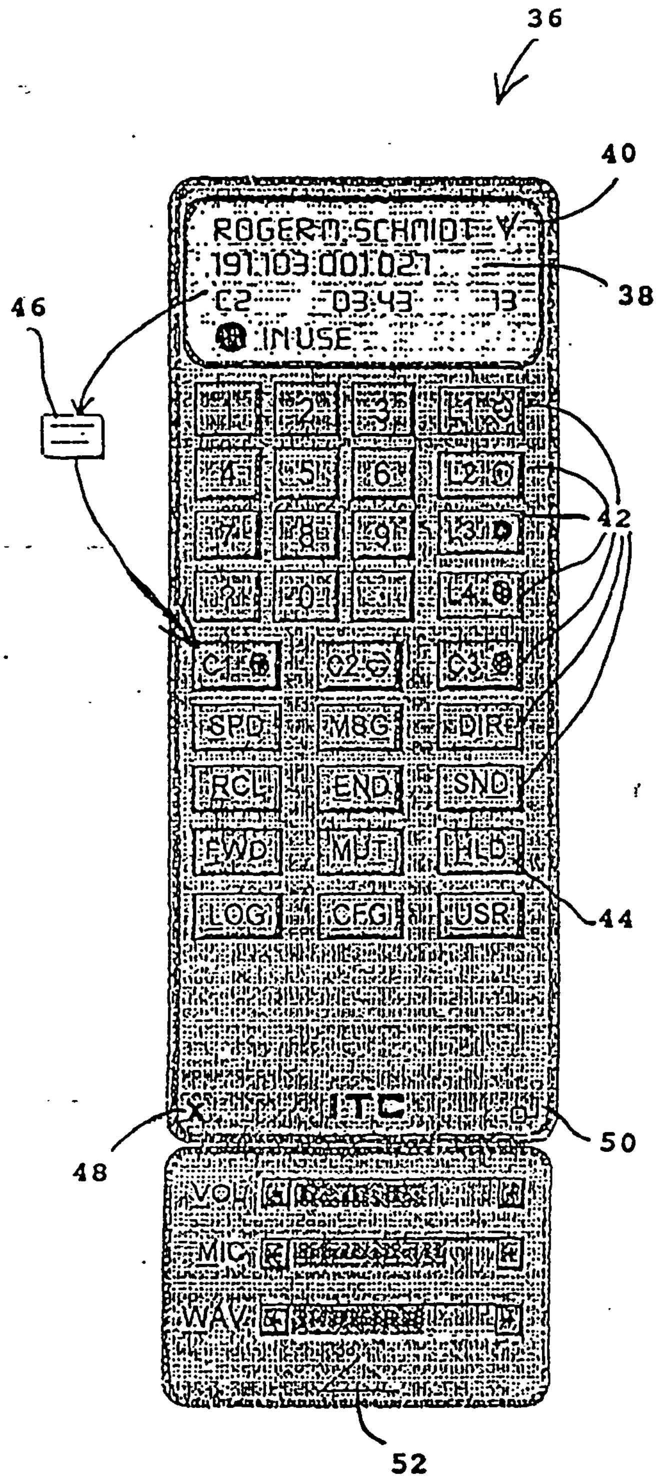


FIG. 5

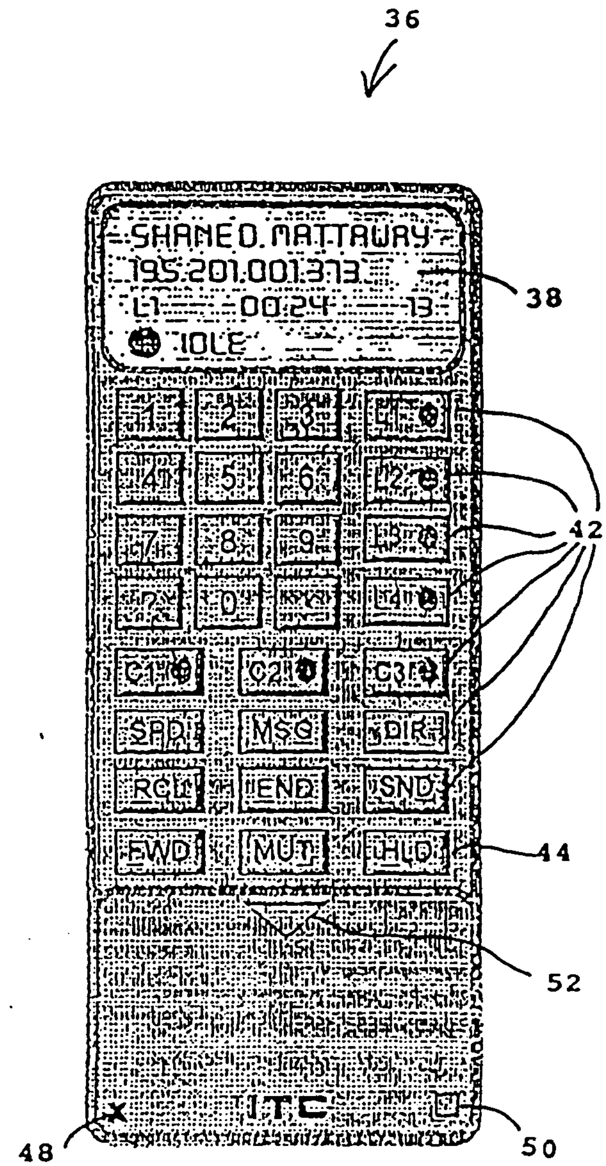


FIG. 6

08/721316

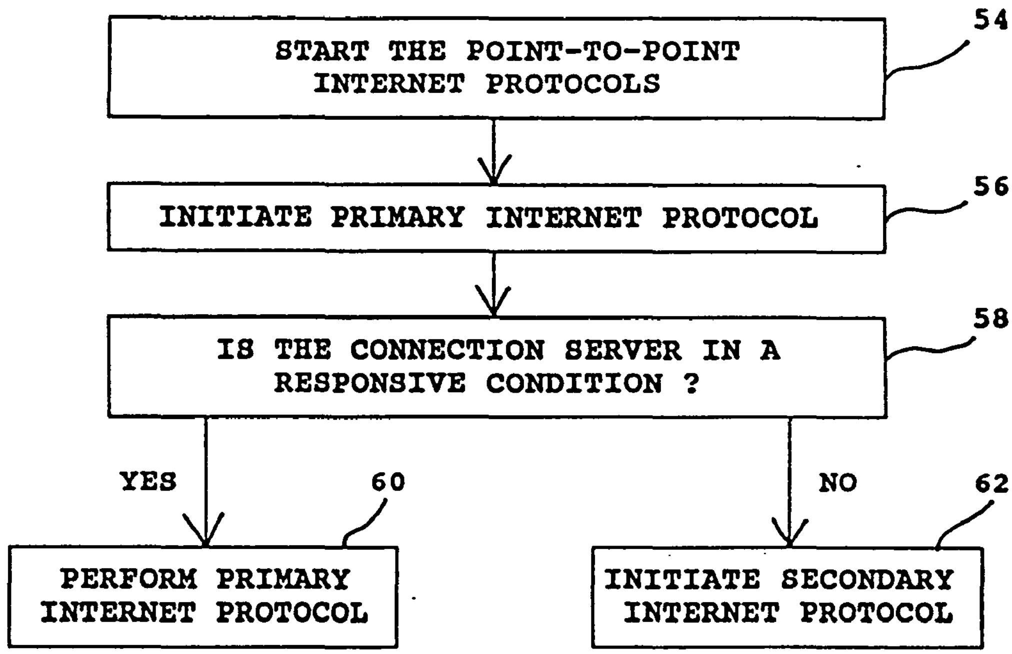

54
START THE POINT-TO-POINT INTERNET PROTOCOLS
56
INITIATE PRIMARY INTERNET PROTOCOL
58
IS THE CONNECTION SERVER IN A RESPONSIVE CONDITION ?
YES
60
NO
62
PERFORM PRIMARY INTERNET PROTOCOL
INITIATE SECONDARY INTERNET PROTOCOL

FIG. 7

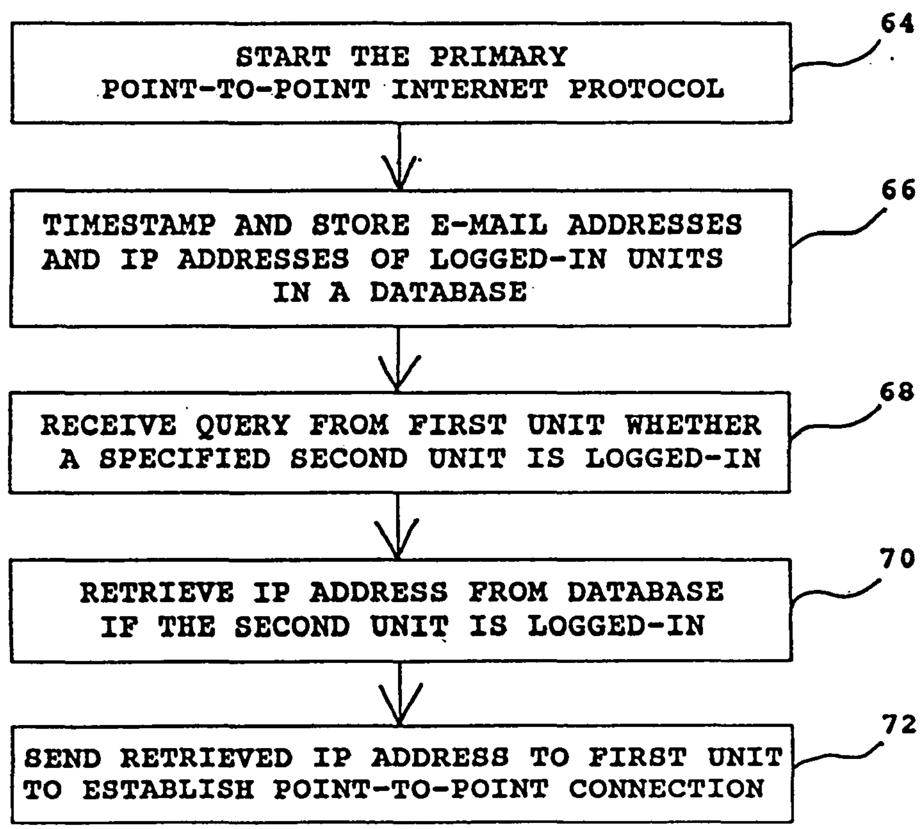

64
START THE PRIMARY POINT-TO-POINT INTERNET PROTOCOL
66
TIMESTAMP AND STORE E-MAIL ADDRESSES AND IP ADDRESSES OF LOGGED-IN UNITS IN A DATABASE
68
RECEIVE QUERY FROM FIRST UNIT WHETHER A SPECIFIED SECOND UNIT IS LOGGED-IN
70
RETRIEVE IP ADDRESS FROM DATABASE IF THE SECOND UNIT IS LOGGED-IN
72
SEND RETRIEVED IP ADDRESS TO FIRST UNIT TO ESTABLISH POINT-TO-POINT CONNECTION

FIG. 8

08/721316

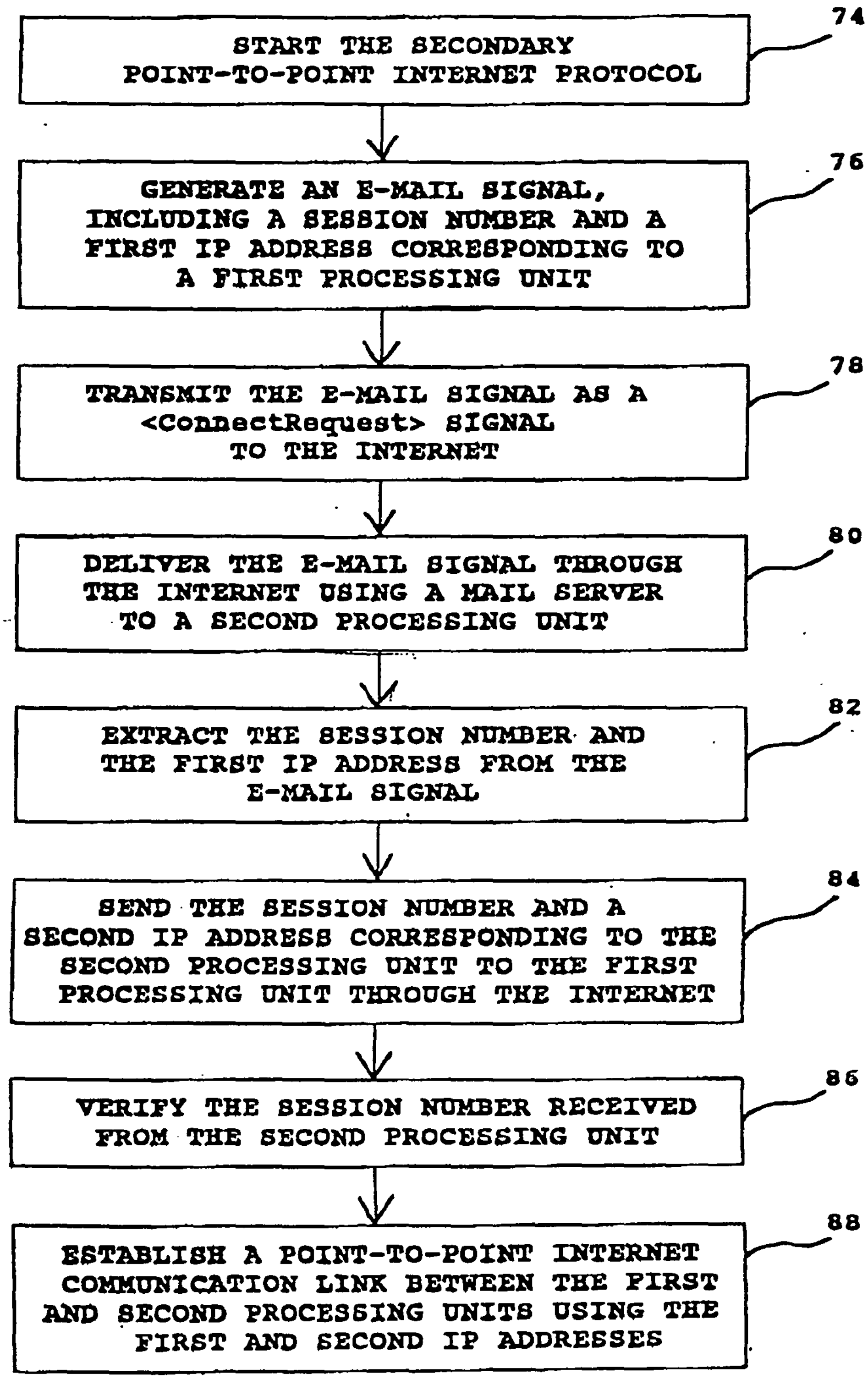


FIG. 9

08/721316

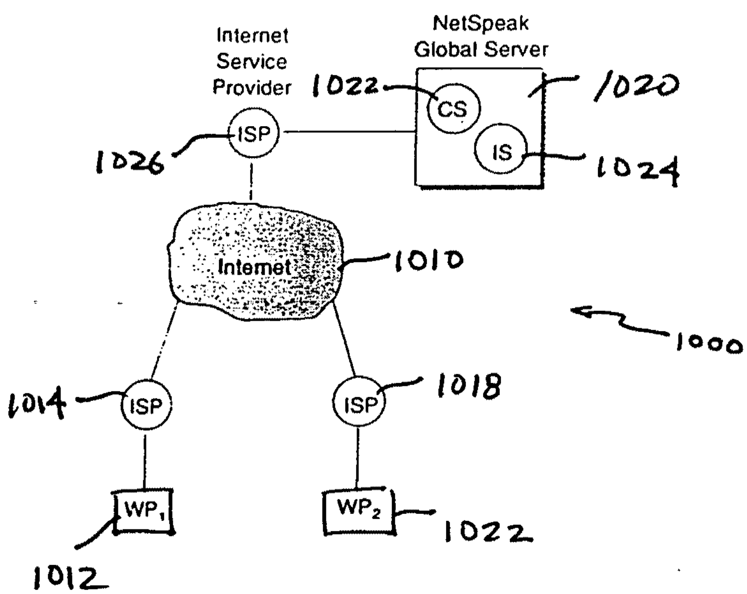

Internet
Service
Provider
NetSpeak
Global Server
1022
CS
1020
ISP
1026
IS
1024
Internet
1010
1000
1014
ISP
ISP
1018
WP1
WP2
1022
1012

Fig. 10

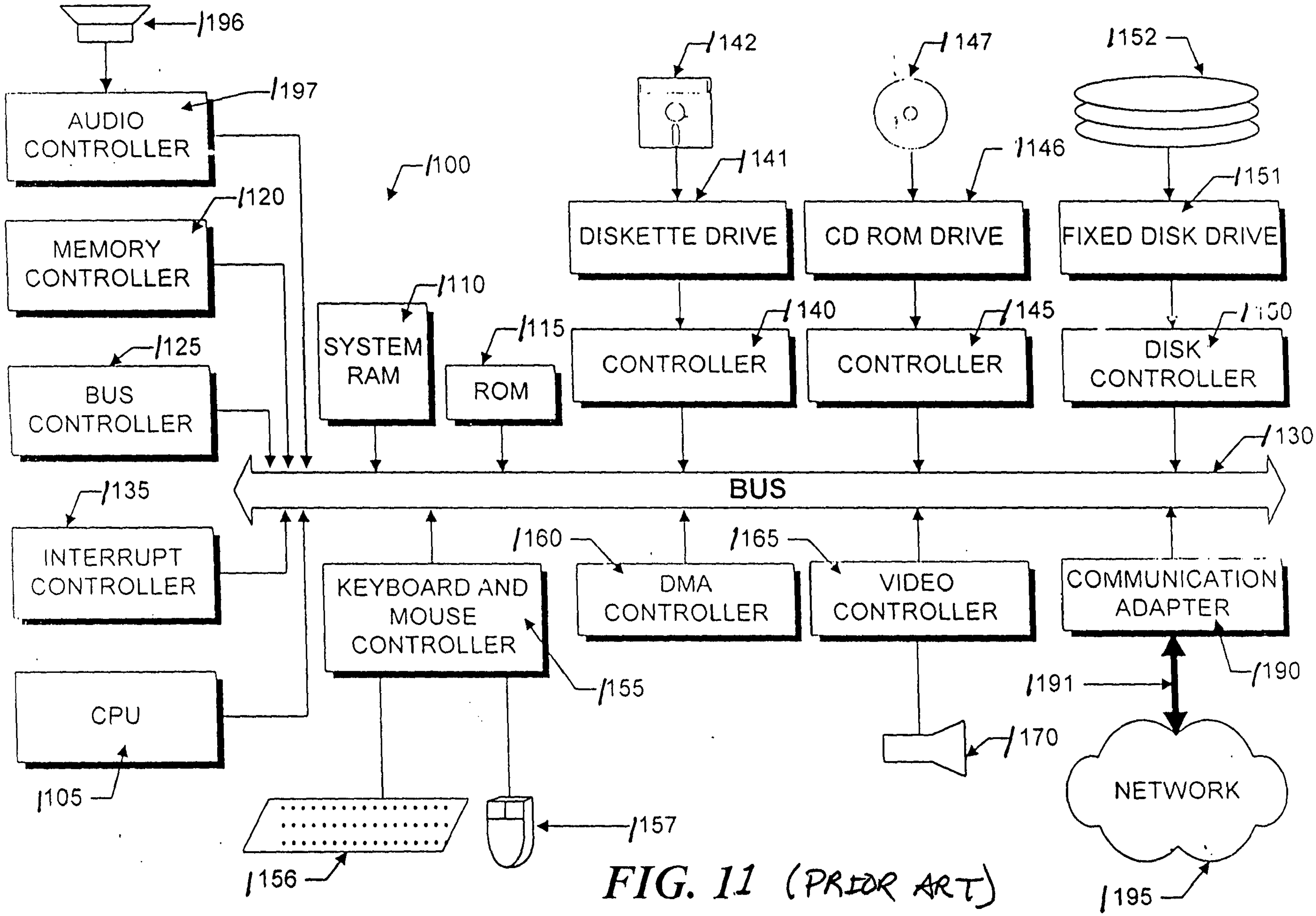


FIG. 11 (PRIOR ART)

08/721316

08/721316

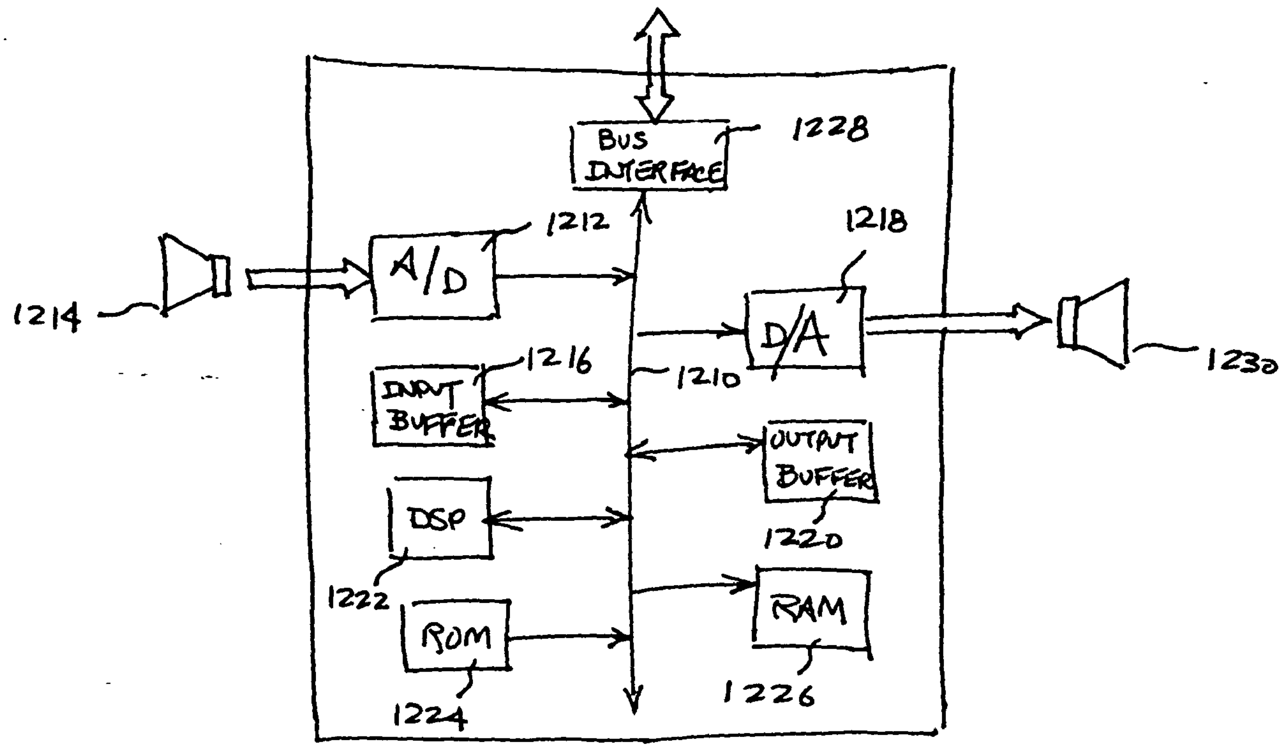


Fig. 12
(PRIOR ART)

08/721316

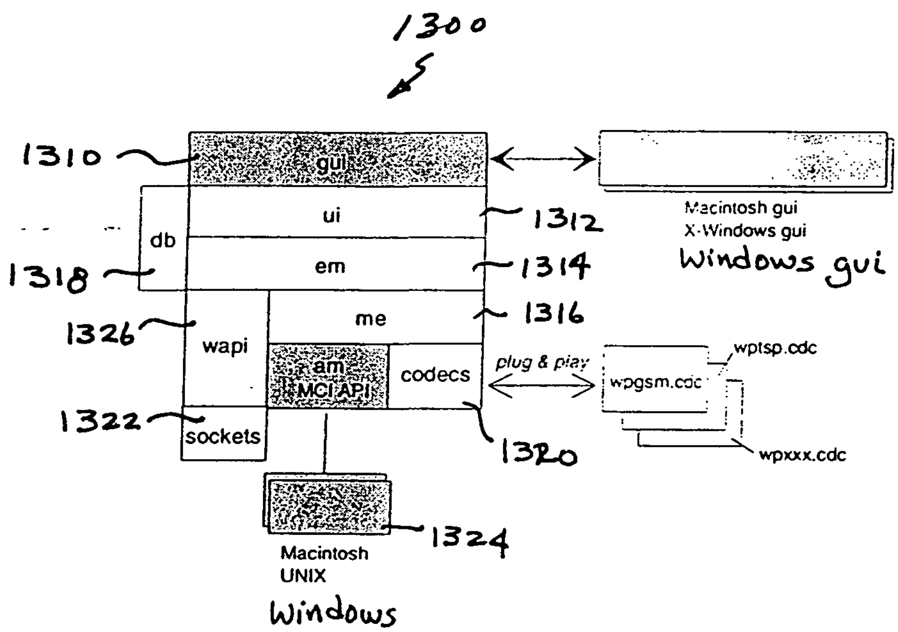


Fig. 13A

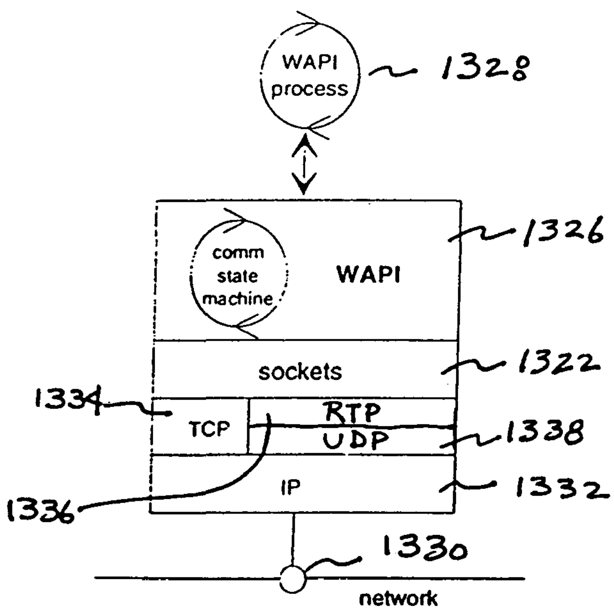

WAPI
process
1328
comm
state
machine
WAPI
1326
sockets
1322
1334
TCP
RTP
UDP
1338
1336
IP
1332
1330
network

Fig. 13B

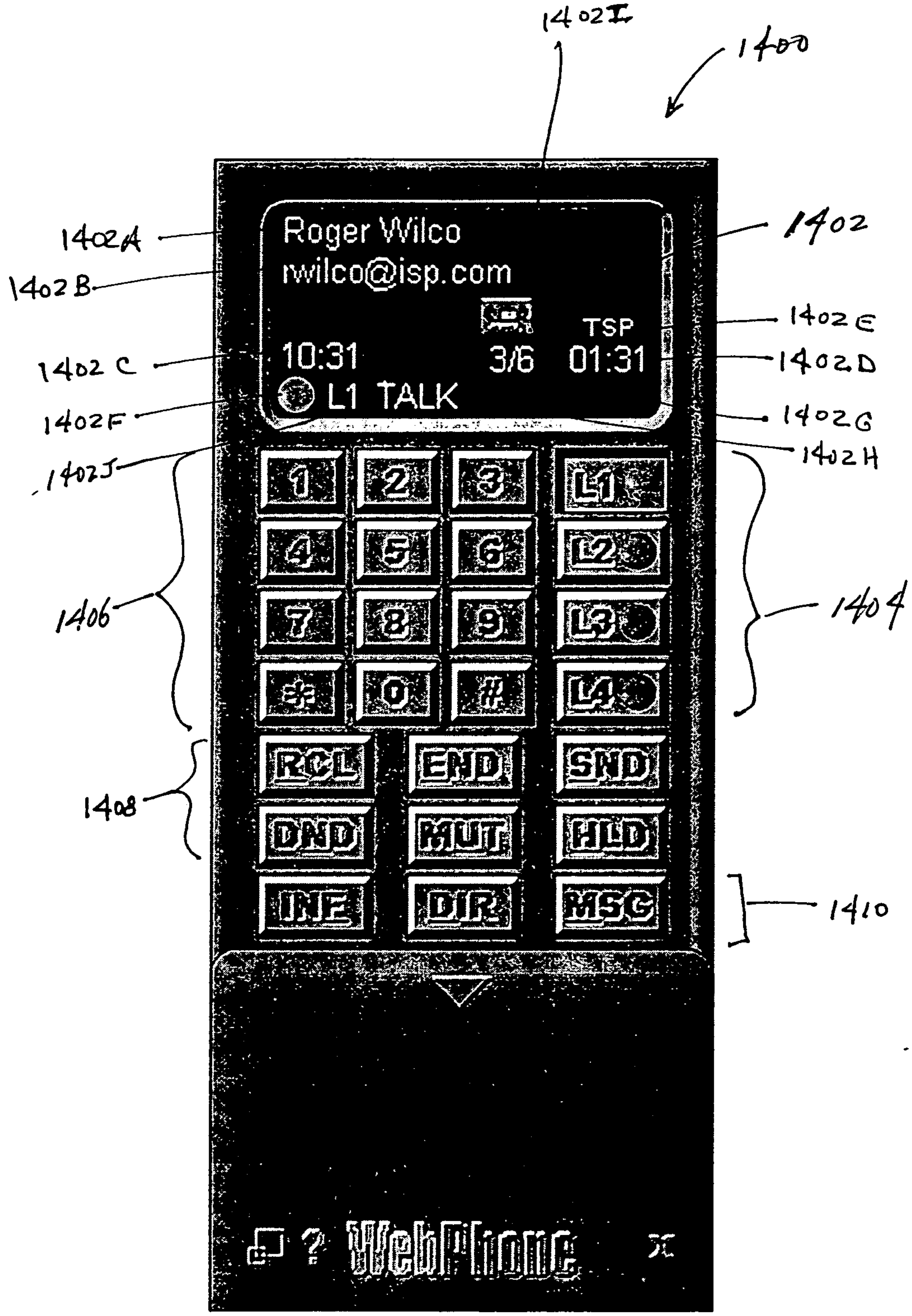

1402I
1400
1402A
1402B
1402C
1402F
1402J
1402
1402E
1402D
1402G
1402H
Roger Wilco
rwilco@isp.com
TSP
10:31
3/6
01:31
L1 TALK
1
2
3
L1
4
5
6
L2
7
8
9
L3
*
0
#
L4
1406
1404
RCL
END
SND
DND
MUT
HLD
INF
DIR
MSG
1408
1410
WebPhone

Figure 14

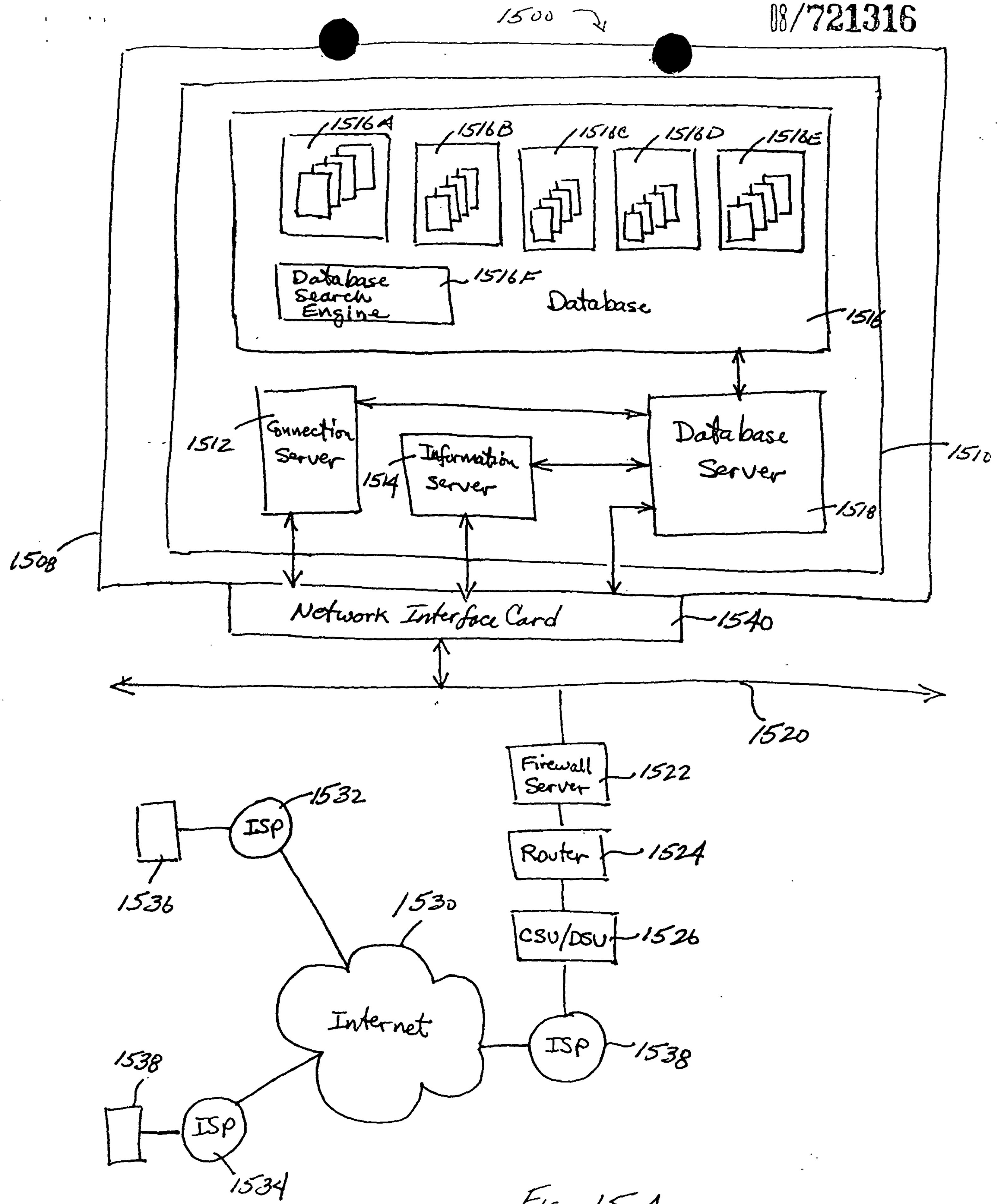

1500
1516A
1516B
1516C
1516D
1516E
Database Search Engine
1516F
Database
1516
Connection Server
1512
Information Server
1514
Database Server
1518
1510
1508
Network Interface Card
1540
1520
Firewall Server
1522
Router
1524
CSU/DSU
1526
ISP
1532
1536
1530
Internet
ISP
1538
1538
ISP
1534

Fig. 15A

08/721316

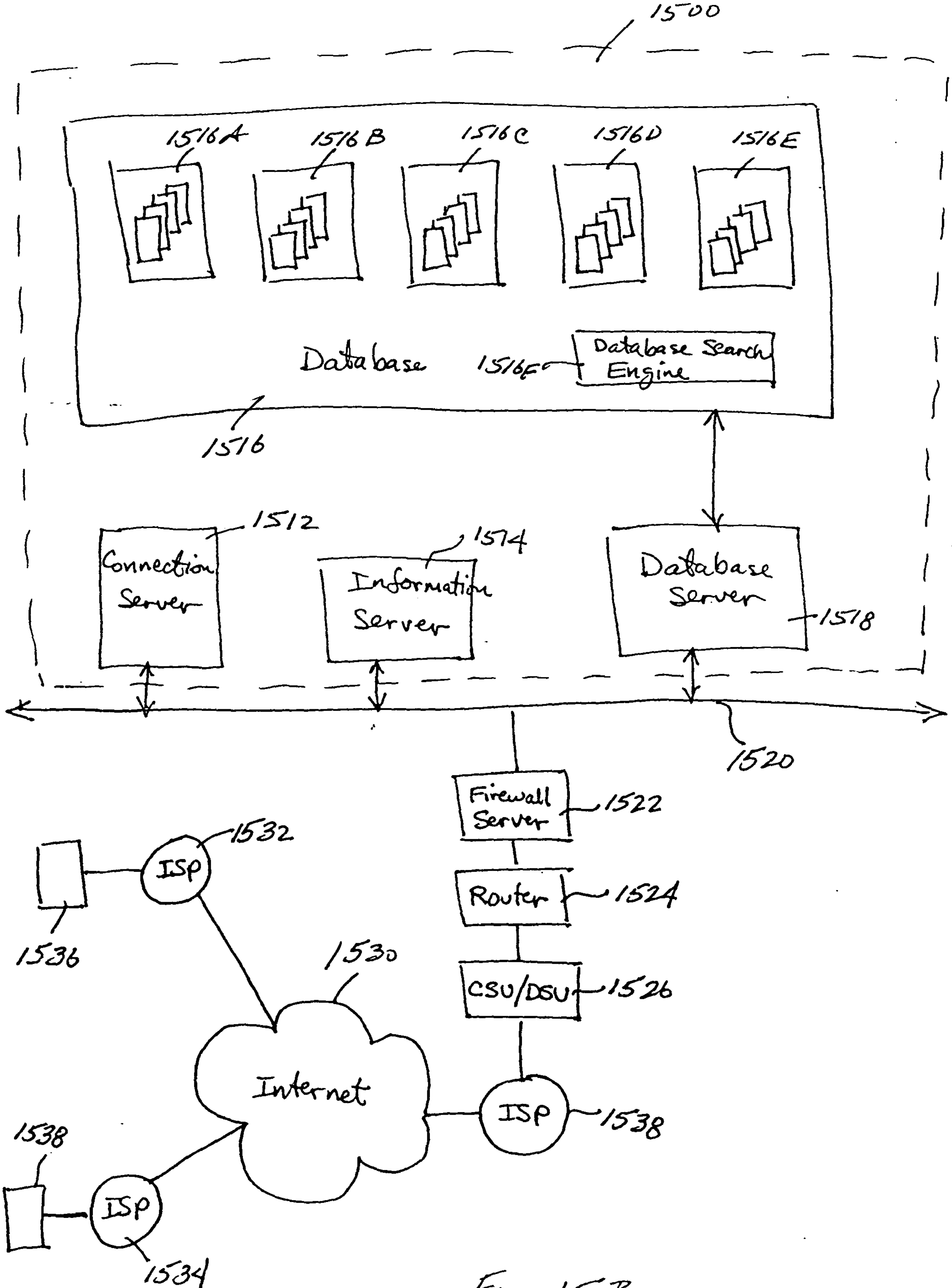


Fig. 15B

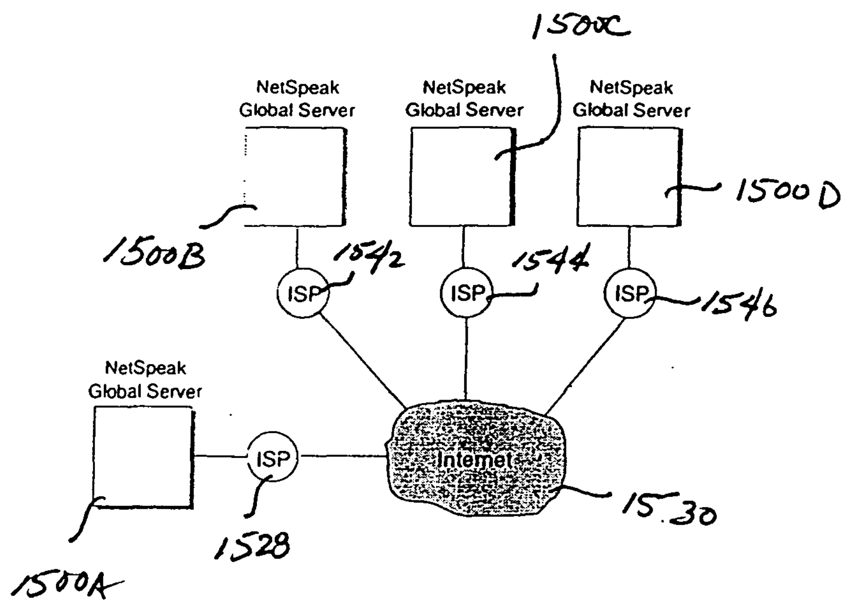

1500C
NetSpeak Global Server
NetSpeak Global Server
NetSpeak Global Server
1500D
1500B
1542
1544
ISP
ISP
ISP
1546
NetSpeak Global Server
ISP
Internet
1530
1528
1500A

Fig. 15C

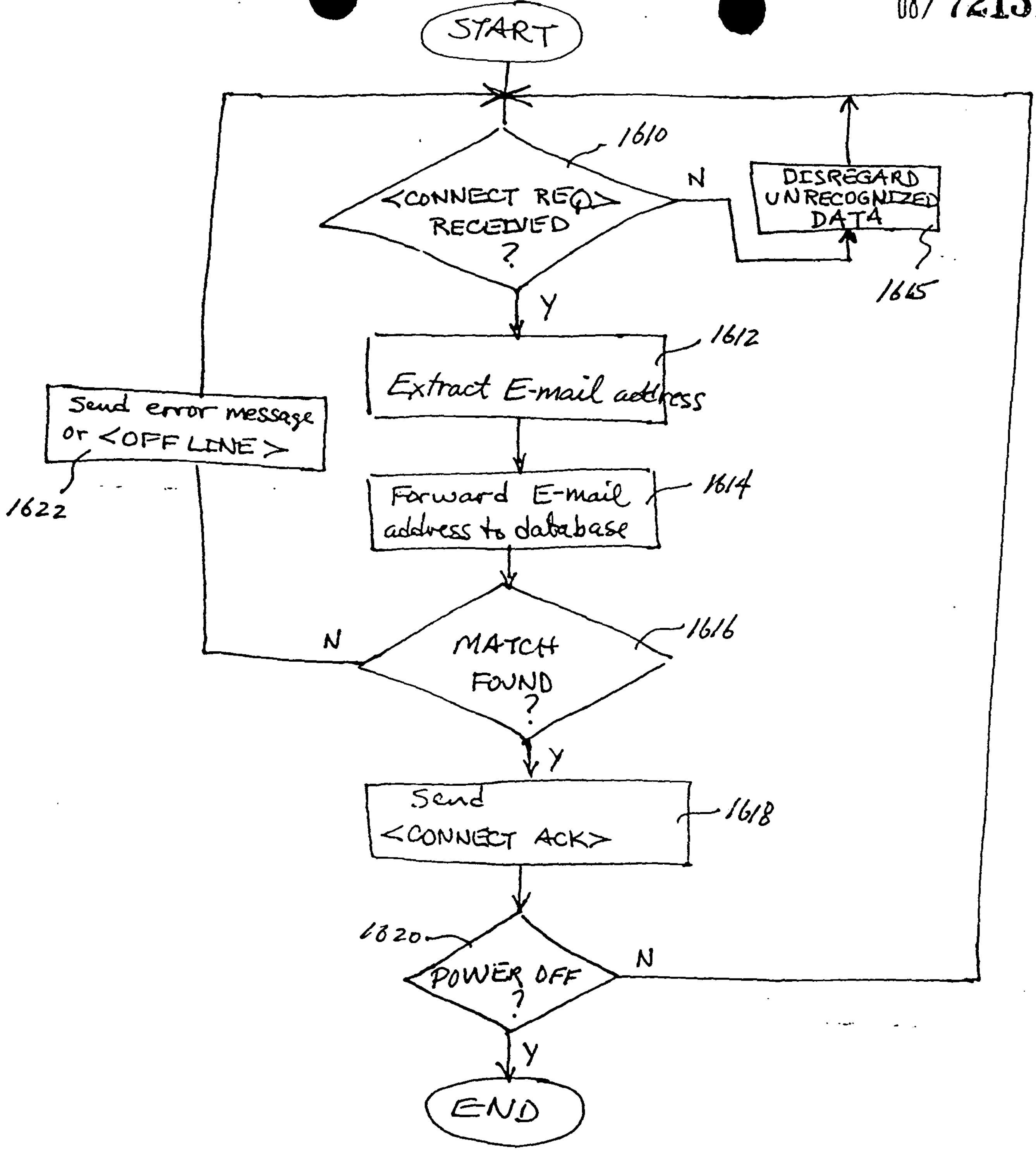

START
1610
<CONNECT REQ>
RECEIVED
?
N
DISREGARD
UNRECOGNIZED
DATA
1615
Y
1612
Extract E-mail address
Send error message
or <OFF LINE>
1622
Forward E-mail
address to database
1614
N
MATCH
FOUND
?
1616
Y
Send
<CONNECT ACK>
1618
1620
POWER OFF
?
N
Y
END

Fig. 16A

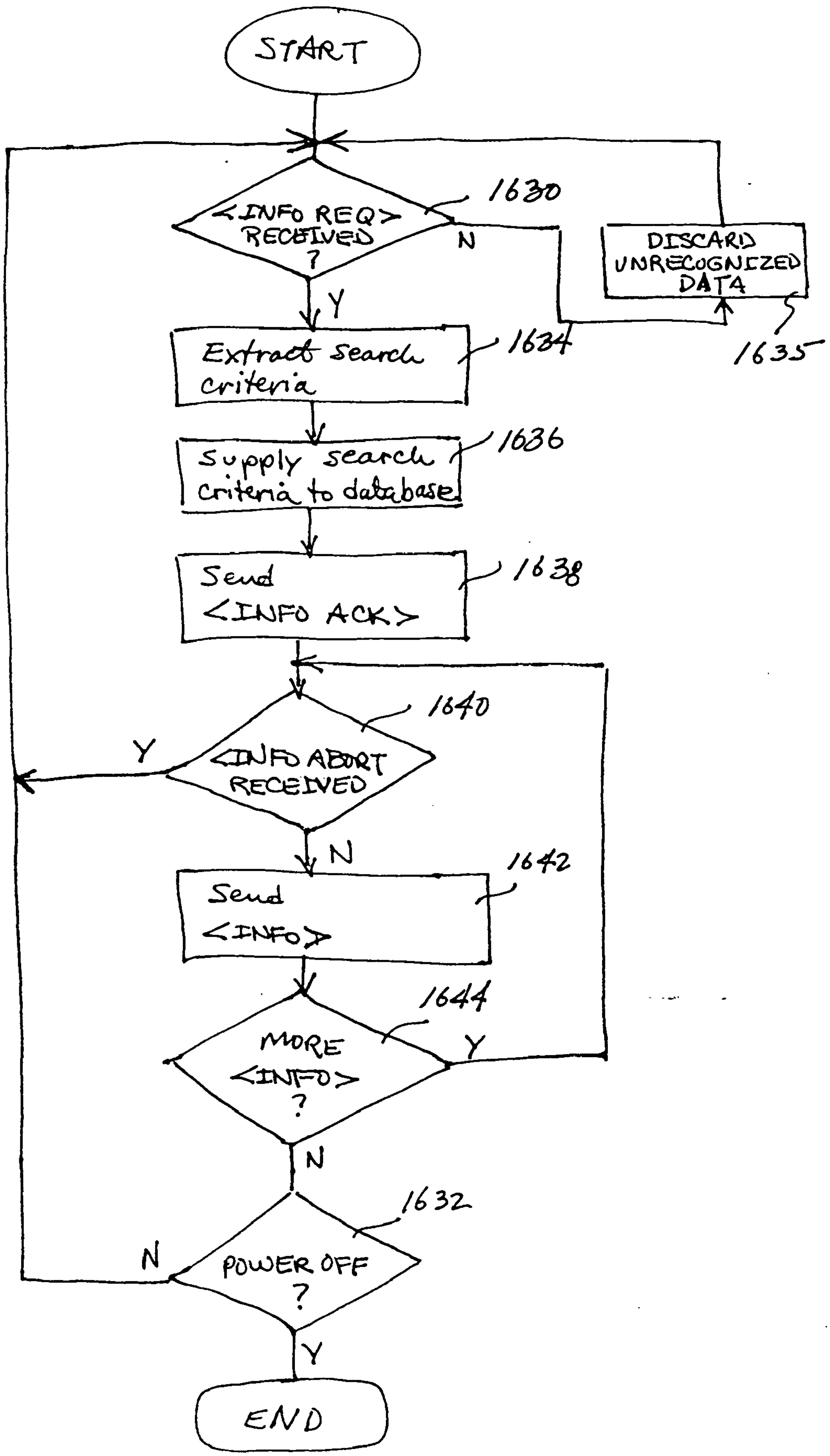

START
<INFO REQ> RECEIVED ?
1630
N
Y
DISCARD UNRECOGNIZED DATA
1635
Extract search criteria
1634
Supply search criteria to database
1636
Send <INFO ACK>
1638
<INFO ABORT RECEIVED
1640
Y
N
Send <INFO>
1642
MORE <INFO> ?
1644
Y
N
POWER OFF ?
1632
N
Y
END

Fig. 16B

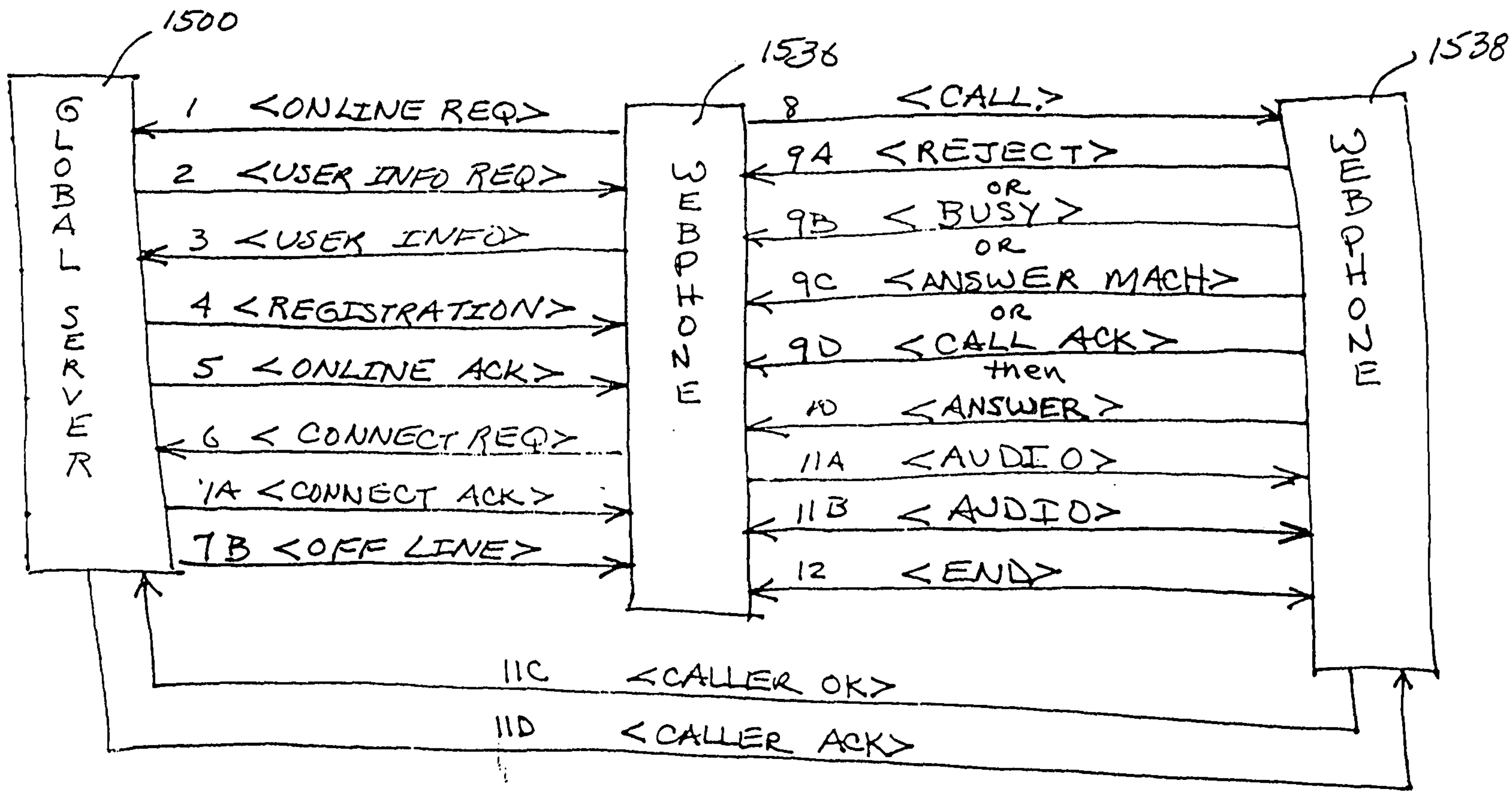


Fig. 17A

08/721316

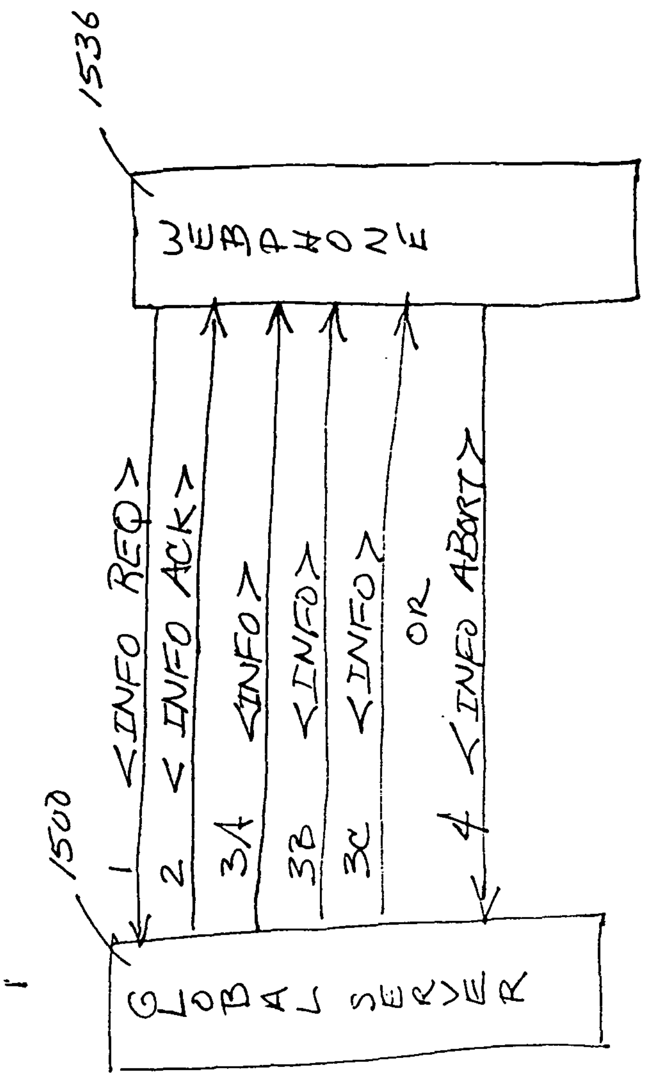

1536
WEBPHONE
1
<INFO REQ>
2
<INFO ACK>
3A
<INFO>
3B
<INFO>
3C
<INFO>
OR
4
<INFO ABORT>
1500
GLOBAL SERVER

Fig. 17B

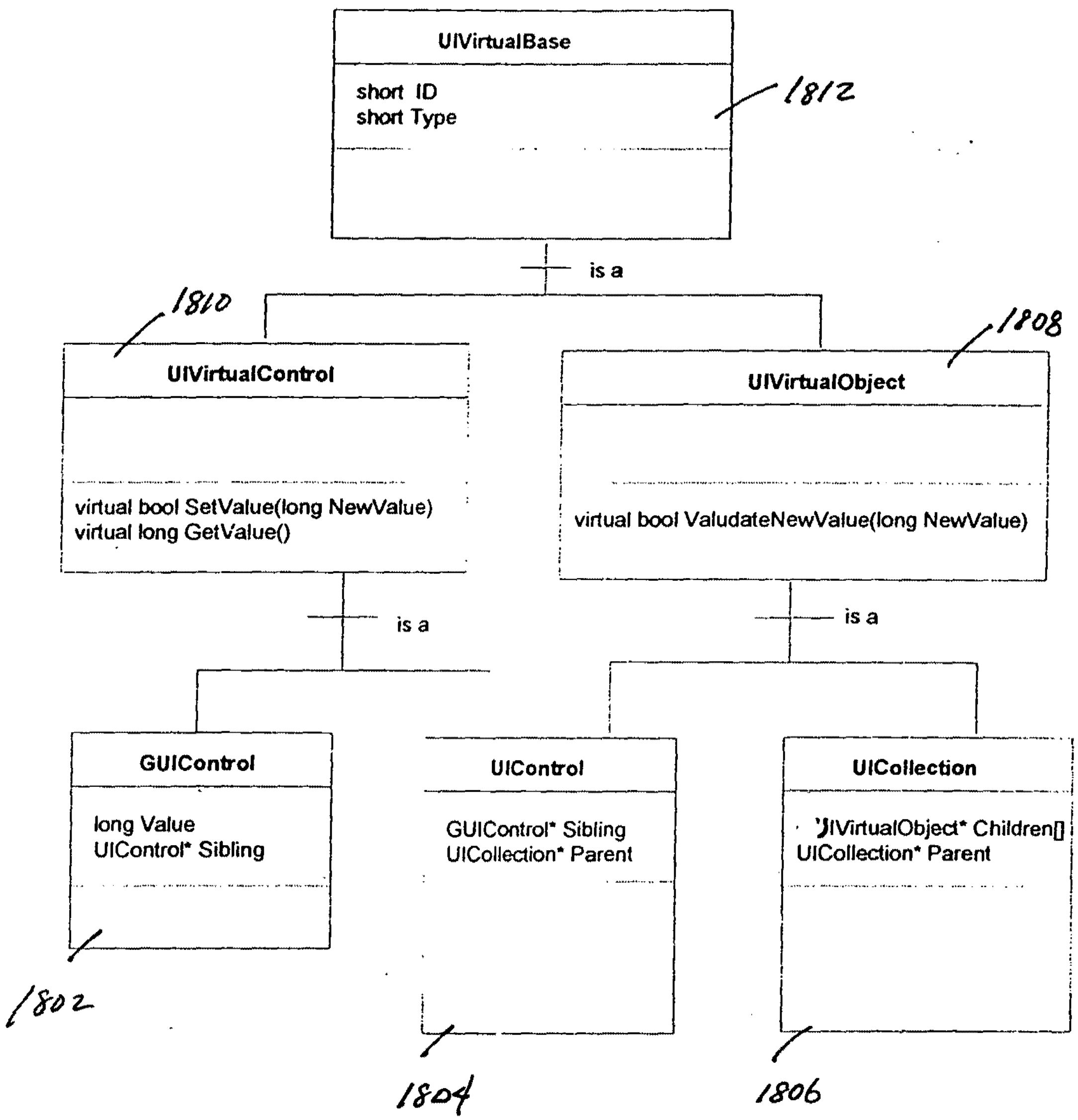

UIVirtualBase
short ID
short Type
1812
is a
1810
UIVirtualControl
virtual bool SetValue(long NewValue)
virtual long GetValue()
1808
UIVirtualObject
virtual bool ValudateNewValue(long NewValue)
is a
is a
GUIControl
long Value
UIControl* Sibling
UIControl
GUIControl* Sibling
UICollection* Parent
UICollection
UIVirtualObject* Children[]
UICollection* Parent
1802
1804
1806

Fig. 18A

16

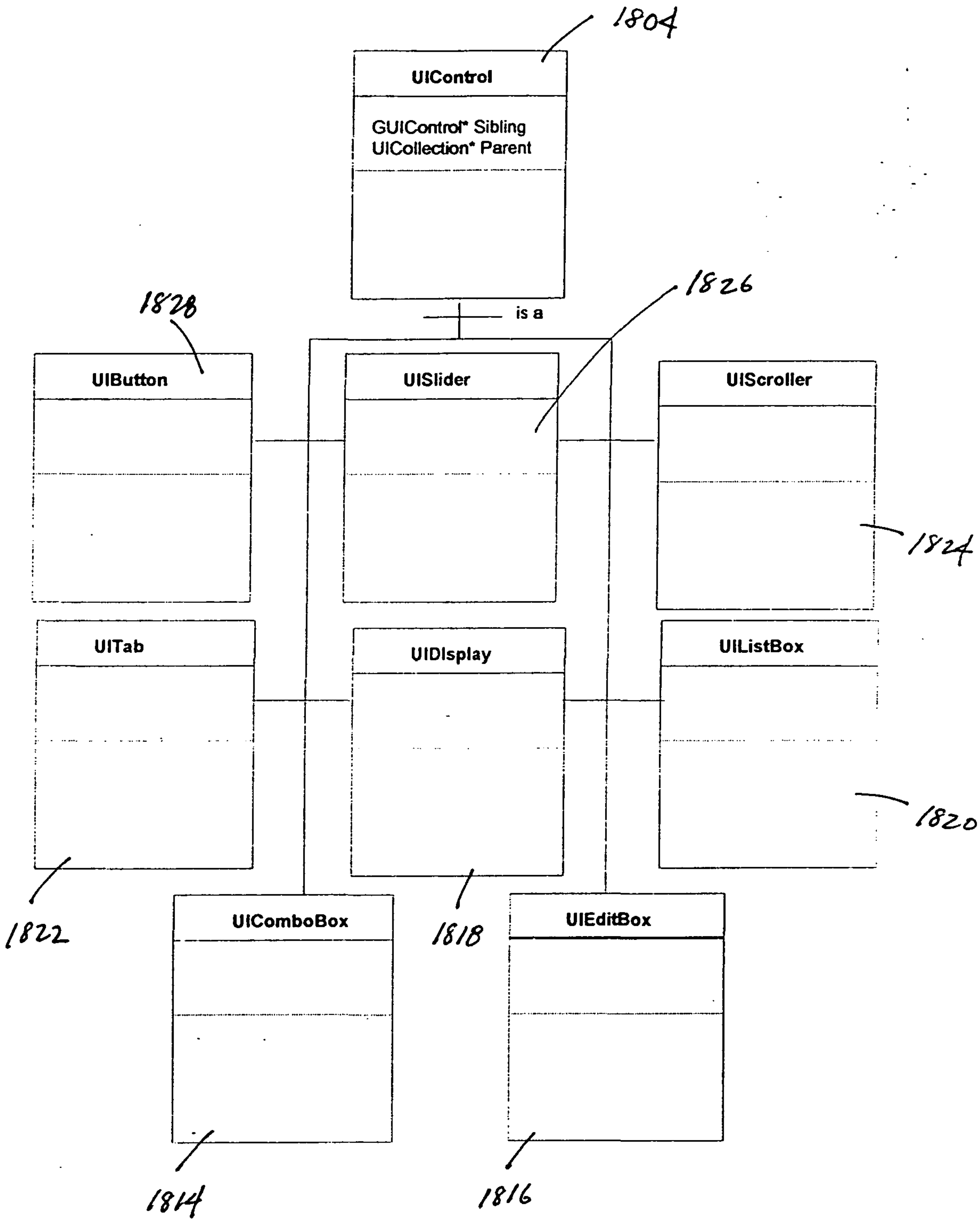


Fig. 18B

08/721316

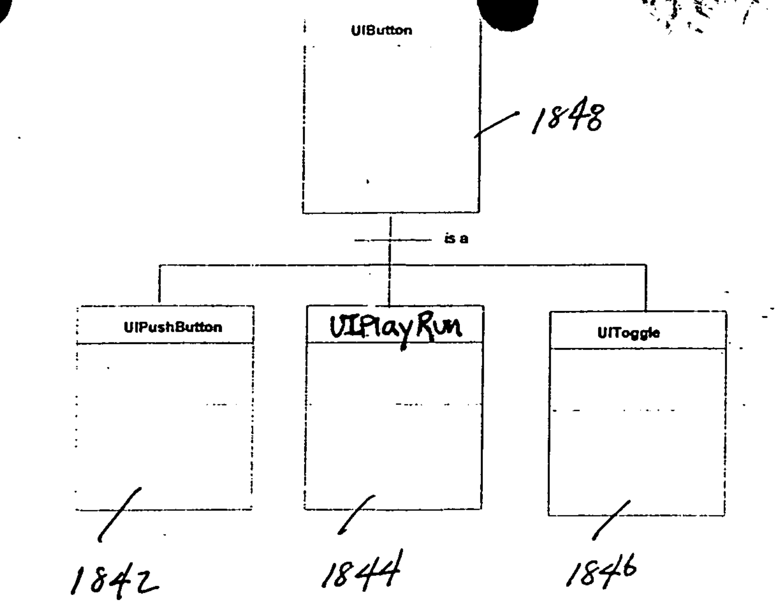


Fig. 18C

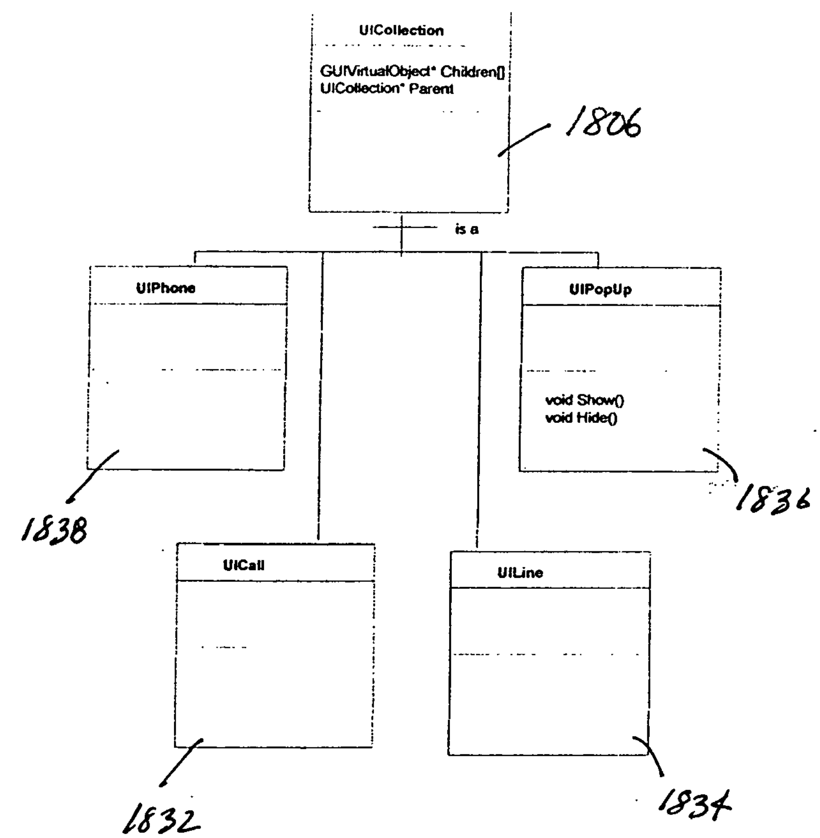


Fig. 18D

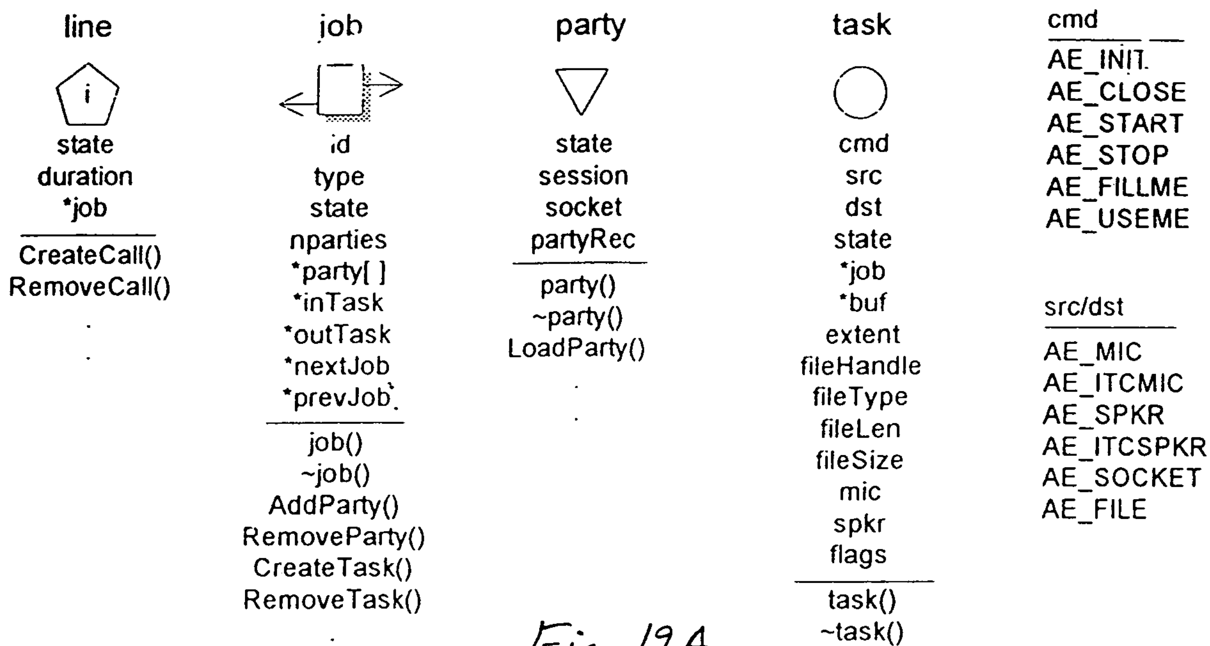


Fig. 19A

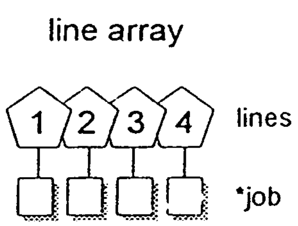


Fig. 19B

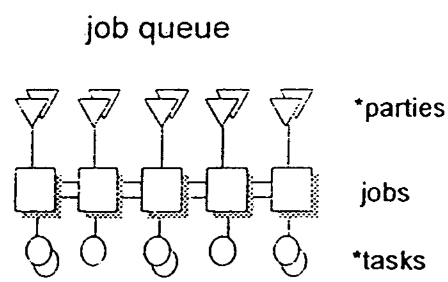


Fig. 19C

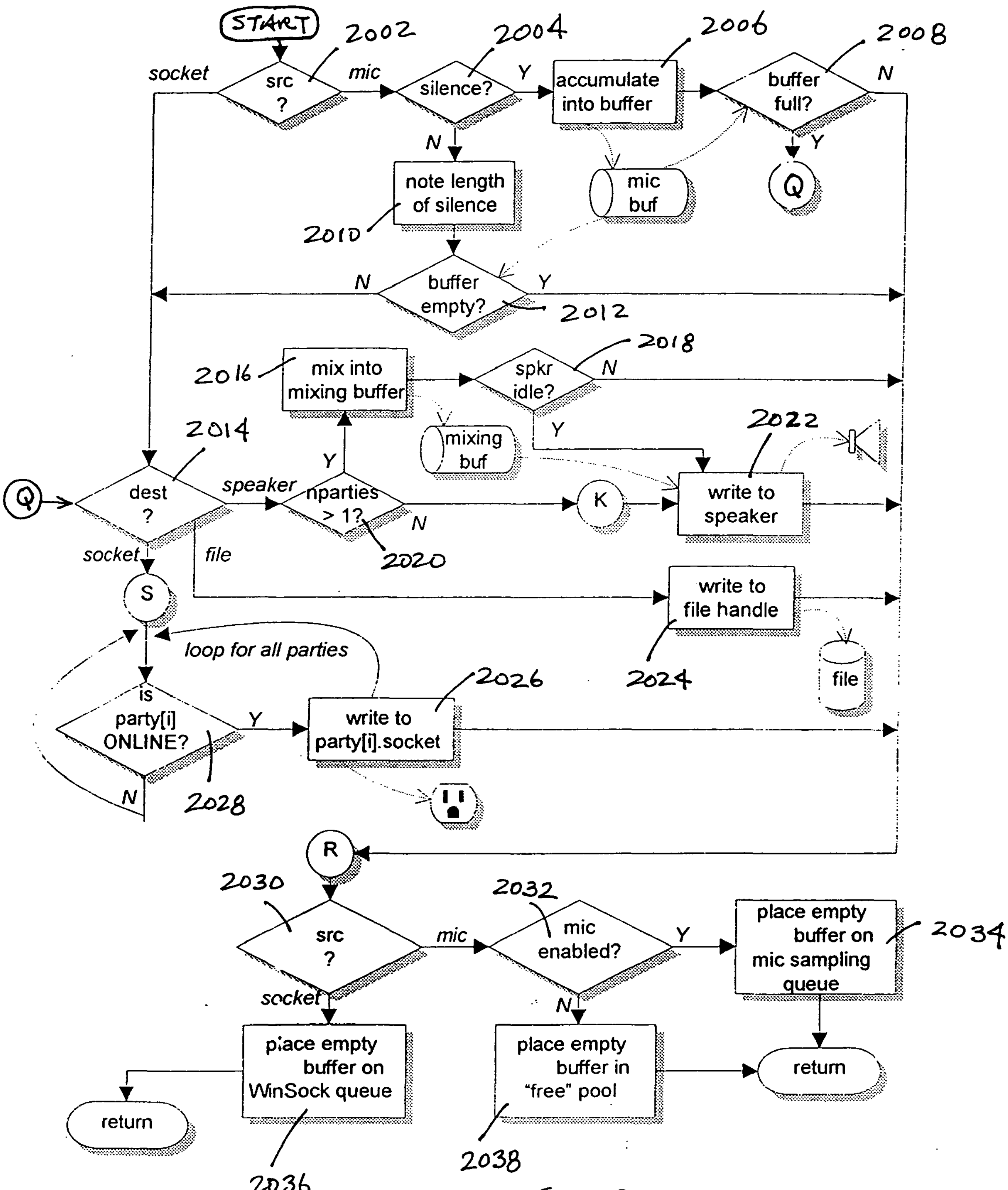

START
2002
src ?
socket
mic
2004
silence?
Y
N
2006
accumulate into buffer
2008
buffer full?
N
Y
Q
mic buf
note length of silence
2010
buffer empty?
N
Y
2012
2016
mix into mixing buffer
2018
spkr idle?
N
Y
mixing buf
2022
2014
dest ?
speaker
nparties > 1?
Y
N
2020
K
write to speaker
Q
socket
file
S
write to file handle
2024
file
loop for all parties
is party[i] ONLINE?
Y
N
2028
write to party[i].socket
2026
R
2030
src ?
mic
socket
2032
mic enabled?
Y
N
place empty buffer on mic sampling queue
2034
place empty buffer on WinSock queue
2036
place empty buffer in "free" pool
2038
return
return

Fig. 20A

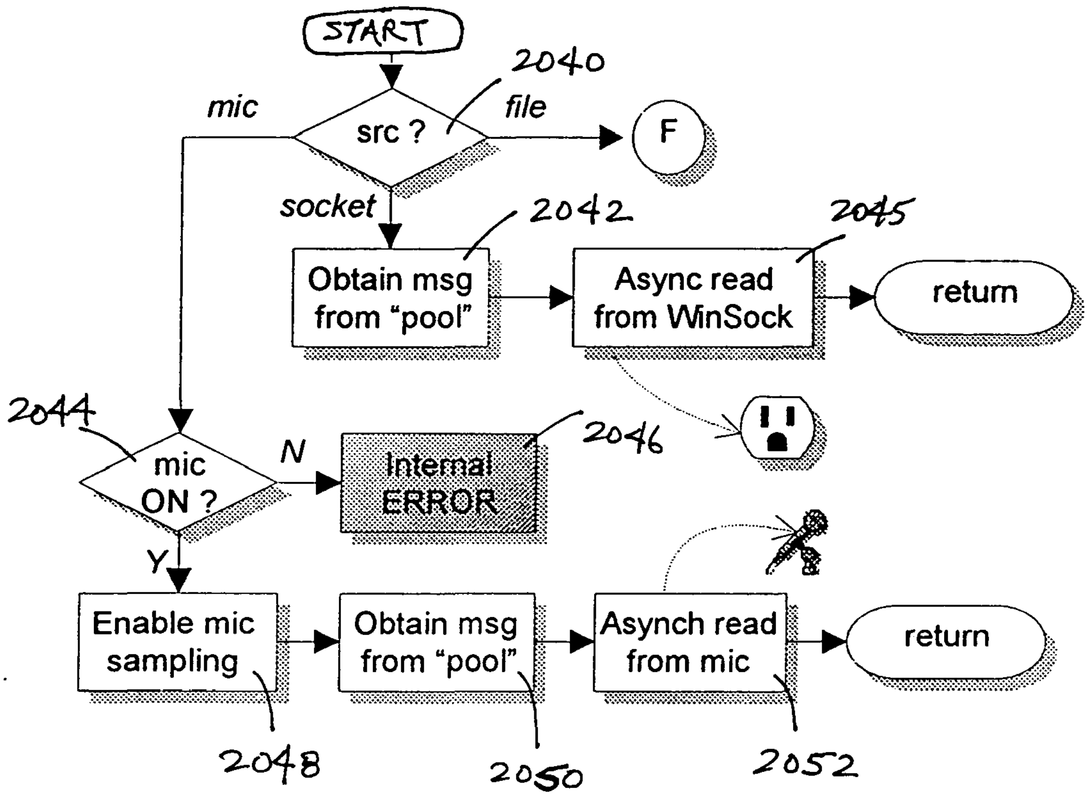

START
2040
mic
src ?
file
F
socket
2042
2045
Obtain msg from "pool"
Async read from WinSock
return
2044
mic ON ?
N
Internal ERROR
2046
Y
Enable mic sampling
Obtain msg from "pool"
Asynch read from mic
return
2048
2050
2052

Fig. 20B

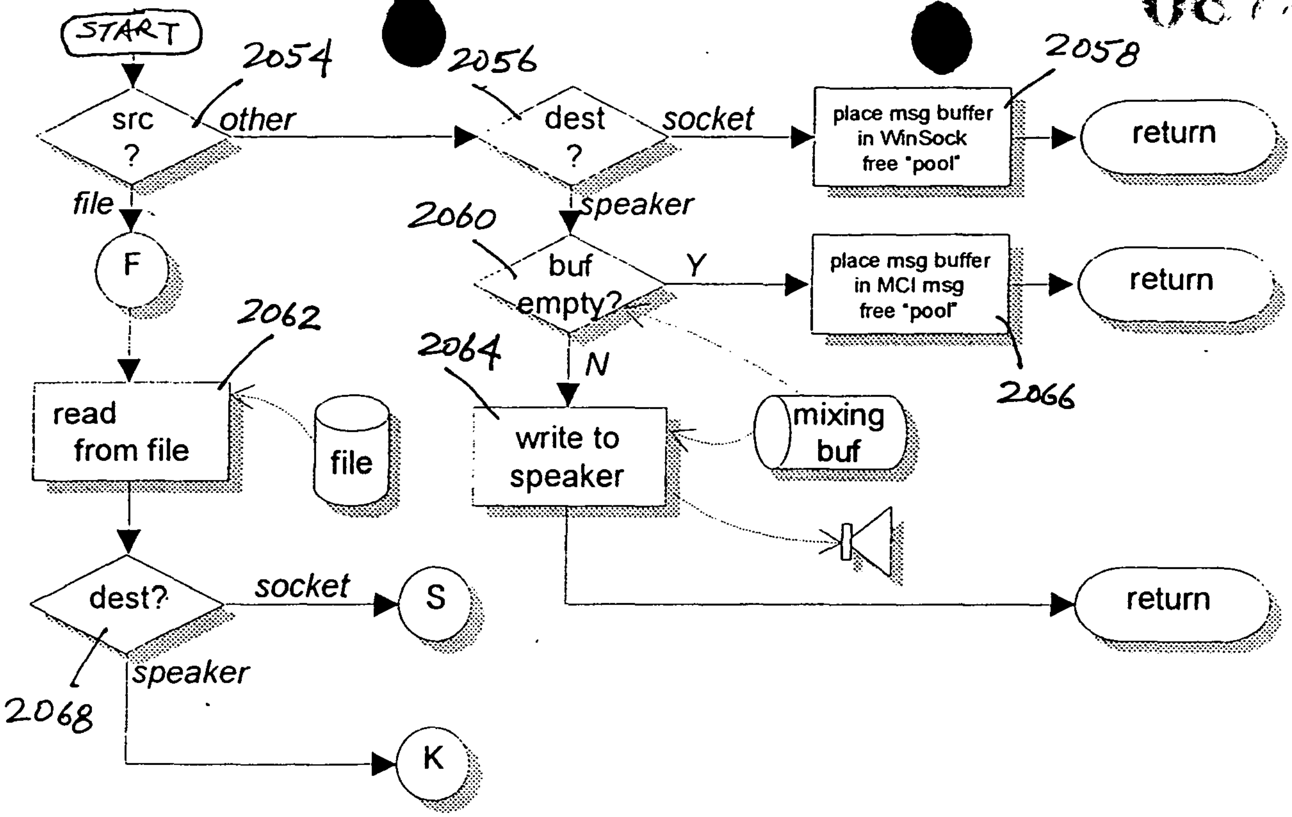

START
src ?
2054
other
file
F
2056
dest ?
socket
speaker
2058
place msg buffer in WinSock free "pool"
return
2060
buf empty?
Y
N
place msg buffer in MCI msg free "pool"
return
2066
2062
read from file
file
2064
write to speaker
mixing buf
return
dest?
socket
S
speaker
2068
K

Fig. 20C

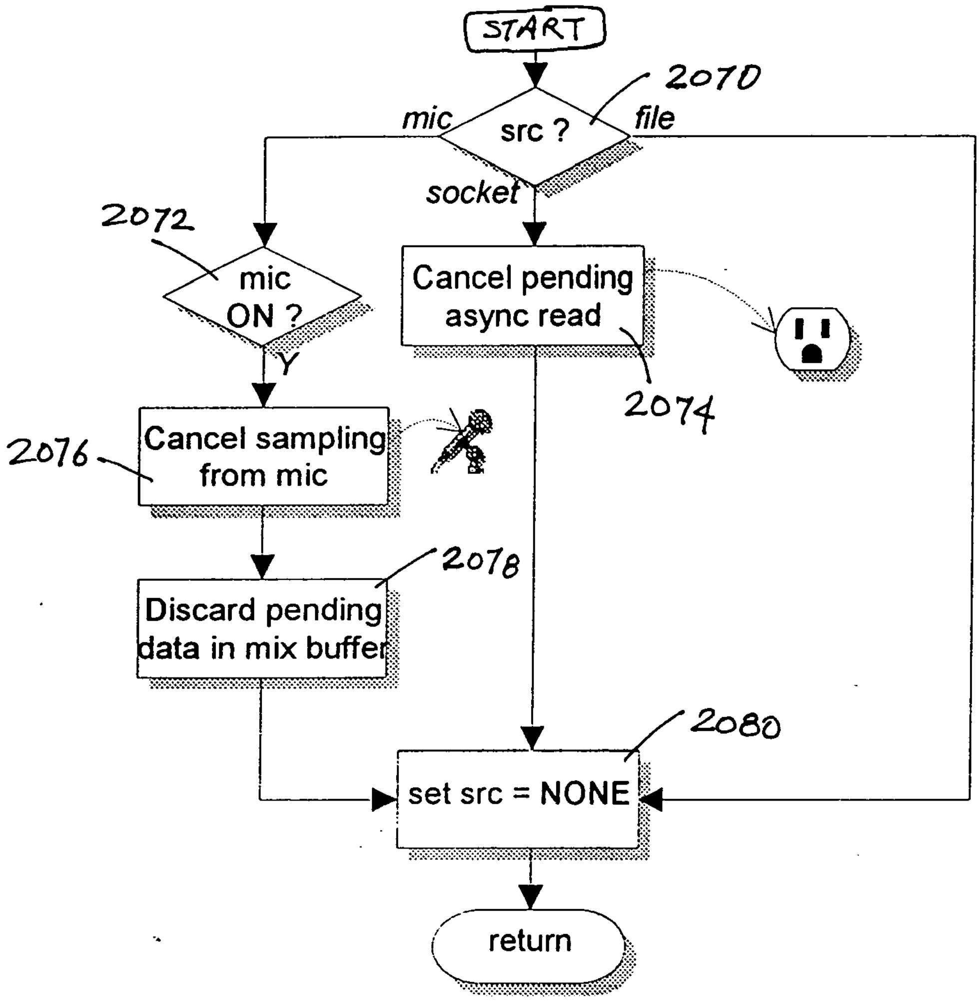

START
2070
mic
src ?
file
socket
2072
mic
ON ?
Y
Cancel pending
async read
2074
Cancel sampling
from mic
2076
2078
Discard pending
data in mix buffer
2080
set src = NONE
return

Fig. 20D

PATENT
N0003/7002

MAIL ROOM
15 SEP 1998

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to:

ASSISTANT COMMISSIONER FOR PATENTS AND TRADEMARKS, WASHINGTON, DC 20231

and bearing Label Number EM316008331US

Bruce D. Jobse

PATENT

Inventors: Shane D. Mattaway, Glenn W. Hutton, and Craig B. Strickland

GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

RELATED APPLICATIONS

This application is a continuation-in-part of United States patent application serial number 08/533,115 (Pending) entitled Point-to-Point Internet Protocol, by Glenn W. Hutton, filed September 25, 1995, commonly assigned, the subject matter of which is incorporated herein by reference.

To the extent that any matter contained herein is not already disclosed in the above-identified parent application, this application claims priority to United States provisional patent application 60/025,415 ~~08/523,770~~ ~~XX/XXX,XXX~~ entitled Internet Telephony Apparatus and Method by Mattaway et al., filed September 4, 1996, and United States provisional patent application serial number 60/024,251 ~~XX/XXX,XXX~~ entitled System and Methods for Point-To-Point Communications Over a Computer Network, by Mattaway et al., filed August 21, 1996.

In addition, this application is one of a number of related applications filed on an even date herewith and commonly assigned, the subject matters of which are incorporated herein by reference, including the following:

U.S. Patent Application Serial No. 08/719,894 ~~XX/XXX,XXX,~~ entitled Directory Server For Providing Dynamically Assigned Network Protocol Addresses, by Mattaway et al.;

U.S. Patent Application Serial No. 08/719,554 ~~XX/XXX,XXX,~~ entitled Point-to-point Computer Network Communication Utility Utilizing Dynamically Assigned Network Protocol Addresses, by Mattaway et al.;

U.S. Patent Application Serial No. 08/719,640 ~~XX/XXX,XXX~~, entitled Method And Apparatus For Dynamically Defining Data Communication Utilities, by Mattaway et al.;

08/721316

U.S. Patent Application Serial No. 08/719,891 ~~XX/XXX,XXX,~~ entitled Method And Apparatus For Distribution And Presentation Of Multimedia Data Over A Computer Network, by Mattaway et al.;

U.S. Patent Application Serial No. 08/719,898 ~~XX/XXX,XXX~~, entitled Method And Apparatus For Providing Caller Identification Based Out-going Messages In A Computer Telephony Environment, by Mattaway et al.;

U.S. Patent Application Serial No. 08/718,911 ~~XX/XXX,XXX,~~ entitled Method And Apparatus For Providing Caller Identification Based Call Blocking In A Computer Telephony Environment, by Mattaway et al.; and

U.S. Patent Application Serial No. 08/719,639 ~~XX/XXX,XXX,~~ entitled Method And Apparatus For Providing Caller Identification Responses In A Computer Telephony Environment, by Mattaway et al.

FIELD OF THE INVENTION

The present invention relates, in general, to data processing systems, and more specifically, to a method and apparatus for facilitating audio communications over computer networks.

BACKGROUND OF THE INVENTION

The increased popularity of on-line services such as AMERICA ONLINE™, COMPUSERVE®, and other services such as Internet gateways have spurred applications to provide multimedia, including video and voice clips, to online users. An example of an online voice clip application is VOICE E-MAIL FOR WINCIM and VOICE E-MAIL FOR AMERICA ONLINE™, available from Bonzi Software, as described in "Simple Utilities Send Voice E-Mail Online", MULTIMEDIA WORLD, VOL. 2, NO. 9, August 1995, p. 52. Using such Voice E-Mail software, a user may create an audio message to be sent to a predetermined E-mail address specified by the user.

Generally, devices interfacing to the Internet and other online services may communicate with each other upon establishing respective device addresses. One type of device address is the Internet Protocol (IP) address, which acts as a pointer to the device associated with the IP address. A typical device may have a Serial Line Internet Protocol or Point-to-Point Protocol (SLIP/PPP) account with a permanent IP address for receiving E-mail, voicemail, and the like over the Internet. E-mail and voicemail is generally intended to convey text, audio, etc., with any routing information such as an IP address and routing headers generally being considered an artifact of the communication, or even gibberish to the recipient.

Devices such as a host computer or server of a company may include multiple modems for connection of users to the Internet, with a temporary IP address allocated to each user. For example, the host computer may have a general IP address "XXX.XXX.XXX," and each user may be allocated a successive IP address of XXX.XXX.XXX.10, XXX.XXX.XXX.11, XXX.XXX.XXX.12, etc. Such temporary IP addresses may be reassigned or recycled to the users, for example, as each user is successively connected to an outside party. For example, a host computer of a company may support a maximum of 254 IP addresses which are pooled and shared between devices connected to the host computer.

Permanent IP addresses of users and devices accessing the Internet readily support point-to-point communications of voice and video signals over the Internet. For example, real-time video teleconferencing has been implemented using dedicated IP addresses and mechanisms known as reflectors. Due to the dynamic nature of temporary IP addresses of some devices accessing the Internet, point-to-point communications in real-time of voice and video have been generally difficult to attain.

4

The ability to locate users having temporary or dynamically assigned Internet Protocol address has been difficult without the user manually initiating the communication. Accordingly, spontaneous, real-time communications with such users over computer networks have been impractical. Further, it is desirable to have a communication utility which contains familiar features and functions to current communication utility such as telephones and cellular telephones. It is even further desirable to utilize the current graphic user interface technology associated with computer software in a manner to achieve a more flexible interface to a such a communication utility, without the limitations associated with hardware.

Accordingly, a need exists for a way to determine whether computer users are actively connected to a computer network.

A further need exists for a way to obtain the dynamically assigned Internet Protocol address of a user having on-line status with respect to a computer network, particularly the Internet.

An even further need exists for a method and apparatus by which to establish real-time, point-to-point communications over a computer network using a communication utility having an interface which combines the familiar aspects of current hardware communication utilities but which allows for the flexibility associated with graphic user interfaces.

SUMMARY OF THE INVENTION

The above deficiencies in the prior art and previously described needs are fulfilled by the present invention which provides a virtual communications utility displayable on computer system interfaces which enables real-time, point-to-point communications over computer networks. According to one embodiment of the present invention, a computer program product for use with a computer system having a display and an audio transducer comprises a computer usable medium having computer readable code means embodied therein comprising program code means for generating a user interface, program code means responsive to user input commands for establishing a point-to-point communication link with another computer over a network and program code means responsive to audio data from the audio transducer for transmitting the audio data over the communication link.

According to another embodiment of the present invention, a computer program product for use with a computer system comprises a computer usable medium having computer readable program code means embodied thereon comprising code means for transmitting from a client process to a server a query as to whether a second client process is connected to the computer network, program code means for receiving the network protocol address of the second process from the server, and program code means responsive to the network protocol address of the second client process for establishing a point-to-point communication link between the first client process and the second client process.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the invention will become more readily apparent and may be better understood by referring to the following detailed description of an illustrative embodiment of the present invention, taken in conjunction with the accompanying drawings, in which:

Fig. 1 illustrates, in block diagram format, a system for the disclosed point-to-point Internet protocol;

Fig. 2 illustrates, in block diagram format, the system using a secondary point-to-point Internet protocol;

Fig. 3 illustrates, in block diagram format, the system of FIGS. 1-2 with the point-to-point Internet protocol established;

Fig. 4 is another block diagram of the system of FIGS 1-2 with audio communications being conducted;

Fig. 5 illustrates a display screen for a processing unit;

Fig. 6 illustrates another display screen for a processing unit;

Fig. 7 illustrates a flowchart of the initiation of the point-to-point Internet protocols;

Fig. 8 illustrates a flowchart of the performance of the primary point-to-point Internet protocols;

Fig. 9 illustrates a flowchart of the performance of the secondary point-to-point Internet protocol;

Fig. 10 illustrates schematically a computer network over which the present invention may be utilized;

Fig. 11 is a block diagram of a computer system suitable for use with the present invention;

Fig. 12 is a block diagram of an audio processing card suitable for use with the computer system of FIG. 10;

Fig. 13 A-B are schematic block diagrams of the elements comprising the inventive computer network telephony mechanism of the present invention;

Fig. 14 is a screen capture illustrating an exemplary user interface of the present invention;

Fig. 15 is a schematic diagram illustrating the architecture of the connection server apparatus suitable for use with the present invention;

Fig. 16A is a flowchart illustrating the process steps performed by the connection server in accordance with the present invention;

Fig. 16B is a flowchart illustrating the process steps performed in accordance with the information server of the present invention;

Figs. 17A-B are schematic block diagrams illustrating of the packet transfer sequence in accordance with the communication protocol of the present invention;

Fig. 18A-D are conceptual block diagrams illustrating user interface and graphic user interface objects utilized by the communication utility of the present invention;

Fig. 19A-C are conceptual block diagrams illustrating the event manager and media engine objects utilized by the communication utility of the present invention; and

Figs. 20A-D illustrate process steps performed by the media engine function of the communication utility in accordance with the present invention.

DETAILED DESCRIPTION

Referring now in specific detail to the drawings, with like reference numerals identifying similar or identical elements, as shown in FIG. 1, the present disclosure describes a point-to-point network protocol and system 10 for using such a protocol.

In an exemplary embodiment, the system 10 includes a first processing unit 12 for sending at least a voice signal from a first user to a second user. The first processing unit 12 includes a processor 14, a memory 16, an input device 18, and an output device 20. The output device 20 includes at least one modem capable of, for example, 14.4 Kilobit-per-second communications and operatively connected via wired and/or wireless communication connections to the Internet or other computer networks such as an Intranet, i.e., a private computer network. One skilled in the art would understand that the input device 18 may be implemented at least in part by the modem of the output device 20 to allow input signals from the communication connections to be received. The second processing unit 22 may have a processor, memory, and input and output devices, including at least one modem and associated communication connections, as described above for the first processing unit 12. In an exemplary embodiment, each of the processing units 12, 22 may execute the WEBPHONE® Internet telephony application available from NetSpeak Corporation, Boca Raton, FL, which is capable of performing the disclosed point-to-point Internet protocol and system 10, as described herein.

The first processing unit 12 and the second processing unit 22 are operatively connected to the Internet 24 by communication devices and software known in the art, such as an Internet Service Provider (ISP) or an Internet gateway. The processing units 12, 22 may be operatively interconnected through the Internet 24 to a connection server 26, and may also be operatively connected to a mail server 28 associated with the Internet 24.

The connection server 26 includes a processor 30, a timer 32 for generating time stamps, and a memory such as a database 34 for storing, for example, E-mail and Internet Protocol (IP) addresses of logged-in units. In an exemplary embodiment, the connection server 26 may be a SPARC 5 server or a SPARC 20 server, available from SUN MICROSYSTEMS, INC., Mountain View, CA, having a central processing unit (CPU) as processor 30, an operating system (OS) such as UNIX, for providing timing operations such as maintaining the timer 32, a hard drive or fixed drive, as well as dynamic random access memory (DRAM) for storing the database 34, and a keyboard and display and/or other input and output devices (not shown in FIG. 1). The database 34 may be an SQL database available from ORACLE or INFORMIX.

In an exemplary embodiment, the mail server 28 may be implemented with a Post Office Protocol (POP) Version 3 mail server and the Simple Mail Transfer Protocol (SMTP), including a processor, memory, and stored programs operating in a UNIX environment, or, alternatively, another OS, to process E-mail capabilities between processing units and devices over the Internet 24.

In the illustrative embodiment, the POP protocol is utilized to retrieve E-mail messages from mail server 28 while the SMTP protocol is used to submit E-mail message to Internet 24.

The first processing unit 12 may operate the disclosed point-to-point Internet protocol by a computer program described hereinbelow in conjunction with FIG. 6, which may be implemented from compiled and /or interpreted source code in the C++ programming language and which may be downloaded to the first processing unit 12 from an external computer. The operating computer program may be stored in the memory 16, which may include about 8 MB RAM and/or a hard or fixed drive having about 8 MB of available memory. Alternatively, the source code may be implemented in the first processing unit 12 as firmware, as an erasable read only memory (EPROM), etc. It is understood that one skilled in the art would be able to use programming languages other than C++ to implement the disclosed point-to-point network protocol and system 10.

The processor 14 receives input commands and data from a first user associated with the first processing unit 12 though the input device 18, which may be an input port connected by a wired, optical, or a wireless connection for electromagnetic transmissions, or alternatively may be transferable storage media, such as floppy disks, magnetic tapes, compact disks, or other storage media including the input data from the first user.

The input device 18 may include a user interface (not shown) having, for example, at least one button actuated by the user to input commands to select from a plurality of operating modes to operate the first processing unit 12. In alternative embodiments, the input device 18 may include a keyboard, a mouse, a touch screen, and/or a data reading device such as a disk drive for receiving the input data from input data files stored in storage media such as a floppy disk or, for example, an 8 mm storage tape. The input device 18 may alternatively include connections to other computer systems to receive the input commands and data therefrom.

The first processing unit 12 may include a visual interface for use in conjunction with the input device 18 and output device 20 similar to those screens illustrated in FIGS. 5-6, discussed below. It is also understood that alternative devices may be used to receive commands and data from the user, such as keyboards, mouse devices, and graphical user interfaces (GUI) such as WINDOWS™ 3.1 available form MICROSOFT Corporation, Redmond, WA., and other operating systems and GUIs, such as OS/2 and OS/2 WARP, available from IBM CORPORATION, Boca Raton, FL. Processing unit 12 may also include microphones and/or telephone handsets for receiving audio voice data and commands, speech or voice recognition devices, dual tone multi-frequency (DTMF) based devices, and/or software known in the art to accept voice data and commands and to operate the first processing unit 12.

In addition, either of the first processing unit 12 and the second processing unit 22 may be implemented in a personal digital assistant (PDA) providing modem and E-mail capabilities and Internet access, with the PDA providing the input/output screens for mouse interactions or for touchscreen activation as shown, for example, in FIGS. 5-6, as a combination of the input device 18 and output device 20.

For clarity of explanation, the illustrative embodiment of the disclosed point-to-point Internet protocol and system 10 is presented as having individual functional blocks, which may include functional blocks labeled as "processor" and "processing unit". The functions represented by these blocks may be provided through the use of either shared or dedicated hardware, including, but not limited to, hardware capable of executing software. For example, the functions of each of the processors and processing units presented herein may be provided by a shared processor or by a plurality of individual processors. Moreover, the use of the functional blocks with accompanying labels herein is not to be construed to refer exclusively to hardware capable of executing software. Illustrative embodiments may include digital signal processor (DSP) hardware, such as the AT&T DSP16 or DSP32C, read-only memory (ROM) for storing software performing the operations discussed below, and random access memory (RAM) for storing DSP results. Very large scale integration (VLSI) hardware embodiments, as well as custom VLSI circuitry in combination with a general purpose DSP circuit, may also be provided. Any and all of these embodiments may be deemed to fall within the meaning of the labels for the functional blocks as used herein.

The processing units 12, 22 are capable of placing calls and connecting to other processing units connected to the Internet 24, for example, via dialup SLIP/PPP lines. In an exemplary embodiment, each processing unit assigns an unsigned long session number, for example, a 32-bit long sequence in a *.ini file for each call. Each call may be assigned a successive session number in sequence, which may be used by the respective processing unit to associate the call with one of the SLIP/PPP lines, to associate a <ConnectOK> response signal with a <Connect Request> signal, and to allow for multiplexing and demultiplexing of inbound and outbound conversations on conference lines, as explained hereinafter.

For callee (or called) processing units with fixed IP addresses, the caller (or calling) processing unit may open a "socket", i.e. a file handle or address indicating where data is to be sent, and transmit a <Call> command to establish communication with the callee utilizing, for example, datagram services such as Internet Standard network layering as well as transport layering, which may include a Transport Control Protocol (TCP) or a User Datagram Protocol (UDP) on top of the IP. Typically, a processing unit having a fixed IP address may maintain at least one open socket and a called processing unit waits for a <Call> command to assign the open socket to the incoming signal. If all lines are in use, the callee processing unit sends a BUSY signal or message to the caller processing unit. As shown in FIG. 1, the disclosed point-to-point Internet protocol and system 10 operate when a callee processing unit does not have a fixed or predetermined IP address. In the exemplary embodiment and without loss of generality, the first processing unit 12 is the caller processing unit and the second processing unit 22 is the callee processing unit. When either of processing units 12, 22 logs on to the Internet via a dial-up connection, the respective unit is provided a dynamically allocated IP address by an Internet service provider.

Upon the first user initiating the point-to-point Internet protocol when the first user is logged on to the Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server 26. The connection server 26 then stores these addresses in the database 34 and time stamps the stored addresses using timer 32. The first user operating the first processing unit 12 is thus established in the database 34 as an active on-line party available for communication using the disclosed point-to-point Internet protocol. Similarly, a second user operating the second processing unit 22, upon connection to the Internet 24 through an Internet service provider, is processed by the connection server 26 to be established in the database 34 as an active on-line party.

The connection server 26 may use the time stamps to update the status of each processing unit; for example, after 2 hours, so that the on-line status information stored in the database 34 is relatively current. Other predetermined time periods, such as a default value of 24 hours, may be configured by a systems operator.

The first user with the first processing unit 12 initiates a call using, for example, a Send command and/or a command to speeddial an N^{TH} stored number, which may be labeled [SND] and [SPD] [N], respectively, by the input device 18 and/or the output device 20, such as shown in FIGS. 5-6. In response to either the Send or speeddial commands, the first processing unit 12 retrieves from memory 16 a stored E-mail address of the callee corresponding to the N^{TH} stored number. Alternatively, the first user may directly enter the E-mail address of the callee.

The first processing unit 12 then sends a query, including the E-mail address of the callee, to the connection server 26. The connection server 26 then searches the database 34 to determine whether the callee is logged-in by finding any stored information corresponding to the callee's E-mail address indicating that the callee is active and on-line. If the callee is active and on-line, the connection server 26 then performs the primary point-to-point Internet protocol; i.e. the IP address of the callee is retrieved from the database 34 and sent to the first processing unit 12. The first processing unit 12 may then directly establish the point-to-point Internet communications with the callee using the IP address of the callee.

If the callee is not on-line when the connection server 26 determines the callee's status, the connection server 26 sends an OFF-LINE signal or message to the first processing unit 12. The first processing unit 12 may also display a message such as "Called Party Off-Line" to the first user.

When a user logs off or goes off-line from the Internet 24, the connection server 26 updates the status of the user in the database 34; for example, by removing the user's information, or by flagging the user as being off-line. The connection server 26 may be instructed to update the user's information in the database 34 by an off-line message, such as a data packet, sent automatically from the processing unit of the user prior to being disconnected from the connection server 26. Accordingly, an off-line user is effectively disabled from making and/or receiving point-to-point Internet communications.

As shown in FIGS. 2-4, the disclosed secondary point-to-point Internet protocol may be used as an alternative to the primary point-to-point Internet protocol described above, for example, if the connection server 26 is non-responsive, unreachable, inoperative, and/or unable to perform the primary point-to-point Internet protocol, as a non-responsive condition. Alternatively, the disclosed secondary point-to-point Internet protocol may be used independent of the primary point-to-point Internet protocol. In the disclosed secondary point-to-point Internet protocol, the first processing unit 12 sends a <ConnectReq> message via E-mail over the Internet 24 to the mail server 28. The E-mail including the <ConnectReq> message may have, for example, the subject

[*wp#XXXXXXXX#nnn.nnn.nnn.#emailAddr]

where nnn.nnn.nnn.nnn. is the current (i.e. temporary or permanent) IP address of the first user, and XXXXXXXX is a session number, which may be unique and associated with the request of the first user to initiate point-to-point communication with the second user.

The following E-mail messages are transmitted to a remote users post office protocol server via simple mail transport protocol using MIME by the event manager, as explained hereinafter.

<ConnectRequest>

<CampRequest>

<VoiceMail>

<FileTransfer>

<E-mail>

The following E-mail messages are received from a local WebPhone users POP server via the POP protocol using MIME by the event manager, as explained hereinafter.

<Connect Request>

<Camp Request>

<Voice Mail>

<File Transfer>

<E-mail>

<Registration>

As described above, the first processing unit 12 may send the <ConnectReq> message in response to an unsuccessful attempt to perform the primary point-to-point Internet protocol. Alternatively, the first processing unit 12 may send the <ConnectReq> message in response to the first user initiating a SEND command or the like.

After the <ConnectRequest> message via E-mail is sent, the first processing unit 12 opens a socket and waits to detect a response from the second processing unit 22. A timeout timer, such as timer 32, may be set by the first processing unit 12, in a manner known in the art, to wait for a predetermined duration to receive a <ConnectOK> signal. The processor 14 of the first processing unit 12 may cause the output device 20 to output a Ring signal to the user, such as an audible ringing sound, about every 3 seconds. For example, the processor 14 may output a *.wav file, which may be labeled RING.WAV, which is processed by the output device 20 to output an audible ringing sound.

Second processing unit 22 polls mail server 28 at an interval, for example, once a minute, to check for incoming E-mail. Generally, second processing unit 22 checks the messages stored on mail server 28 at regular intervals to wait for and detect incoming E-mail indicating a <CONNECT REQ> message from first processing unit 12.

Typically, for sending E-mail to user's having associated processing units operatively connected to a host computer or server operating an Internet gateway, E-mail for a specific user may be sent over Internet 24 and directed to the permanent IP address of the mail server providing the target user's mail services. The E-mail is transported by a standard protocol, for example, SMTP, and stored into memory (not shown in Fig. 1) associated with mail server 28.

The E-mail may subsequently be retrieved by processing unit 22 on behalf of the user with another standard protocol, for example POP 3. The actual IP address utilized by the user's processing unit is immaterial to the retrieval of E-mail, as the mail server 28 can, for example, be polled or queried from any point on the network.

Upon receiving the incoming E-mail signal from the first processing unit 12, the second processing unit 22 may assign or may be assigned a temporary IP address. Therefore, the delivery of the E-mail through the Internet 24 provides the second processing unit 22 with a session number as well as IP addresses of both the first processing unit 12 and the second processing unit 22.

Point-to-point communication may then be established by the processing unit 22 processing the E-mail signal to extract the <ConnectRequest> message, including the IP address of the first processing unit 12 and the session number. The second processing unit 22 may then open a socket and generate a <ConnectOK> response signal, which includes the temporary IP address of the second processing unit 22 as well as the session number of the first processing unit.

The second processing unit 22 sends the <ConnectOK> signal directly over the Internet 24 to the IP address of the first processing unit 12 without processing by the mail server 28, and a timeout timer of the second processing unit 22 may be set to wait and detect a <Call> signal expected from the first processing unit 12.

Real-time point-to-point communication of audio signals over the Internet 24, as well as video and voicemail, may thus be established and supported without requiring permanent IP addresses to be assigned to either of the users or processing units 12, 22. For the duration of the realtime point-to-point link, the relative permanence of the current IP addresses of the processing units 12, 22 is sufficient, whether the current IP addresses were permanent (i.e. predetermined or preassigned) or temporary (i.e. assigned upon initiation of the point-to-point communication).

In the exemplary embodiment, a first user operating the first processing unit 12 is not required to be notified by the first processing unit 12 that an E-mail is being generated and sent to establish the point-to-point link with the second user at the second processing unit 22. Similarly, the second user is not required to be notified by the second processing unit 22 that an E-mail has been received and/or a temporary IP address is associated with the second processing unit 22. The processing units 12, 22 may perform the disclosed point-to-point Internet protocol automatically upon initiation of the point-to-point communication command by the first user without displaying the E-mail interactions to either user. Accordingly, the disclosed point-to-point Internet protocol may be transparent to the users. Alternatively, either of the first and second users may receive, for example, a brief message of "CONNECTION IN PROGRESS" or the like on a display of the respective output device of the processing units 12, 22.

After the initiation of either the primary or the secondary point-to-point Internet protocols described above in conjunction with FIGS. 1-2, the point-to-point communication link over the Internet 24 may be established as shown in FIGS. 3-4 in a manner known in the art. For example, referring to FIG. 3, upon receiving the <ConnectOK> signal from the second processing unit 22, the first processing unit 12 extracts the IP address of the second processing unit 22 and the session number, and the session number sent from the second processing unit 22 is then checked with the session number originally sent from the first processing unit 12 in the <ConnectReq> message as E-mail. If the session numbers sent and received by the processing unit 12 match, then the first processing unit 12 sends a <Call> signal directly over the Internet 24 to the second processing unit 22; i.e. using the IP address of the second processing unit 22 provided to the first processing unit 12 in the <ConnectOK> signal.

Upon receiving the <Call> signal, the second processing unit 22 may then begin a ring sequence, for example, by indicating or annunciating to the second user that an incoming call is being received. For example, the word "CALL" may be displayed on the output device of the second processing unit 22. The second user may then activate the second processing unit 22 to receive the incoming call.

Referring to FIG. 4, after the second processing unit 22 receives the incoming call, realtime audio and/or video conversations may be conducted in a manner known in the art between the first and second users through the Internet 24, for example, by compressed digital audio signals. Each of the processing units 12, 22 also display to each respective user the words "IN USE" to indicate that the point-to-point communication link is established and audio or video signals are being transmitted.

In addition, either user may terminate the point-to-point communication link by, for example, activating a termination command, such as by activating an [END] button or icon on a respective processing unit, causing the respective processing unit to send an <End> signal which causes both processing units to terminate the respective sockets, as well as to perform other cleanup commands and functions known in the art.

FIGS. 5-6 illustrate examples of display screens 36 which may be output by a respective output device of each processing unit 12, 22 of FIGS. 1-4 for providing the disclosed point-to-point Internet protocol and system 10. Such display screens may be displayed on a display of a personal computer (PC) or a PDA in a manner known in the art.

As shown in FIG. 5, a first display screen 36 includes a status area 38 for indicating, for example, a called user by name and/or by IP address or telephone number; a current function such as C2; a current time; a current operating status such as "IN USE", and other control icons such as a down arrow icon 40 for scrolling down a list of parties on a current conference line. The operating status may include such annunciators as "IN USE," "IDLE," "BUSY," "NO ANSWER," "OFFLINE," "CALL," "DIALING," "MESSAGES," and "SPEEDDIAL."

Other areas of the display screen 36 may include activation areas or icons for actuating commands or entering data. For example, the display screen 36 may include a set of icons 42 arranged in columns and rows including digits 0-9 and commands such as END, SND, HLD, etc. For example, the END and SND commands may be initiated as described above, and the HLD icon 44 may be actuated to place a current line on hold. Such icons may also be configured to substantially simulate a telephone handset or a cellular telephone interface to facilitate ease of use, as well as to simulate function keys of a keyboard. For example, icons labeled L1-L4 may be mapped to function keys F1-F4 on standard PC keyboards, and icons C1-C3 may be mapped to perform as combinations of function keys, such as CTRL-F1, CTRL-F2, and CTRL-F3, respectively. In addition, the icons labeled L1-L4 and C1-C3 may include circular regions which may simulate lamps or light emitting diodes (LEDs) which indicate that the function or element represented by the respective icon is active or being performed.

Icons L1-L4 may represent each of 4 lines available to the caller, and icons C1-C3 may represent conference calls using at least one line to connect, for example, two or more parties in a conference call. The icons L1-L4 and C1-C3 may indicate the activity of each respective line or conference line. For example, as illustrated in FIG. 5, icons L1-L2 may have lightly shaded or colored circles, such as a green circle, indicating that each of lines 1 and 2 are in use, while icons L3-L4 may have darkly shaded or color circles, such as a red or black circle, indicating that each of lines 3 and 4 are not in use. Similarly, the lightly shaded circle of the icon labeled C2 indicates that the function corresponding to C2 is active, as additionally indicated in the status are 38, while darkly shaded circles of icons labeled C1 and C3 indicate that such corresponding functions are not active.

The icons 42 are used in conjunction with the status area 38. For example, using a mouse for input, a line that is in use, as indicated by the lightly colored circle of the icon, may be activated to indicate a party's name by clicking a right mouse button for 5 seconds until another mouse click is actuated or the [ESC] key or icon is actuated. Thus, the user may switch between multiple calls in progress on respective lines.

Using the icons as well as an input device such as a mouse, a user may enter the name or alias or IP address, if known, of a party to be called by either manually entering the name, by using the speeddial feature, or by double clicking on an entry in a directory stored in the memory, such as the memory 16 of the first processing unit 12, where the directory entries may be scrolled using the status area 38 and the down arrow icon 40.

Once a called party is listed in the status area 38 as being active on a line, the user may transfer the called party to another line or a conference line by clicking and dragging the status area 38, which is represented by a reduced icon 46. Dragging the reduced icon 46 to any one of line icons L1-L4 transfers the called party in use to the selected line, and dragging the reduced icon 46 to any one of conference line icons C1-C3 adds the called party to the selected conference call.

Other features may be supported, such as icons 48-52, where icon 48 corresponds to, for example, an ALT-X command to exit the communication facility of a processing unit, and icon 50 corresponds to, for example, an ALT-M command to minimize or maximize the display screen 36 by the output device of the processing unit. Icon 52 corresponds to an OPEN command, which may, for example, correspond to pressing the O key on a keyboard, to expand or contract the display screen 36 to represent the opening and closing of a cellular telephone. An "opened" configuration is shown in FIG. 5, and a "closed" configuration is shown in FIG. 6. In the "opened" configuration, additional features such as output volume (VOL) controls, input microphone (MIC) controls, waveform (WAV) sound controls, etc.

The use of display screens such as those shown in FIGS. 5-6 provided flexibility in implementing various features available to the user. It is to be understood that additional features such as those known in the art may be supported by the processing units 12, 22.

Alternatively, it is to be understood that one skilled in the art may implement the processing units 12, 22 to have the features of the display screens in FIGS. 5-6 in hardware; i.e. a wired telephone or wireless cellular telephone may include various keys, LEDs, liquid crystal displays (LCDs), and touchscreen actuators corresponding to the icons and features shown in FIGS. 5-6. In addition, a PC may have the keys of a keyboard and mouse mapped to the icons and features shown in FIGS. 5-6.

Referring to FIG. 7, the disclosed point-to-point Internet protocol and system 10 is illustrated. First processing unit 12 initiates the point-to-point Internet protocol in step 56 by sending a query from the first processing unit 12 to the connection server 26. If connection server 26 is operative to perform the point-to-point Internet protocol, in step

58, first processing unit 12 receives an on-line status signal from the connection server 26, such signal may include the IP address of the callee or a "Callee Off-Line" message. Next, first processing unit 12 performs the primary point-to-point Internet protocol in step 60, which may include receiving, at the first processing unit 12, the IP address of the callee if the callee is active and on-line. Alternatively, processing unit 60 may initiate and perform the secondary point-to-point Internet protocol in step 62, if connection server 26 is not operable.

Referring to FIG. 8, in conjunction with FIGS. 1 and 3-4, the disclosed point-to-point Internet protocol and system 10 are illustrated. Connection server 26 starts the primary point-to-point Internet protocol, in step 64, and timestamps and stores E-mail and IP addresses of logged-in users and processing units in the database 34 in step 66. Connection server 26 receives a query from a first processing unit 12 in step 68 to determine whether a second user or second processing unit 22 is logged-in to the Internet 24, with the second user being specified, for example, by an E-mail address. Connection server 26 retrieves the IP address of the specified user from the database 34 in step 70, if the specified user is logged-in to the Internet, and sends the retrieved IP address to the first processing unit 12 in step 72 to enable first processing unit 12 to establish point-to-point communications with the specified second user.

The disclosed secondary point-to-point Internet protocol operates as shown in FIG. 9. First processing unit 12 generates an E-mail signal, including a session number and a first IP address corresponding to a first processing unit in step 76. First processing unit 12 transmits the E-mail signal as a <ConnectRequest> signal to the Internet 24 in step 78. The E-mail signal is delivered through the Internet 24 using a mail server 28 to the second processing unit 22 in step 80. Second processing unit 22 extracts the session number and the first IP address from the E-mail signal in step 82 and transmits or sends the session number and a second IP address corresponding to the second processing unit 22, back to the first processing unit 12 through the Internet 24, in step 84. First processing unit 12 verifies the session number received from the second processing unit 22 in step 86, and establishes a point-to-point Internet communication link between the first processing unit 12 and second processing unit 22 using the first and second IP addresses in step 88.

The primary and secondary point-to-point Internet protocols previously described enable users to establish real-time direct communication links over the Internet or other computer networks without the need for any interaction with connection server 26, the connection server providing only directory and information related services.

Fig. 10 illustrates an exemplary computer network 1000 over which the invention may operate. A first processing unit 1012 is coupled to a computer network, illustrated here as the Internet 1010, through an Internet service provider 1014. Similarly, a second processing unit 1022 is coupled to Internet 1010 through Internet service provider 1018. The inventive directory server 1020 is similarly coupled to Internet 1010 through Internet service provider 1026. Directory server 1020 further comprises a connection server 1022 and information server 1024, as will be explained hereinafter. The first processing unit 1012, second processing unit 1022 and directory server 1020 are operatively coupled to each other via the Internet 1010. It will be obvious to those reasonably skilled in the art that network 1000 is not restricted to implementation over the Internet 1010 but may comprise other network configurations such as a local area network (LAN), a wide area network (WAN), a global area network or any number of private networks currently referred to as an Intranet. Such networks may be implemented with any number of hardware and software components, transmission media and network protocols.

Exemplary Computer Architecture

Fig.11 illustrates the system architecture for a computer system 1100 such as an IBM PS/2®, suitable for implementing first and second processing units 1012 and 1022, respectively, of Fig. 10, as well as global server 1020. The exemplary computer system of Fig.11 is for descriptive purposes only. Although the description may refer to terms commonly used in describing particular computer systems, such as in IBM PS/2 computer, the description and concepts equally apply to other computer systems ranging from personal digital assistants (PDAs) to workstations to mainframe systems.

Computer system 1100 includes a central processing unit (CPU) 1105, which may be implemented with a conventional microprocessor. System 1100 further includes a random access memory (RAM) 1110 for temporary storage of information, and a read only memory (ROM) 1115 for permanent storage of information. A memory controller 1120 is provided for controlling RAM 1110. A bus 1130 interconnects the components of computer system 1100. A bus controller 1125 is provided for controlling bus 1130. An interrupt controller 1135 is used for receiving and processing various interrupt signals from the system components.

Mass storage may be provided by diskette 1142, CD ROM 1147, or hard drive 1152. Data and software may be exchanged with computer system 1100 via removable media such as diskette 1142 and CD ROM 1147. Diskette 1142 is insertable into diskette drive 1141 which is, in turn, connected to bus 1130 by a controller 1140. Similarly, CD ROM 1147 is insertable into CD ROM drive 1146 which is, in turn, connected to bus 1130 by controller 1145. Hard disk 1152 is part of a fixed disk drive 1151 which is connected to bus 1130 by controller 1150.

User input to computer system 100 may be provided by a number of devices. For example, a keyboard 1156 and mouse 1157 are connected to bus 1130 by controller 1155. An audio transducer 1196, which may act as both a microphone and a speaker, is connected to bus 1130 by audio controller 1197, as illustrated. It will be obvious to those reasonably skilled in the art that other input devices, such as a pen and/or tablet may be connected to bus 1130 with an appropriate controller and software, as required. DMA controller 1160 is provided for performing direct memory access to RAM 1110. A visual display is generated by video controller 1165 which controls video display 1170. Computer system 1100 also includes a communications adaptor 1190 which allows the system to be interconnected to a network such as a local area network (LAN), a wide area network (WAN), or the Internet , schematically illustrated by transmission medium 1191 and network 1195.

In the illustrative embodiment, computer system 1100 may include an Intel microprocessor such as the 80486DX-33 MHz, or faster, a 14.4 Kb communication modem or faster, and a sound card, as further described with reference to Fig. 12.

Operation of computer system 1100 is generally controlled and coordinated by operating system software, such as the OS/2® operating system, available from International Business Machines Corporation, Boca Raton, FL, or Windows® DOS-based operating system available from Microsoft Corp., Redmond, WA. The operating system controls allocation of system resources and performs tasks such as process scheduling, memory management, networking, and I/O services, among other things.

Fig. 12 illustrates schematically an audio sound card 1200 which may be used to implement audio controller 1197 of Fig. 11. Specifically, sound card 1200 may comprise, in the exemplary embodiment, an analog-to-digital (A/D) converter 1212, an input buffer 1216, a digital signal processor (DSP) 1222, ROM 1224, RAM 1226, an output buffer 1220, and an analog-to-digital (D/A) converter 1218, all of which may be interconnected over a bus 1210. Bus 1210 is in turn coupled to a bus interface 1228 which, in turn, is coupled to bus controller 1125 of computer system 1100 of Fig. 11.

As illustrated in Fig. 12, A/D converter 1212 is coupled to audio transducer 1214 which is typically a microphone. Conversely, D/A converter 1218 is coupled to audio transducer 1230, typically a speaker. It will be obvious to those reasonably skilled in the art that audio transducers 1214 and 1230, may be combined into a single element which serves as both a transmitter and receiver of audio signal.

In operation, A/D converter 1212 samples the audio signals supplied to it by transducer 1214 and stores the digital samples in buffer 1216. The digital sampling occurs under control of a program typically stored in ROM 1224, or, alternatively, under the control of digital signal processor 1222. The digital samples stored in input buffer 1216 are forwarded periodically, typically when the buffer reaches near capacity, over bus 1210 to bus 1130 of Fig. 11, for further processing by computer system 1100. The device driver for audio sound card 1200 generates system interrupts which will cause the digital samples stored in input buffer 1216 to be retrieved for processing. In the exemplary embodiment, the digital samples are uncompressed as supplied to computer system 1100. However, compression of the digital samples may occur using DSP 1222 executing an appropriate compression algorithm, if desired.

Digital audio samples from computer system 1100 are also be converted to analog signals by sound card 1200. The digital samples are supplied to bus 1210 and temporarily stored into output buffer 1220. The digital samples are then converted by D/A converter 1218 into an analog signals which are then supplied to audio transducer 1230, i.e., a speaker, or to further amplification and processing devices.

Sound card 1200 contemplated for use with the present invention may be implemented with any number of Windows compliant sound cards, such as the Sound Blaster sound card, commercially available from Creative Technologies Ltd., Singapore. Such Window compliant sound cards have a Windows compliant software interface allowing a standardized mechanism for software programs to operate the sound card device, such as ~~Winsoc~~ Winsock 1.1.

WebPhone Application

In the exemplary embodiment of the present invention, each of first processing unit 1012 and second processing unit 1022 of Fig. 10 are executing a software application capable of enabling point-to-point communication over network 1000, such as an Internet telephone application. One such application suitable for use with the present invention is the WebPhone Version 1.0 or higher, software, hereafter referred as the "WebPhone," commercially available from NetSpeak Corporation, Boca Raton, FL. A description of the architecture and operation of the WebPhone is provided herein with reference to Figs. 5-6, 13A-B and 14. An extensive detailed description of the architecture, application program interface, graphic user interface, and operation of the WebPhone can be found in copending U.S. patent application serial number 08/719,554 ~~XX/XXX,~~ ~~XXX~~ entitled "Point-to-Point Computer Network Communication Utility Utilizing Dynamically Assigned Internet Protocol Addresses" by Mattaway et al. filed on an even date herewith and commonly assigned, the complete subject matter of which is incorporated herein by reference.

Referring to Figs. 13A-B, schematic block diagrams of the WebPhone architecture are illustrated. The WebPhone is an end-user software application which enables users to send real-time audio data to other WebPhone users over the Internet or any public or private TCP/IP based computer networks. The WebPhone application and architecture may be designed to run on any number of operating systems or computer architectures. In the illustrative embodiment, the WebPhone application is implemented as a Windows compatible application executable on an IBM PC architecture or a clone thereof.

Referring to Fig. 13A, the WebPhone 1300 comprises a set of object modules, written in a programming language such as C++, which work together in a concerted fashion to provide real-time, multitasking, network-based media transmission and reception. WebPhone 1300 comprises a graphic user interface (GUI) 1310, a user interface (UI) 1312, an event manager 1314, a media engine 1316, a database dynamic link library 1318, one or more audio compression/decompression (codecs) 1320, an audio manager 1324, a WebPhone application program interface (API) 1326, and a network interface 1322.

WebPhone GUI 1310 comprises the visual objects seen on a computer display by the user, as illustrated by the screen capture of Fig. 14 discussed hereinafter. WebPhone GUI 1310 serves only to display the artwork associated with the underlying objects of WebPhone UI 1312. WebPhone GUI 1310 may be implemented in a modular fashion distinct from the WebPhone UI for rapid portability. In this manner, other graphic user interface environments such as those compatible with the MacIntosh, X-Windows or OS/2 operating systems, may be substituted via the Plug and Play protocol, as would be understood by those reasonably skilled in the arts.

The WebPhone UI 1312 objects maintain the state of the WebPhone GUI and provide feedback to the WebPhone GUI objects from events originating from either the user or the event manager 1314. When WebPhone changes a state that requires user notification, WebPhone UI objects notify associated WebPhone GUI objects to display the appropriate art work to the user. WebPhone UI objects also interface with the database dynamic link library 1318 to maintain the WebPhone database information, e.g. configuration information, phone directory information, etc.

The WebPhone event manager 1314 processes all the events originating from the user, via WebPhone UI 1312, the media engine 1316, and WebPhone API 1326. Event manager 1314 may be implemented as a table-driven state machine that processes the above-identified events and performs the functions necessary to bring the WebPhone from one state to another. For example, event manager 1314 interacts with media engine 1316 to create, control and remove concurrently executing jobs managed by media engine 1316. Event manager 1314 also interfaces with the WebPhone API 1326 to provide communications with other WebPhones and connection servers, as described in more detail hereinafter. WebPhone database 1318 is a dynamic link library of tree-based subroutines that provide fast database access to the WebPhone configuration information, personal phone directory, etc.

WebPhone media engine 1316 manages the allocation of associated resources to provide a multitasking environment and controls the flow of real-time data streams, e.g., conversations, outgoing messages, etc., and non-real-time data streams, e.g., voice mail, graphic images, files, etc., to and from a user network connection. The objects representing tasks are created by event manager 1314, thereby freeing media engine 1316 to manage resource routing. Specifically, the media engine routes data streams from sources such as a microphone, file or network socket, to destinations such as speaker, destination file or other network socket. To perform such routing functions the media engine interfaces with the WebPhone API 1326 to control communication with other processes, and further communicates with audio manager 1324 to communicate with the system input/output apparatus, such as sound card 1200 of Fig. 12. Media engine 1314 may be designed to employ heuristic methods to sense and efficiently utilize available bandwidth to achieve timely and accurate delivery of all data streams, both real-time and non-real-time.

Media engine 1316 further interacts with WebPhone codec 1320 to achieve compression and decompression of audio data streams. Codec 1320 provides coding of digital samples from the sound card 1200 of Fig. 12 into a compressed format more suitable for transmission over a computer network. Codec 1320 further provides decoding of a compressed signal prior to its submission to sound card 1200 for subsequent conversion to an audible analog signal. In the exemplary embodiment, WebPhone codec 1320 is implemented in a modular fashion so that codecs may be replaced and updated with newer, more efficient compression/decompression algorithms via the Plug and Play protocol. A codec suitable for use with the present invention is the True Speech codec, version 8.5, commercially available from the DSP Group, Inc., Santa Clara, California. The True Speech codec is an enhanced linear predicative coding algorithm, specifically designed to efficiently encode and decode human speech data. The True Speech codec samples the digital sample stream from sound card 1200, and, using a look-up table-based algorithm, tries to predict the value of the next data sample in the digital data stream based on the history of prior data sample values. The compressed data stream comprises a combination of identifiers of the predicted sample values, as well as error values used to correct the predictive values. Accordingly, the amount of digital data actually transmitted to represent the audio signal is significantly reduced in comparison to transmission of the actual data samples generated by sound card 1200. The True Speech codec provides temporal, frequency domain compression of the digital data representing the audio signal.

Audio manager 1324 handles communication with the audio sound card 1200 and presents a common interface to media engine 1314. Audio manager 1324 interfaces with sound card 1200 through one or more application program interfaces. In the illustrative embodiment, audio manager 1324 utilizes low-level Microsoft Windows wave input/output routines to interface with MCI compliant sound cards. As with codecs 1320, audio manager 1324 may be implemented to adhere to the Plug and Play protocol so other compliant audio sound cards or circuits, such as those for the Apple MacIntosh, commercially available from Apple Computer Company, Cupertino, California, or a Unix compatible sound card or circuit may interact with the audio manager 1324.

The WebPhone API 1326 enables the WebPhone to communicate with other WebPhones, connection and directory assistance servers, Internet gateway servers, credit processing servers, database access servers and other client processes implementing the WebPhone API. As illustrated in Fig. 13B, the WebPhone API utilizes sockets, i.e., a file handle or address indicating where data is to be sent, allowing WebPhone API enabled processes to reside on the same computer, on a local area network, on a wide area network, or over the Internet. A process 1328 communicates with the WebPhone API 1326 through a plurality of sockets 1322. The sockets 1322 are accessible by network 1330 through a number of protocols including Internet Protocol (IP) 1332, Transmission Control Protocol (TCP) 1334, Real-Time Protocol (RTP) 1336 and User Datagram Protocol (UDP) 1338. The WebPhone API provides remote command control of WebPhones and servers via the TCP. WebPhone API 1326 transfers real-time and streamed audio via the UDP protocol and real-time audio and video data via the UDP and RTP protocols. The WebPhone API utilizes TCP to transfer data of different types, i.e., file, image, graphics, etc. as well as to transfer streamline video and other multimedia data types, such as Java developed by Sun MicroSystems, Mountain View, CA. In addition, the WebPhone API provides user definable commands and data types.

Fig. 14 illustrates the graphic display produced upon invoking the WebPhone application. Display 1400 is an alternative embodiment to that illustrated in Figs. 5-6 with similar graphic elements, icons and display areas functioning as previously described with reference to Figs. 5-6.

<u>WebPhone Global Server</u>

Having described the architecture of the WebPhone software which enables the first and second processing units to establish point-to-point communication over a network, a discussion of the global connection/information server is appropriate.

Referring to Fig. 15A, a network diagram, similar to that shown in Fig. 10, is illustrated, including a schematic diagram of the global server 1500 and the various devices operatively coupling server 1500 to the Internet 1530. A first processing unit executing the WebPhone application, hereafter referred to as WebPhone 1536, is coupled to Internet 1530 through an Internet service provider 1532. Similarly, a second processing unit executing the WebPhone application, referred to as WebPhone 1538, is coupled to the Internet 1530 by an Internet service provider 1534. Global server 1500 is coupled to Internet 1530 by an Internet service provider 1528, a CSU/DSU 1526, a router 1524, and a fire wall server 1522. In the illustrative embodiment, fire wall server 1522 and global server 1500 are connected through a local area network 1520. Network 1520 may be implemented with an Ethernet or other suitable transport for TCP/IP communications. However, as will be obvious to those recently skilled in the arts, server 1500 may be connected directly to fire wall server 1522.

In the illustrative embodiment, firewall server 1522 is a single firewall mechanism which protects unauthorized access from network 1530 into global server 1500. Firewall server 1522 may be implemented on a work station, such as a SPARC 5 or SPARC 20 server from Sun MicroSystems, executing a commercially available firewall software application such as Raptor, available from Raptor Systems. Essentially, the firewall server prevents unauthorized access into global server 1500 and thereby prevents destruction of any of the information contained therein by checking the source of requests for information to global server 1500.

Router 1524 translates logical addresses among networked topologies and may be implemented with any number of commercial router devices such as the CISCO model 2501 router executing CISCO 11.0 software, both commercially available from CISCO Systems, Inc., San Jose, CA.

CSU/DSU 1526 (Channel Send Unit/Data Send Unit) functions as a sophisticated modem, converting network data to high speed serial data for transfer over a T1 or T3 line. Such high speed data is connected to another CSU/DSU, typically at the telephone company over the T1 or T3 line. An apparatus suitable for use in implementing CSU/DSU 1526 in the present invention is the AT&T Paradigm by AT&T Laboratories, Murray Hill, NJ.

Fig. 15A further illustrates a logical schematic of global server 1500. The server comprises a hardware platform 1508 on which an operating system 1510 executes. In the illustrative embodiment, hardware platform 1508 may comprise any number of commercially available high end work stations such as a DEC Alpha 4100 System, commercially available from Digital Equipment Corporation, Maynard, MA, or a SPARC 5 or a SPARC 20, both commercially available from Sun Micro Systems, Mountain View, CA. Operating system 1510, in the illustrative embodiment, may comprise the Unix, commercially available from Novell, Windows NT, commercially available from Microsoft Corporation, or Solaris, commercially available from Sun MicroSystems, Inc. Executing on operating system 1510 are a number of processes including connection server 1512, information server 1514, database server 1518 and database 1516.

Connection Server

Connection server 1512 provides a directory information service to WebPhone client processes currently on-line with respect to the computer network. Connection server 1512 behaves like a virtual machine within global server 1500 and interacts with database 1516 through database server 1518 and with network interface card 1540 through the WebPhone API. The basic function of connection server 1512 is to provide a one-to-one mapping between an identifier of a WebPhone client process, such as a

E-mail address, and the current IP address, dynamic or fixed, associated with that WebPhone client process.

As described in further detail hereinafter, when a WebPhone client transmits a <CONNECT REQ> packet to global server 1500, an E-mail address such as "Shane@netspeak.com" is provided to connection server 1512. Connection server 1512 then compares the E-mail address with the values of the records contained in on-line table 1516B and, if a match occurs with one of the records contained therein, transmits the value of the Internet Protocol address associated with that record to the requesting WebPhone client, i.e., a one-to-one matching between E-mail addresses and Internet Protocol addresses.

Referring to Fig. 16A, a flow chart illustrating the basic process steps used by connection server 1512 to implement a one-to-one mapping of E-mail addresses to Internet Protocol addresses in accordance with the present invention is illustrated. The coding of the process steps of the flowchart of Fig. 16A into instructions suitable to control global server 1500 will be understandable by those having ordinary skill in the art of programming. Connection server 1512 remains in an idle state until a <CONNECT REQ> packet is transmitted from a WebPhone client to global server 1500, as illustrated by decisional block 1610 of Fig. 16A. Upon receipt of the packet, connection server 1512 extracts the E-mail address from the packet and supplies the E-mail address to database server 1518 which them communicates using the ODBC standard with database 1516 to perform a search of On-line Table 1516B, as illustrated by process blocks 1612 and 1614. Database 1516 performs a search of on-line Table 1516B and supplies the current Internet Protocol address of the WebPhone client associated with the E-mail address to connection server 1512, via database server 1518. If a corresponding Internet Protocol address is found for the E-mail address contained in the query, connection server 1512 supplies the Internet protocol address to the requesting WebPhone client by transmitting a <CONNECT ACK> packet, as illustrated by decisional block 1616 and process block 1618. If, however, there is no Internet Protocol address associated with the queried E-mail address or the WebPhone client is off line, connection server 1512 will send an <OFFLINE> packet to the WebPhone client, as illustrated by process block 1622. Connection server 1512 will return to an idle state to await the receipt of another <CONNECT REQ> packet, as illustrated by Fig. 16A. A description of the above described packets as well as a diagram illustrating the packet transfer sequence between a WebPhone client and global server 1500 can be found with reference to Tabes 7-8 and Fig. 17A, respectively.

Information Server

Information server 1514 provides an interface between requests from WebPhone client processes and database 1516. Information server 1514 includes code written to extract the search criteria from an <INFO REQ> packet and supply the search criteria to the database search engine of database 1516 using the ODBC standard. In particular, referring to Fig. 16B, a flow chart illustrating the basic process steps used by information server 1514 in performing information/directory service functions in accordance with the present invention is illustrated. The coding of the process steps of the flow chart into instructions suitable for execution by global server 1500 will be understood by those having ordinary skill in the art of programming. Information server 1514 remains idle until an <INFO REQ> packet is received from a WebPhone client process, as illustrated by decisional step 1630. Next, information server 1514 extracts the data elements defined within the <INFO REQ> packet and supplies them to database server 1518 which, in turn, forward them to database 1516, as represented by the process step 1634 and 1636. The search engine contained within database 1516 performs the search and supplies to information server 1514 all client records meeting the search criteria specified in the <INFO REQ> packet, or a message indicating that no records were found. Next, information server 1514 transmits a <INFO ACK> packet to the WebPhone client process indicating the number of records satisfying the search criteria, as indicated by process step 1638. The WebPhone client may wish to receive all records satisfying the search criteria, or, if the number is excessively large, may desire to further refine the search by transmitting a <INFO ABORT> packet to information server 1514 and defining new search parameters to be sent with a subsequent <INFO REQ> packet. If a <INFO ABORT> packet is received by information server 1514, the process will return to an idle state, as illustrated by decisional block 1640. If no <INFO ABORT> packet was received, information server 1514 will transmit one or more <INFO> packets to the requesting WebPhone client until all records have been received by the WebPhone client, as illustrated by process step 1642. Information server 1514 will return to an idle state awaiting another <INFO REQ> packet, as illustrated in Fig. 16B. A description of the packets comprising the WebPhone protocol is illustrated in Tables 7-8 and a diagram illustrating the packet transfer sequence defined in Fig. 17A-B.

Network interface card 1540 interfaces with connection server 1512, information 1514, and database server 1518 using the WebPhone API definition, as described herein, and the Windows Sockets 1.1 Protocol, or, in a Unix-based operating system, Berkeley Sockets Network API. Network interface card 1514 may comprise, in illustrative embodiment, an Ethernet card capable of transmitting data at rates of 100 Mbps or greater, such cards being commercially available through a number of different vendors.

The connection from CSU/DSU 1526 to ISP 1528 may comprise a T1 connection, i.e., a long-distance, digital, point-to-point communication circuit capable of transmitting a signal at 1.544 Mbps with 24 channels at 64 Kbps. Alternatively, a T3 connection may be used, i.e., a connection is similar to a T1 connection except it is capable of transmitting at 44.746 Mbps per second with up to 28 T1 channels. Other connections may be suitable, depending on specific requirements and availability.

Database

Database 1516 of global server 1500 may be implemented with any of a number of commercially available structured query language (SQL) database engines, such as Oracle 7.x, Informix, or Microsoft SQL server 6.x. The SQL database resides on a RAID 1 and RAID 5 mirrored disk array. As will be explained hereinafter, database 1516 interacts with control server 1512 and information server 1514 through database server 1518. In the illustrative embodiment, database 1516 comprises a Client table 1516A, an On-line table 1516B, a WebBoard table 1516C, a WebBoard configuration table 1516D and a WebBoard Source table 1516E.

Client table 1516A comprises a plurality of records, each of which may have the fields and corresponding data elements as described in Table 1. Each WebPhone user, hereinafter "client," has a separate record in table 1516A containing the information defining the client's profile of personal information. In Table 1, the "activated," "paid," and "published" fields are boolean yes/no fields. The "id" field comprises a unique ID sequence identifying a particular WebPhone client. The "activation date," "address change date," and "access date" fields are time references measured in seconds since 00:00 Coordinated Universal Time (UTC), January 1, 1970. The "IPAddr" field represents the Internet protocol address of the WebPhone client and, if unknown, has a default value of 0.0.0.0. The database record containing a WebPhone client's profile, is defined upon first logging-on to global server 1500 and may be updated each time a WebPhone user's profile changes, as explained hereinafter.

The On-line table 1516B provides a dynamic list of those clients from 1516A who are currently On-line, as well as their current Internet protocol address. On-line Table 1516B comprises a plurality of records each of which may have the fields and data types illustrated in Table 2. The record entries of On-line table 1516B are used by connection server 1512 and information server 1514, as explained hereinafter, to provide a directory of those WebPhone client processes currently having on-line status with respect to the computer network.

The WebBoard™ is a virtual multimedia billboard which is transmitted as a series of multimedia data files to WebPhone client processes while the WebPhone application is activated. An extensive description of the WebBoard utility and its operation can be found in copending U.S. patent application serial number 08/719,891 ~~XX/XXX,XXX~~ entitled Method and Apparatus for Distribution of Multimedia Data Over a Computer Network by Mattaway et al., commonly assigned, the subject matter of which is incorporated herein by reference.

A number of tables are associated with the WebBoard functionality including WebBoard table 1516C, a WebBoard configuration table 1516D, and a WebBoard source table 1516E. WebBoard table 1516C includes a plurality of records each describing a specific WebBoard and having the field and data types illustrated in Table 3. The "id" field of Table 3 provides a unique identification number for the WebBoard file. The "imageType" field defines the video format of the image such as JPEG,TIF, GIF, etc. The "audio" field defines the nature of the audio file, e.g. a .wav file or a MIDI file, while the "audioType" field defines the codec, if any, used to compress/decompress the audio file. The "hits" field defines the number of times the WebBoard has been selected by WebPhone clients, while the "hits profile" field defines the file name of the file identifying those WebPhone clients generating hits to the subject WebBoard.

The WebBoard configuration table 1516D may have at least one record having the fields and data types illustrated in Table 4. The count field represents the number of WebBoard records currently in the table 1516C.

The WebBoard source table 1516E may comprise a plurality of records each having the fields and data types defined in Table 5. The "URL" field of Table 5 defines a data link in accordance with Uniform Resource Locator protocol to the home page or Web site of the source. In the illustrative embodiment, any entity, including vendors, advertisers, individuals or groups wishing to post information or having a Web site or home page may have a WebBoard displayable through the present invention.

Database Server

Database server 1518 serves as the interface between database 1516 and connection server 1512 and information server 1514. Specifically, connection server 1512 and information server 1514 communicate with database engine 1518 through application program interfaces embedded in the code implementation of both the connection server and the information server. Database server 1518 communicates with database 1516, in the illustrative embodiment, using the open database connectivity (ODBC) standard, developed by Microsoft Corporation, Redmond, WA. Database server 1518 functions to supply structured database queries to database 1516 and to supply the results therefrom to connection server 1514 and information server 1512. In the illustrative embodiment, database server 1518 may be implemented as a "virtual machine" executing on global server 1500, or, alternatively, may be implemented on a separate computer system such as a DEC Alpha 4100 Workstation executing DEC Unix operating system, both available from Digital Equipment Corporation, Maynard, MA. Database server 1518 communicates with network interface card 1518 using the WebPhone Application Program Interface described herein.

Global Server Network

In the illustrative embodiment, global server 1500 is implemented as a single server apparatus on which a plurality of "virtual machines" execute simultaneously. However, it will be obvious to those reasonably skilled in the art that a plurality of separate servers, one dedicated to each of connection server 1512, information server 1514, and database server 1518 may be interconnected to database 1516 and to each other using a local area network, to form a composite "virtual" global server, as illustrated by Fig. 15B, the construction of the system illustrated in Fig. 15B being within the knowledge of those reasonably skilled in the art in light of the descriptions contained herein.

It is further contemplated within the present invention that more than one global server 1500 may be utilized, as illustrated by Fig. 15C. In this implementation, multiple global servers 1500A-D are maintained for fault tolerant load sharing, each one performing the above-described connection server, information server and database server processes. Each of global servers 1500A-D are connected to the Internet via a separate T1 or T3 connection to different Internet service providers, and are synchronized with each other via database server replication. In such an embodiment, multiple global servers may be located in close proximity or in geographically disparate locations. In such an embodiment, the WebPhone application is provided with the network address information of each global server 1500A-D. In the event that any one of the global servers initially contacted is nonresponsive the WebPhone application will attempt connection to one or more of the remaining global servers to obtain directory and information services.

Further, in an implementation with multiple global servers, if the initially contacted global server is unable to accommodate a WebPhone client request, or, is not geographically convenient, the global server can provide the network address of another global server capable of servicing the WebPhone client's request or which is logically more convenient. This process may occur during the initial log-in of the WebPhone client process, as described with references to messages 1-5 of Fig. 17A.

As previously described, if none of the global servers are available, the WebPhone application can rely on the secondary Internet Protocol technique in which a WebPhone client process sends its current dynamically assigned Internet Protocol address to a prospective WebPhone callee through an E-mail message, as described herein.

WebPhone Protocol

Prior to describing the interaction of the connection server 1512 and information server 1514 with WebPhone client processes, a description of the WebPhone protocol by which the WebPhone client processes and the global server 1500 communicate is appropriate. Tables 6-7 below illustrate the packet definitions of the packets comprising the WebPhone protocol (WPP) including the packet type, the direction and the data elements comprising each packet. In Tables 6-7 the symbol "→" indicates a packet transmitted by a WebPhone client process, while the "←" symbol indicates a packet transmitted by the global server. Tables 8-9 define the data elements described in Tables 6-7. In Tables 6-9, the terms "ULONG" and "UNSIGNED LONG" designate an unsigned long integer value, i.e., 32-bit integer value. Similarly, the terms "USHORT" and "UNSIGNED SHORT" designate an unsigned short integer value, i.e., 16-bit integer value. The term "CHAR" designates a single character, typically assuming a binary value of either 1 or 0. The term "VARCHAR(X)", where X is an integer, value symbolizes a variable length character string, with the number of characters indicated with the integer value. The term "UNSIGNED CHAR" designates an 8-bit character code, i.e., no sign bit. Finally, the term "variable" indicates a variable length data field.

Figure 17A illustrates a schematic block diagram of a packet transfer sequence between a pair of WebPhone client processes and the global server, in accordance with the present invention. Each WebPhone application, also referred to as a WebPhone client process, connects to global server 1500 upon start up to inform global server 1500 that the WebPhone client process is on-line and available to make and/or receive calls. Specifically, as illustrated in Fig. 17A, WebPhone 1536 opens a socket to the global server 1500 and transmits an <ONLINE REQ> packet from WebPhone 1536 to Global server 1500, as illustrated by message 1 and Fig. 17A. The <ON LINE REQ> packet may have the format and data illustrated in Table 6, and additional Feature bits which define the functionality of the WebPhone application, as explained in greater detail hereinafter. In response, connection server 1512 and information server 1514 of global server 1500 use the information contained in the <ONLINE REQ> packet to update the status of database 1516. In the event that the WebPhone client process is logging on for the first time, global server 1500 returns to the WebPhone 1536 a <USER INFO REQ> packet, as illustrated by message 2 of Fig. 17A. The <USER INFO REQ> packet includes the elements as defined in Table 9. In response, WebPhone 1536 returns a <USER INFO> packet as illustrated by message 3 of Fig. 17A. The <USER INFO> packet contains the data elements defined in Table 8. Connection server 1512 and information server 1514 of global server 1500 utilize the data in the <USER INFO> packet to update database 1516. Specifically, information server 1514 utilizes such data to create a record in client table 1516A representing WebPhone 1536. Next, global server 1500 transmits to WebPhone 1536 a <REGISTRATION> packet, as illustrated by message 4 of Figs. 17A. The

<REGISTRATION> packet contains the data described in Table 7 plus Feature bits, as described hereinafter. The <REGISTRATION> packet returned to WebPhone 1536 enables certain functions within the WebPhone architecture based on predetermined criteria, for example, whether the user has paid for the product, or which version of the product the user possesses. Following the <REGISTRATION> packet, global server 1500 further transmits an <ONLINE ACK> packet, as illustrated by message 5 of Fig. 17A. Prior to transmission of the <ONLINE ACK> packet, connection server 1514 updates database 1516, specifically On-line table 1516B to indicate that WebPhone 1536 is on-line with respect to the computer network. Upon receiving the <ON-LINE ACK> packet, WebPhone 1536 closes the socket to global server 1500.

In the event WebPhone 1536 had previously registered with global server 1500, only messages 1 and 5 are required to establish WebPhone 1536 as being on-line. If WebPhone 1536 had new user information to supply to global server 1500, then packet sequence illustrated by messages 3 and 4 would occur.

Although the packet sequence illustrated by messages 1-5 is described with reference to WebPhone 1536, WebPhone 1538 interacts in a similar manner with global server 1500 to establish on-line status. No further interaction occurs between the respective WebPhone client processes and the global server unless the WebPhones require directory or search assistance about a prospective callee.

In one calling scenario, a WebPhone user knows the E-mail address of another WebPhone user to which he/she wishes to establish a point-to-point communication, however, the current dynamically assigned Internet protocol address of the callee is unknown to the caller. In this scenario, the user of WebPhone 1536 requests assistance from global server 1500 to obtain the current dynamically assigned Internet Protocol address of the prospective callee WebPhone. First, the user of WebPhone 1536 specifies the callee by entering all or part of the callee party's name or alias in the party name field area of the graphic user interface. If the party is not in the WebPhone user's local directory, the IP address or E-mail address of the callee WebPhone may be entered into the number field area of the graphic user interface, followed by activation of the send button or icon on the graphic user interface. As a result, WebPhone 1536 opens a socket to global server 1500 and transmits a <CONNECT REQ> packet having the format described in Table 6. Connection server 1512 of global server 1500 utilizes the value of the E-mail address specified in the <CONNECT REQ> packet to perform a one-to-one mapping in the on-line table 1516B to determine the current Internet Protocol address of the indicated callee, as illustrated by the flowchart of Fig. 15A. Once this mapping is performed, the server 1500 transmits to WebPhone 1536 a <CONNECT ACK> packet, as indicated by message 7A of Fig. 17A. The <CONNECT ACK> packet has the format and content as illustrated in Table 6 and includes the IP address of the callee as well as information such as an error code to indicate that no WebPhone application is associated with that callee. Alternatively, if the selected callee is off line, global server 1500 transmits to WebPhone 1536 an <OFF LINE> packet to indicate that the desired party is not on-line, as illustrated by message 7B of Fig. 17A. Following the receipt of either a <CONNECT ACK> or an <OFF LINE> packet by WebPhone 1536, the socket to global server 1500 opened by WebPhone 1536 is closed.

If the current Internet Protocol address of the callee was returned from global server 1500, the packet transmission sequence illustrated between WebPhones 1536 and 1538 of Fig. 17A transpires. Whether a calling WebPhone knows the Internet Protocol address of the callee WebPhone, as in the case of a fixed Internet Protocol address, or obtains the Internet Protocol address from global server 1500, as previously described, the calling sequence to establish a call occurs as follows. WebPhone 1536 opens a socket to WebPhone 1538. Next, WebPhone 1536 transmits to WebPhone

1538 a <CALL> packet as illustrated by message 8 of Fig. 16A. The <CALL> packet has the format illustrated in Table 6 and may, optionally, include information identifying the compression/decompression (codec) used by the caller WebPhone. In response to the <CALL> packet, WebPhone 1538 may return with a number of different packets, as illustrated by messages 9A-D. First, callee WebPhone 1538 may respond to caller WebPhone 1538 with a <REJECT> packet, as illustrated by message 9A, indicating that the callee WebPhone does not wish to be disturbed, e.g. total call blocking, or, that the callee WebPhone does not wish to talk to caller WebPhone, e.g. party specific or group specific call blocking. In the event of party or group specific call blocking, the user information contained within the <CALL> packet of message 9A is compared by the caller WebPhone application to a predefined list of WebPhone user information profiles which the callee does not wish to converse, such list having been predefined by the callee in the WebPhone user's personal directory, as explained hereinafter. Upon receiving the <REJECT> packet the caller WebPhone annunciates the result to the user and the socket to the callee WebPhone is closed.

Alternatively, callee WebPhone 1538 may return a <BUSY> packet, as illustrated by message 9B of Fig. 17A. The <BUSY> packet indicates that the callee WebPhone is currently utilizing all available lines within its WebPhone application.

A further possible response from callee WebPhone 1538 is to issue an <ANSWER MACH> packet, as illustrated by message 9C of Fig. 17A. The <ANSWER MACH> packet includes data indicating whether the machine is capable of receiving voice mail type messages, as described in greater detail in copending U.S. patent application serial number 08/719,898 ~~XX/XXX,XXX~~ entitled "Method and Apparatus for Providing Caller Identification Based Out-Going Messages in a Computer Telephony Environment," by Mattaway et al., commonly assigned and incorporated herein by reference.

The preferred response by callee WebPhone 1538 is to transmit a call acknowledge <CALL ACK> packet, as illustrated by message 9D of Fig. 17A. The <CALL ACK> packet has the data content illustrated in Table 6. Both the <CALL> and <CALL ACK> packets contain the information of the WebPhone users sending the packet. This information is useful by the recipient of the packet for a number of purposes. For example, the user information is displayed on the enunciator area of the WebPhone graphic display to identify the party placing the call. Second, the user may select such information and, using the drag and drop functionality of the WebPhone graphic user interface, add the user information to the callee WebPhone user's personal directory resident within his/her specific WebPhone application. In such a manner, both parties are completely identified to each other prior to commencing audio communications. The transmission of complete caller identification information with the <CALL> and <CALL ACK> symbols packets enables such functions as individual or group specific call blocking, party specific outgoing messages, visual caller identification, and party specific priority ringing and sound effects, as explained herein.

Following transmission of <CALL ACK> packet by callee WebPhone 1538, the callee WebPhone further transmits an <ANSWER> packet to caller WebPhone 1536, as illustrated by message 10 of Fig. 17A. Like the <BUSY> packet, the <ANSWER> packet is essentially empty, containing nothing more than a session ID number which is unique to the call. The socket previously opened by caller WebPhone 1536 over which the forgoing packets were transmitted remains open for the transmission of control information between caller WebPhone 1536 and callee WebPhone 1538. Such control information may comprise an <END> packet signaling the end of a call, a <HOLD> packet indicating that one of the parties to a call has placed the call "on hold" or other packets related to advance functionality of the WebPhone architecture. In addition, caller WebPhone 1536 opens a second socket to callee WebPhone 1538 over which the respective WebPhones may exchange <AUDIO> packets, as illustrated by messages 11A-B of Fig. 17A. The <AUDIO> packets have the data content illustrated in Table 6. The WebPhone application enables the parties to converse in real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks. If both WebPhone client processes are utilized with full duplex sound cards, such as that illustrated in Fig. 12, the WebPhone users may transmit and receive audio packets simultaneously, similar to normal telephone conversation. However, if the WebPhone client processes are used with half duplex sound cards, a WebPhone user may only transmit or receive audio data simultaneously, similar to a speaker phone. Exchange of <AUDIO> packets continues until either the callee WebPhone or the caller WebPhone transmits an <END> packet, as illustrated by message 12 of Fig. 16A. Following the receipt of an end packet, the WebPhone client process will cease to accept subsequent audio packets.

Following either transmission or receipt of an <END> packet by the caller WebPhone, the socket opened by the caller WebPhone to the callee WebPhone over which real-time audio communication occurred is closed. Similarly, the previously opened socket over which control information was transmitted between the callee and caller WebPhones is likewise closed.

Referring now Fig. 17B, if a WebPhone caller seeks to determine whether a prospective WebPhone callee is connected to the computer network, but, has little information regarding the client process, information server 1514 may be utilized as described. The WebPhone user defines One or more of the first name, last name, company, city, state, or country values of the Query field contained within the <INFO REQ> packet sends the packet to the global server. WebPhone 1536 opens a socket to global server 1500 and forwards <INFO REQ> packet to global server 1500, as illustrated by message 1 of Fig. 17B. Information server 1514 extracts the values specified the query field of the <INFO REQ> packet and queries the database 1516, as previously described with reference to Fig. 16B. Global server 1500 then transmits a <INFO ACK> packet back to WebPhone 1536, as illustrated by message 2 of Fig. 17B. The <INFO ACK> packet has the format and data elements indicated in Table 7, including the number of parties satisfying the search criteria, specified in the <INFO REQ> packet. If the user of WebPhone 1536 wishes to receive the number of parties satisfying the search criteria global server 1500 automatically transmits to WebPhone 1536 one or more <INFO> packets, as illustrated by messages 3A-C of Fig. 17B. The <INFO> packet has the format and data elements as described in Tables 6-7. At any time following transmission of the <INFO ACK> packet, WebPhone 1536 may transmit an <INFO ABORT> packet to either prevent transmission of any <INFO> packets or to stop transmission of any remaining packets, as illustrated by message 4 of Fig. 17B. The <INFO ABORT> packet has the format and data elements as described in Table 6-7.

Once the user receives the information contained within the <INFO> packets satisfying the search criteria, the user may store such information in his/her personal WebPhone directory by dragging and dropping the information from the annunciator area to the direction dialog box using the WebPhone GUI.

The methods and apparatus described herein provide computer users with a powerful protocol in which to directly establish real-time, point-to-point communications over computer networks directly without server required linking. The a directory server assists in furnishing the current dynamically assigned internet protocol address of other similarly equipped computer users or information about such users.

<u>WebPhone Graphic User Interface</u>

Referring again to Fig. 14, the WebPhone GUI 1400 consists of a main window which has the look of a modern cellular flip phone and a set of dialog boxes launched from window. Operation of the WebPhone is controlled by selecting objects, i.e., buttons, text and images, and dragging objects, i.e., lines, parties, messages, etc., as explained hereinafter.

WebPhone GUI 1400 comprises a plurality of visual objects, including display 1402, number pad 1406, line pad 1404, call function buttons 1408, phone function buttons 1410 and audio controls (not shown). Display 1402 provides a number of distinct area for presentation of entering of information useful in operation of the WebPhone application. A party name field 1402A displays the name of the caller when an incoming call arrives and may also be used for entering the name of a party, up to 25 characters. By entering the name of a party in the party name field 1402A and pressing one or more of the phone function buttons 1410, various activities may be accommodated. For example, entering the name of a party in the party name field and pressing the [SND] button causes the WebPhone to first search the personal information directory for the information profile of the party entered. If such party's information is not already resident in the personal information directory, the WebPhone will open up a directory assistance dialog allowing the user to enter information to be submitted to the information server 1514 for searching, as described previously. Further, clicking the entered party name with the right mouse button causes a dialog box to appear enabling the user to modify the current directory entry, if any, for the party entered.

Entering the IP address of a party in the party IP address field followed by the [SND] button causes initiation of a call. If the callee's name exists within the caller's personal directory, or the call is established, the callee's name will appear in a party name field for caller ID purposes.

The third line of the display 1402 serves as a status annunciator line for displaying iconic feedback about the status of events within the WebPhone. Such status icons may include icons indicating enablement of call forwarding, call blocking, do not disturb, priority ringing, file transfer occurring, voice mail transfer occurring or call camping.

The line number annunciator indicates the line, i.e., lines 1-4, currently active, as illustrated by annunciated field 1402J. A main LED 1402F indicates when a line is active by changing color. Time field 1402C displays the local time when no lines are active. When one of the lines L1-L4 are active, time field 1402C displays the callee party's time. By single clicking the time field the user can cycle through the two different time values.

The line status field 1402H displays the status of the currently selected line, illustrated in Fig. 14 as displaying "talk" status. A call duration field 1402D displays the elapsed time in minutes and seconds since the currently displayed call commenced.

The V-mail field 1402G displays the number of the new voice mail messages and the total number of voice mail messages received.

When one or more call functions such as call conferencing, call blocking, priority ringing, call camping, or call forwarding are activated, the list of those parties within the WebPhone personal directory having such functionality active for their information profile can be viewed in the party name field by selecting a list arrow (not shown) icon which appears whenever one of the previously described functions is activated. Pressing the icon arrow allows the parties to be viewed sequentially.

The number pad buttons 0-9 also serve as speeddial buttons. Right clicking on any one of the number pad buttons 0-9 causes the name, alias, e-mail address and IP address, if known, of the party assigned to that speed dial position to be displayed on display 1402.

If a user right clicks on any of lines L1-L4 the name, alias, e-mail address and IP address of the party on that line will similarly appear for a predetermined period of time and then revert back to the normal display.

The keypad buttons displayed on WebPhone GUI 1400 may assume one of two states. A button may be a momentary button which, when pressed, i.e., left clicked, gets pushed in and then pops back out again. A second type of button is a toggle button which when pressed gets pushed in and stays in until pressed again. Number pad buttons 0-9 are momentary buttons which may be used to enter the Internet Protocol address of a party and which each house a speed-dial position. The user may assign a party to one of the ten speed-dial positions by selecting the user's information displayed in display 1402 and then dragging it onto the keypad button. To speed-dial one of the ten buttons the user simply presses the appropriate number followed by the [SND] button. As stated previously, if the user right clicks on one of the number pad buttons, the information about the party assigned to the speed-dial position will be displayed.

The line pad 1404 comprises four toggle buttons L1-L4, each of which has a letter, a number and an LED indicating the status of the line. When one or more parties are associated, i.e., dragged and dropped, with a line, the letter designating the appropriate line turns from an L to C indicating a conference call. When only one party is left on the line the letter designation reverts from a C back to an L indicating a regular call. Only one line, button may be selected at a time when an incoming call arrives. Pressing any of the line buttons assigns the incoming call to the selected line. Pressing a line button, i.e., left clicking, when the line is in use places the line on hold. Subsequent depressing the line button takes the call off hold.

A number of call function buttons 1408, including the [RCL], [END], [SND], [DND], [MUT], [HLD], [CMP], [BLK], [PRI], [FWD], not all of which are shown in Fig. 14, are used to control operation of calls. The [RCL] button is a momentary button used to recall the last number dialed. Pressing [RCL] recalls the last party called by displaying the party's name, alias, e-mail address and IP address, if known. Selecting a free line following depression of the [RCL] button followed by the [SND] button will cause the party last called to be dialed. The [END] button is a momentary button and terminates a call upon depression. The [SND] button is a momentary button and is used to both place and answer calls. Depressing the [SND] button when a call is being announced causes the call to be answered on a preselected line or a line indicated by the user. Depression of the [SND] button once a callee's information is entered into display 1402 causes the party to be called, if the required information is present, or otherwise causes an information server connection to be established and activated, as previously described.

The [DND] button is a toggle button and is used to activate the Do Not Disturb function of the WebPhone. When activated, the [DND] button causes all inbound calls to be routed to the answering machine.

The [MUT] button is a toggle button which, upon depression, causes disabling of the microphone associated with a user's WebPhone system. When the [MUT] button is enabled, the main LED 1402F and the status line 1402H change to indicate that the call muted. Depression of the [MUT] button is undetected by one or more callees.

The [HLD] button is a momentary button and is used to place a call on hold. When a user depresses the [HLD] button a party or parties to a conference call are placed on hold, e.g., the microphone and speaker of the system are effectively disabled. When a called is placed on hold, the main LED 1402F and call status field 1402H indicate the change. To take a call off hold, the user depresses the line button of the call being held.

The [CMP] button is a momentary button that causes the WebPhone user to camp on a party, i.e., perpetual redial. Camping on a party serves to insure that the user's call will go through when the party is available. After placing a call, if the callee responds with either a busy or on off-line status, the user may press the [CPM] button to camp on that party. To remove a camp from a party, the user presses the delete key from the computer keyboard.

The [BLK] button is a toggle button and enables or disables call blocking. Depression of the [BLK] button enables call blocking causing all inbound calls from parties who have call blocking designated in their information profile within the personal information directory to be either rejected or routed to the answer machine. Whether a call is to be rejected or routed to the answering machine is specified in a party's information profile record within the personal information directory, in a manner, as previously described.

The [PRI] button is a toggle button which enables or disables priority ringing. Depression of the button enables priority ringing of all inbound calls from parties, i.e. generation of customized sound effects and/or graphic announcements when a call arrives. As with call blocking, priority ringing is specified within a party's information profile record in the user's personal information directory.

The [FWD] button is a toggle button which enables or disables call forwarding. Depression of the button enables call forwarding of selected inbound calls to the party specified in the appropriate information profile record in the personal information directory. The WebPhone will first search in the personal information directory for an information profile record which matches the inbound call. If a match occurs, and call forwarding is enabled, the inbound call will be forwarded to the party designated within the matched information profile record. If no party is designated, the call will be forwarded to a default forwarding party.

In addition to the call function buttons, a number of phone function buttons 1410 including a [CFG], [DIR], [MSG], [DAT], [LOG], [], and ? buttons enable users to further direct functions of a phone. Specifically, the ? button is a momentary button which invokes an interactive, multimedia tutorial and help system about the WebPhone. The [CFG] button is a momentary button, depression of which launches a configuration dialog which enables the user to change the operating parameters of the WebPhone. The [DIR] button is a momentary button, depression of which launches the phone directory dialog which enables a user to add, store, update, view, and delete parties and to obtain directory assistance from global server 1500, as described previously. The [MSG] button is likewise a momentary button, depression of which launches the voicemail message dialog which enables a user to view, sort, playback, delete, save and restore voicemail messages, as well as to create, playback, delete, save, and restore custom outgoing messages and assign them to information profile records in the personal information directory.

The [DAT] button is a momentary button, depression of which launches a data file transfer dialog enabling a user to monitor and control the progress of a data file transferred over the communication link established with the WebPhone, such dialog further enables a user to retrieve and create E-mail.

The [LOG] button is a momentary button, depression of which launches a call activity log dialog which enables a user to use, sort, search for, print, and delete call related events. An "X" icon is provided to exit the WebPhone. If one or more calls are active when the X icon is selected, a dialog box will appear asking the user if he/she really wishes to exit and terminate active calls. Other icons are provided for minimizing or iconifying the WebPhone application.

In addition to the above-described display, the WebPhone GUI 1400 includes a number of audio control buttons and sliders (not shown in Fig. 14). These graphic elements enable the user to control the recording the playback of voicemail and outgoing messages and operate similar to conventional audio tape deck controls. In the illustrative embodiment, and similar to that shown in Fig. 5, a progress bar is illustrated which displays the extent of progress during playback and audio recording processes. Momentary buttons may be provided for rewinding the "virtual tape" to the beginning and for fast forwarding the tape to the end of a recording. Further, momentary buttons are provided for aborting, as well as stopping, playback of audio. A speaker card button, implemented as a toggle button, is provided to play back audio on the sound card's speaker. A special momentary button for audio playback is provided. When initially depressed, audio playing commences. The button then pops out and becomes a pause button. Subsequent depression pauses the audio. The button then pops out again to become a play button. A record button, in the form of a toggle button is provided to control recording of audio. When the button is depressed the user is in an audio record mode and can record voicemail or outgoing messages. To stop recording, the button is pressed again or the stop is button is pressed. A slider-type graphic potentiometer is provided to control speaker volume and enables the user to adjust output volume of the audio received during conversation and playback of voicemail and outgoing messages. The speaker control will attenuate the sound card speaker volume. A similar control is provided to control microphone volume and enables the user to adjust the input volume of audio recorded during conversation and recording of voicemail and outgoing messages. The microphone slider control attenuates the sound card's microphone volume.

<u>WebPhone Application Object Implementation</u>

As previously described, with reference to Figs. 13A-B, the WebPhone application comprises a set of object modules which work together in a concerted fashion to provide real-time, multitasking, network-based media transmission and reception. Specifically, the WebPhone GUI, user interface, event manager, and media engine utilize a number of objects to house and manipulate data associated with the operation of the WebPhone application. The GUI objects control the look and feel of the graphic user interface controls which comprise the WebPhone user interface. Some user interface objects maintain and manage many of the states of the WebPhone and control the behavior of the GUI controls, as illustrated in Figs. 18A-D.

Fig. 18A illustrates the hierarchical relationship between objects within the WebPhone. The UIVirtualBase 1812 is a class from which UIVirtualControl object 1810 and UIVirtual object 1808 inherit their respective attributes and member functions. GUIControl object 1802 inherits its attributes and member functions from UIVirtualControl 1810, as illustrated. UICollection object 1806 inherits its properties from the UIVirtual object class 1808. The UIControl object inherits its attributes and member functions from both the UIVirtual control object class 1810 and the UIVirtual object class 1808.

Referring to Fig. 18B the UIControl object 1804 itself serves as a class from which the UIButton object 1828, UISlider object 1826, UIScroller object 1824, UITab object 1822, UIDisplay object 1818, UIListBox object 1820, UIComboBox 1814, and UIEditBox 1816 are subclasses. As illustrated in Fig. 18C, the UIPushButton 1842, UIPlayRun object 1844 and UIToggle object 1846, are subclasses of the UIButton object 1848. As illustrated in Fig. 18D, the UIPhone object 1838, UICall object 1832, UILine object 1834, and UIPopUp object 1836 are derived from or inherit their attributes and member functions from the UICollection object class 1806.

Each WebPhone control has two objects associated therewith, a windowing system specific GUIcontrol object 802 and a generic UI control object 1804. When the GUIcontrol object's state is changed by the user, GUIcontrol 1802 verifies the change with UIcontrol 1804 to validate the change. UIcontrol 1804 is a child of the UIcollection 1806. When UIcontrol's sibling, GUIcontrol 1802 requests UIcontrol 1804 to verify a change, and the change is accepted, GUIcontrol 1802 must verify the change with its parent object. The parent UIcollection 1806 may have its own parent, another UIcollection object, that it must verify the change with. The UIPhone object 1838 is a member of the UI collection class. UIPhone has final approval over all changes in the state of the WebPhone. UIPhone 1838 further tells child objects when the event manager changes the phone state and further creates jobs for the event manager based on user actions.

The WebPhone drag and drop functionality utilizes the standard Windows® drag and drop interface and adds several unique object types to interact therewith. Specifically, each UIcontrol and GUIcontrol object has two new member functions added, e.g., set dragtype and acceptdrop types. The set dragtype call sets the type of drag that the control will perform if the mouse or other pointing device is moved out of the control window with the left mouse button down. The accept droptype defines the types of drags the control will accept.

Event Manager and Media Engine

The event manager is a state machine consisting of an array of pointers to functions and states which make up a state-event table. When an event occurs as caused by the mouse, keyboard, mic, speaker, or socket, it is up to the user interface to determine if the event requires the attention of the event manager. The event manager is not notified of events which effect only the graphic user interface, e.g., the user depresses the [DIR] button to open the phone directory dialog.

Referring to Figs. 19A-C, a conceptual block diagram illustrating the event manager and media engine objects utilized by the WebPhone is presented.

Specifically, the following objects are utilized by both the user interface and the event manager to manager the state of calls and tasks that are to be performed:

- line
- job
- party
- task

As illustrated in Fig. 19A, a Line object is represented by the pentagon shape with a number contained therein. The Line object has the attributes of state and duration and a *job pointer. Member functions for the Line object include createcall () and removecall (). The Job object is illustrated with a rectangle having pointers extended therefrom as illustrated in Fig. 19A. Attributes of the job object include, ID, type, state, and parties, and pointer attributes party, inTask, outTask, nextJob, prevJob. The Job object has the member functions of AddParty, RemoveParty, CreateTask, and RemoveTask. The Party object, illustrated with a triangular symbol, includes the attributes of state, session, socket, and partyRec, and the member functions of LoadParty.

The Task object includes the attributes of command, source, destination, extent, fileHandle, fileType, fileLength, fileSize, mic, speaker, and flags, as wells as pointer attributes *job and *buf. The values assumable by the command attribute of the Task object may include initialize, close, start, stop, fill, and use, etc. The values assumable by the source and destination attributes of the task object may include microphone, speaker, socket, and file. Fig. 19B illustrates the relationship between Line objects and Job objects and the pointers linking the two. Fig. 19 illustrates the relationship between

Party objects, Job objects and Task objects and the pointers linking the Job objects to the parties and tasks.

Media Engine Implementation

Figs. 20A-D illustrate the process steps performed by the media engine of the WebPhone in accordance with the present invention. The coding of the process steps of the flowchart of Figs. 20A-D and to instructions suitable for use by the WebPhone will be understandable by those having ordinary skill in the programming arts. Fig. 20A illustrates the process executed by the media engine when the CMD attribute of a Task object is defined as a AE_USEME command, as previously illustrated in Fig. 19A. The Task objects are set up by the event manager. The media engine manages routing and resources. For example a microphone, file or socket may provide a source of data to media engine while a destination may comprise either a speaker file or socket. The media engine serves to perform compression/decompression as well as copying functions. For the purposes of describing flowcharts 20 A-D the media engine will referred to as media engine 2000.

Referring to Fig. 20A, media engine 2000 first determines the source of a data stream, as illustrated by decisional block 2002. If the source is a microphone, media engine 2000 determines whether or not the current audio data from the microphone source is silence, as illustrated in decisional block 2004. If the audio stream from the microphone is not silent the data will be accumulated into a microphone buffer, as illustrated by procedural block 2006. Next, the media engine will determine whether or not the buffer is full, as illustrated by decisional 2008. If the buffer is full, process flow will proceed to a determination of the destination via connector Q. If in decisional block 2004 the determination was made that the audio data from the microphone was silence, the media engine notes the length of the silence, as illustrated by procedural block

2010. Next, the media engine determines whether or not the buffer is empty, as illustrated by decisional block 2012. If the buffer is empty, process flow proceeds to a determination of the source, via connector R, as illustrated by decisional block 2030.

Returning again to decisional 2014, a determination of the destination of the audio data made after either a determination that the buffer is full, via connector Q, or that the source of the audio data is a socket, e.g., one of the branches of decisional block 2002. If in decisional block 2014 a determination is made that the destination is a socket, media engine 2000 determines if a party is online, as illustrated by decisional block 2028. If the party is online media engine 2000 will write to the socket associated with that party, as illustrated by procedural block 2026. The process as illustrated by decisional 2028 and process block 2026 are repeated for every party associated with the Job object, i.e., conference calls include multiple parties. Following writing to the parties socket, process flow returns decisional block 2030 for a determination of the source, as illustrated. If in decisional block 2014 a determination was made that the speaker was the destination, media engine makes a further determination to whether or not the there is more than one party on the conversation, i.e., conference call, as illustrated by decisional block 2020. If there is only one other party besides the user on the call, process flow proceeds to junction K where the audio data is written to the speaker, as illustrated by process block 2022. If in decisional block 2020 a determination was made that multiple parties were associated with a call media engine 2000 mixes the audio data into a mixing buffer, as illustrated by process block 2016. Next media engine 2000 determines whether or not the speaker is idle. If so, the audio data from the mixing buffer is written to the speaker as illustrated by procedural block 2022. Otherwise, process flow proceeds to junction R. In decisional block 2030 media engine 2000 determines again what the source of an audio data stream is. If the source is determine to be a socket, media engine 2000 will place the empty buffer on the winSock queue, as illustrated by process block 2036. If the source is determined to be a microphone, and the microphone is enabled, as determined in decisional block 2032, media engine 2000 will place the empty buffer on the mic sampling queue, as illustrated by process block 2034. Otherwise, media engine 2000 will place the empty buffer in the free pool of buffer space, as illustrated by process 2038. Either branch of decisional block 2030 will result in a return from the task execution process, as illustrated.

Fig. 20B, illustrates the process flow performed by media engine 2000 upon receiving a task object from the event manager having the CMD attribute defined with a AE_START, i.e., the event manager instructs the media engine to start a copy operation from a source to a destination. First, media engine 2000 determines whether or not the source is a microphone or a file, as illustrated by decisional block 2040. If the source is a file, process flow proceeds to block 2062 of Fig. 20C via connector F, as described hereinafter. If the source is determined to be a microphone, media engine 2000 will determine whether or not the microphone is on, as illustrated by decisional 2044. If the microphone is not on, an internal error notification will be generated, as illustrated by procedural block 2046. If the microphone is on, media engine 2000 will enable microphone sampling, obtain space from the buffer pool, and perform an asynchronous read from the microphone, as illustrated by process blocks 2048, 2050 and 2052, respectively. If in decisional block 2040 media engine 2000 determined that the source was a socket, buffer space will be retrieved from the buffer pool, as illustrated by process block 2042, and an asynchronous read from the socket will be performed, as illustrated by process block 2045. Following the an asynchronous read from either a socket or a microphone, media engine 2000 will return the task to the event manager, as illustrated.

Fig. 20 illustrates the process flow performed by media engine 2000 upon receiving a Task object from the event manager in which the CMD attribute is defined with a AE_FILLME command value, i.e., an empty packet has been returned from either an MCI or WINSOCK asynchronous write operation upon completion. First, media engine 2000 determines whether the source is from a file or either a socket or speaker, as illustrated by decisional block 2054. If the source is a file, media engine 2000 will read a portion of the file, as illustrated by process block 2062. Next, media engine 2000 will make a determination as to whether the destination is either a socket or a speaker, as illustrated by decisional block 2068. If the destination is a socket process flow will return to decisional block 2028 of Fig. 20A via connector S, as illustrated. If the destination is a speaker, process flow will proceed to process block 2022 of Fig. 20A via connector K as illustrated.

If a determination was made in decision 2056 that the destination is a socket, media engine 2000 will place the buffer associated with the task or message in the WINSOCK free pool of buffer space, as illustrated by process block 2058. If the destination is determined to be a speaker, media engine 2000 next determines whether or not the buffer is empty, as illustrated by decision block 2060. If the buffer is not empty, the data within the mixing buffer will be written to the speaker, as illustrated by message 2064. If the buffer is empty, the buffer associated with the message, i.e., task, will be placed in the MCI message free pool, as illustrated by process block 2066. Both branches decisional block 2056 result in a return from the task by media engine 2000, as illustrated. In the above-described flow diagrams, a message may be a task implementation similar to the manner in which Microsoft Windows uses messages for task completion operations.

Fig. 20D illustrates the process path taken by media engine 2000 when the CMD attribute of a Task object is defined as a AE_STOP value, i.e., the event manager instructs the media engine to stop the current operation on behalf of a specified task. The process begins with the determination of whether or not the source is a microphone or file, as illustrated by decisional block 2070. If it is determined that the source is a file, process flow proceeds to block 280 where the source is set to none, i.e., no further data will retrieved or processed. If the process is determined to be a socket, media engine 2000 cancels any pending asynchronous reads from the socket, as illustrated by process block 2074. If a determination is made that the source is a microphone, media engine 2000 will determine whether or not the microphone is on, as illustrated by decisional block 2072. If the microphone is on, media engine 2000 cancels sampling of the audio signal from the microphone, as illustrated by process block 2076, and, discards the pending data in the mix buffer, as illustrated by process block 2078. Regardless of the determination of the source, all branches of the process flow terminate with the setting of the source to none or null, indicating a termination of the operation and a return by media 2000 from the task, as illustrated.

In an alternate embodiment, the various aspects of the invention may be implemented as a computer program product for use with a computer system. Such implementation may comprise a series of computer instructions either fixed on a tangible medium, such as a computer readable media, e.g. diskette 1142, CD-ROM 1147, ROM 1115, or fixed disk 1152 of Fig. 11, or transmittable to a computer system, via a modem or other interface device, such as communications adapter 1190 connected to the network 1195 over a medium 1191. Medium 1191 can be either a tangible medium, including but not limited to optical or analog communications lines, or may be implemented with wireless techniques, including but not limited to microwave, infrared or other transmission techniques. The series of computer instructions embodies all or part of the functionality previously described herein with respect to the invention. Those skilled in the art will appreciate that such computer instructions can be written in a number of programming languages for use with many computer architectures or operating systems. Further, such instructions may be stored using any memory technology, present or future, including, but not limited to, semiconductor, magnetic, optical or other memory devices, or transmitted using any communications technology, present or future, including but not limited to optical, infrared, microwave, or other transmission technologies. It is contemplated that such a computer program product may be distributed as a removable media with accompanying printed or electronic documentation, e.g., shrink wrapped software, preloaded with a computer system, e.g., on system ROM or fixed disk, or distributed from a server or electronic bulletin board over a network, e.g., the Internet or World Wide Web.

Although various exemplary embodiments of the invention have been disclosed, it will be apparent to those skill in the art that various changes and modifications can be made which will achieve some of the advantages of the invention without departing from the spirit and scope of the invention. These and other obvious modifications are intended to be covered by the appended claims.

T660X

TABLE 1
Client Table

Field	Data Type	Comments
id	ulong	Unique ID Sequence
activated	char	0 = NO, 1 = YES
activationDate	ulong	Secs since 00:00 UTC Jan 1, 1970
version capability	ushort	Version of the Webphone
version protocol	ushort	
version vendor	ushort	
paid	char	0 = NO, 1 = YES
prePaidCode	varchar(16)	
firstName	varchar(10)	
lastName	varchar(25)	
alias	varchar(20)	
emailAddr	varchar(90)	
IPAddr	varchar(80)	0.0.0.0 if not known
street	varchar(50)	
apt	varchar(5)	
city	varchar(20)	
state	varchar(20)	
country	varchar(20)	
postalCode	varchar(20)	
phone	varchar(25)	
fax	varchar(25)	
feature bits	ulong	WebPhone Feature Definitions
company	varchar(25)	Company Name
addrChanges	char	No. of address changes
addrChangeDate	ulong	Secs since 00:00 UTC
publish	char	0 = NO, 1 = YES
accessDate	ulong	Secs since 00:00 UTC

TABLE 1 (Con't)

Field	Data Type	Comments
accessCount	ulong	# of log ons
callCount	ulong	# of outbound calls
social security number	ulong	optional
age	ushort	optional
occupation code	ushort	optional
interest codes	ushort	optional
household income range	ushort	optional

T680X

TABLE 2
Online Table

Field	Data Type	Comments
emailAddr	varchar(90)	
IPAddr	varchar(80)	
flags	char	
onlineDate	ulong	Secs since 00:00 UTC

T681X

TABLE 3
WebBoard Table

Field	Data Type	Comments
id	ulong	Unique ID Sequence
image	varchar(255)	Filename of image file
imageType	char	.GIF =0, JPG = 1, RLE = 3
audio	varchar(255)	Filename of TSP encoded.WAV file
audioType	char	GSM=0, TRUESPEECH = 1
hits	ulong	Number of accrued hits
hitsprofile	varchar(8)	Filename of Demographics
version	ulong	version of WebBoard
URL	varchar (255)	home page url

T682X

TABLE 4
Weboard Config Table

Field	Data Type	Comments
count	ulong	Number of WebBoards

TABLE 5
Source Table

Field	Data Type	Comments
id	ulong	Unique ID Seqence
weboardID	ulong	Link to WebBoard record
name	varchar(50)	Company's name
url	varchar(80	URL to Home Page
street	varchar(50)	
apt	varchar(5)	
city	varchar(20)	
state	varchar(20)	
country	varchar(20)	
postalCode	varchar(20)	
phone	varchar(25)	
fax	varchar(25)	
contact	varchar(35)	Name of contact

T690X

TABLE 6
WebPhone Protocol (WPP) Packet Definitions

Packet	Packet Type	Direction	Data
Invalid	WPP_INVALID	←→	WPP_INVALID
Online Req	WPP_ONLINEREQ	→	WPP_ONLINEREQ, sid, version, emailAddr, IPAddr, onlineState, feature bits
OnlineACK	WPP ONLINEACK	←	WPP_ONLINEACK, sid onlineStatus, feature bits
Offline	WPP_OFFLINE	←→	WPP_OFFLINE, sid
Hello	WPP_HELLO	←→	WPP_HELLO, sid, version
Connect Req	WPP_CONNECTREQ	→	WPP_CONNECTREQ, sid, version, callType, partyEmailAddr, emailAddr, IPAddr, connectState
Connect ACK	WPP_CONNECTACK	←→	WPP_CONNECTACK, sid, connectStatus, partyIPaddr
Call	WPP_CALL	←→	WPP CALL, sid, version, emailAddr, IPAddr, userInfo
CallACK	WPP_CALLACK	←→	WPP_CALLACK, sid, version, emailAddr, IpAddr, userInfo
CnfCall	WPP_CNFCALL	←→	WPP_CNFCALL, sid, version, emailAddr, IPAddr, userInfo
CnfCallACK	WPP_CNFCALLACK	←→	WPP_CNFCALLACK, sid, version
Answer	WPP_ANSWER	←→	WPP_ANSWER, sid
Busy	WPP_BUSY	←→	WPP_BUSY, sid
AnsMachine	WPP_ANSMACH	←→	WPP_ANSMACH, sid, state
End	WPP_END	←→	WPP_END, sid
Hold	WPP_HOLD	←→	WPP_HOLD, SID, (ON/OFF)
Reject	WPP_REJECT	←→	WPP_REJECT, sid
Camp	WPP_CAMP	←→	WPP_CAMP, sid
CampACK	WPP_CAMPACK	←→	WPP_CAMPACK, sid
Audio	WPP_AUDIO	←→	WPP_AUDIO, sid, audioType, silence, length, audioData
Pulse	WPP_PULSE	→	WPP_PULSE, sid
Adjpulse	WPP_PULSE	←	WPP_ADJPULSE, sid, adjPulse

T700X

TABLE 6 (con't)

Packet	**Packet Type**	**Direction**	**Data**
Vmail	WPP_VMAIL	←→	WPP_VMAIL, sid, audioType, silence, length, audioData
VmailEnd	WPP_VMAILEND	←→	WPP_VMAILEND, sid
OgmEnd	WPP_OGMEND	←→	WPP_OGMEND, sid
CnfAdd	WPP_CNFADD	←→	WPP_CNFADD, sid, partyEmailAddr, partyIPaddr, partInfo
CnfDrop	WPP_CNFDROP	←→	WPP_CNFDROP, sid
FileXmtReq	WPP_FILEXMTREQ	←→	WPP_FILEXMTREQ, sid, fileType, fileName, fileSize

TABLE 7
WebPhone Protocol (WPP) Packet Definitions

Packet	Packet Type	Direction	Data
FileXmtAck	WPP_FILEXMTACK	←→	WPP_FILEXMTACK, sid
File	WPP_FILE	←→	WPP_FILE, sid, length, fileData
FileXmtEnd	WPP_FILEXMTEND	←→	WPP_FILEXMTEND, sid
FileXmtAbort	WPP_FILEXMTABORT	←→	WPP_FILEXMTABORT, sid
InfoReq	WPP_INFOREQ	→	WPP_INFOREQ, sid, query
InfoACK	WPP_INFOACK	←	WPP_INFOACK, sid, nparties
Info	WPP_INFO	←	WPP_INFO, sid, partyInfo
InfoAbort	WPP_INFOABORT	→	WPP_INFOABORT, sid
UserInfoReq	WPP_USRINFOREQ	←	WPP_USRINFOREQ, sid
UserInfo	WPP_USRINFO	→	WPP_USRINFO, sid, version, userInfo
WBImageStart	WPP_WBIMAGESTART	←	WPP_WBIMAGESTART, sid, fileSize, imageType, url
WBImage	WPP_WBIMAGE	←	WPP_WBIMAGE, sid, length, imageData
WBImageEnd	WPP_WBIMAGEEND	←	WPP_WBIMAGEEND, sid
WBAudioStart	WPP_WBAUDIOSTART	←	WPP_WBAUDIOSTART, sid, fileSize, audioType
WBAudio	WPP_WBAUDIO	←	WPP_WBAUDIO, sid, length, audioData
WBAudioEnd	WPP_WBAUDIOEND	←	WPP_WBAUDIOEND, sid
Registration	WPP_REG	←	WPP_REG, sid, feature bits, EEMAILAddr, customer id
Audio Start	WPP_AUDIO START	← →	WPP_AUDIO START, sid
Audio End	WPP_AUDIO END	← →	WPP_AUDIO END, sid
Caller OK	WPP_CALLEROK	→	WPP_CALLEROK, sid, version, emailAddr, feature bits
Caller ACK	WPP_CALLERACK	←	WPP_CALLERACK, sid, callerStatus, feature bits
Key Pad	WPP_KEYPAD	←	WPP_KEYPAD, sid (ON/OFF)
Key	WPP_KEY	→	WPP_KEY,sid,ascii character
WBLIST	WPP_WBLIST	←	WPP_WBLIST, sid, list of WB IDs
WBLIST REQ	WPP_WBLISTREQ	→	WPP_BBLISTREQ, sid

T720X

TABLE 7 (con't)

Packet	Packet Type	Direction	Data
WB REQ	WPP_WEBBOARDREQ	→	WPP_WEBBOARDREQ, sid, WBid, Client id
WB HIT	WPP_WEBBOARDHIT	→	WPP_WWBOARDHIT, sid, WB id, Client id
ANS FULL	WPP_ANS FULL	→	WPP_ANS FULL, sid

TABLE 8

WebPhone Protocol (WPP) Packet Data Definitions

T730X

Element	Data Type	Comment
WPP_*	unsigned char	WPP message identifier
sid	unsigned long	session id unique per call
version	unsigned(3)	version of the webphone (capability, protocol, vendor)
emailAddr	varchar(90)	email address of caller
IPAddr	varchar(80)	IP Address
onlineState	unsigned char	bit 0 (ACTIVE/INACTIVE)
		bit 1 (Merchant Phone)
		bit 2 (Connection Server)
		bit 3 (webboard disabled)
		bit 4 Not Used
		bit 5 Not Used
		bit 6 Not Used
		bit 7 Not Used
call Type	unsigned char	call type 0: EMAIL / 1:IPCALL
partyEmailAddr	varchar(90)	email address of person to call
connectStatus	unsigned char	0:NO WEBPHONE
		1: ONLINE

TABLE 8 (con't)

Element	Data Type	Comment
		2:OFFLINE
		3:RECONNECT
		4:PERM_RECONNECT
partyIPAddr	varchar(80)	IP Address of person to call
userInfo	varchar(120)	firstName, LastName, alias, emailAddr, street, apt, city, state, country, postalCode, phone, fax, company
audioType	unsigned char	audio compress type
		0:GSM
		1:TRUESPEECH

T750X

TABLE 9
WebPhone Protocol (WPP) Packet Data Definitions

Element	Data Type	Comment
length	unsigned short	length of audio or data in bytes
audioData	512 Bytes	compressed audio data
feature bits	unsigned long	WebPhone feature definition
fileType	unsigned char	file type
		0:DATA
		1:EMAIL
		2:TEXT
		3:BINARY
fileName	varchar(13)	name of file to be transmitted.
fileSize	unsigned long	size of file to be transmitted in bytes
fileData	variable	file data
query	varchar(120)	firstName, lastName, company, city, state, country
nparties	unsigned long	number of parties or query records being sent
size	unsigned long	size of file (IMAGE or AUDIO) to be sent
imageType	unsigned char	image type
		0:GIF
		1:JPG
imageData	512 Bytes	image data
eemailAddr	varchar(90)	encrypted email Address
onlineStatus	unsigned char	0 OK
		-1 Error
callerStatus	unsigned char	0 is unpaid
		1 if paid
onlineState	unsigned char	bit 0 webboard disabled
		bit 1 Not Used
		bit 2 Not Used
		bit 3 Not Used

TABLE 9 (con't)

Element	Data Type	Comment
		bit 4 Not Used
		bit 5 Not Used
		bit 6 Not Used
		bit 7 Not Used
WBid	unsigned long	link to WebBoard record
adjpulse	unsigned long	timer offset in secs

Table 10
Feature Definition

feature bit 0	0 = 1 line		1 = 4 lines
	bit 1	0 = Limited Call Time	1 = Unrestricted Call Time
	bit 2	0 = Limited VMail OGM	1 = Unlimited Vmail OGM
	bit 3	0 = Limited Directory Entries	1 = Unlimited Dir Entries
	bit 4	0 = Webboard Not Disabled	1 = Allowed to Disable
	bit 5	0 = Conferencing(audio) Disabled	1 = Conferencing Enabled
	bit 6	0 = Conferencing(video) Disabled	1 = Conferencing Enabled
	bit 7	0 = Whiteboard Disabled	1 = Whiteboard Enabled
	bit 8	0 = Offline voicemail Disabled	1 = Offline voicemail Enabled
	bit 9 - 27 Reserved		
	bit 28 - 30 Type of Phone		

T76X

0 - Normal webphone
1 - Agent
2 - Business webphone
3 - Gateway
4 - ACD
5-7 reserved

bit 31 1 = Disable all WebPhone features

TABLE 11

Offset	Name	Size	Description
	Reserved		Reserved
+1	SessionID	4	Unique value for duration of this connection
+5	Version	6	WebPhone version and distributor stamp
+11	Codec	1	Audio compression algorithm selected
+12	FirstName	10	Given name, middle initial
+22	LastName	25	Surname
+47	Alias	20	Nickname
+67	EmailAddr	90	Caller's electronic mail address
+157	IpAddr	80	Caller's WebPhone's Internet address
+237	Street	50	Street address of user
+287	Apt	20	Apartment or suite number
+307	City	20	City name
+327	State	20	State or province
+347	Country	20	Country name
+367	ZipCode	20	Zip or postal code
+387	Phone	25	Telephone number
+412	Fax	25	Facsimile telephone number
+437	Company	25	Employer or organization name
+487	File Name	25	Name of file
+512	Action Code	25	Action descriptor
+537	File Type	10	File type descriptor
+547	Status	25	Status of WebPhone utility

T7OK

CLAIMS

Sub A1

1. A computer program product for use with a computer system having a display and an audio transducer, the computer system operatively coupled to other computers and a server over a computer network, the computer program product comprising a computer usable medium having computer readable code means embodied in the medium comprising:
   a. program code means for generating a user-interface through which a user may coact with the computer system;
   b. program code means responsive to user input commands for establishing a point-to-point communications link with another computer over the computer network; and
   c. program code means, responsive to audio data from the audio transducer, for transmitting the audio data over the communication link to the other computer.

2. The computer program product of claim 1 wherein the program code means for establishing a point-to-point communication link further comprises:
   c.1 program code means, responsive to the network protocol address of the second processor, for establishing a point-to-point communication link between the first processor and the second processor over the computer network.

3. The computer program product of claim 2 wherein the program code means for establishing a point-to-point communication link further comprise:
   c.2 program code means for transmitting, from the first processor to the server, a query as to whether the second processor is connected to the computer network; and

c.3 program code means for receiving a network protocol address of the second processor from the server, when the second processor is connected to the computer network.

4. The computer program product of claim 2 wherein the program code means for establishing a point-to-point communication link further comprises:

c.2 program code means for transmitting an E-mail signal containing a network protocol address from the first processor to the server over the computer network;

c.3 program code means for receiving a second network protocol address from the second processor over the computer network.

5. The computer program product of claim 1 further comprising:

d. program code means for processing audio data.

6. The computer program product of claim 5 wherein the program code means for processing the audio data comprises:

program code means for compressing or decompressing the audio data.

add A2

08/722,316

ABSTRACT

A communication utility for establishing real-time, point-to-point communications between processes over a computer network includes apparatus for querying a server as to the network protocol address of another client process, and apparatus for directly establishing a communication link with the client process upon receipt of the network protocol address from the server. In one embodiment, the utility includes a sophisticated user interface having features similar to typical telephony hardware but implementing greater flexibility with software.

BAR CODE LABEL

U.S. PATENT APPLICATION

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT
08/721,316	09/25/96	395	2302

APPLICANT

SHANE D. MATTAWAY, BOCA RATON, FL; GLENN W. HUTTON, MIAMI, FL; CRAIG B. STRICKLAND, TAMARAC, FL.

CONTINUING DATA*******************

VERIFIED THIS APPLN IS A CIP OF 08/533,115 09/25/95

FOREIGN/PCT APPLICATIONS**********

VERIFIED

FOREIGN FILING LICENSE GRANTED 01/25/97

STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS	FILING FEE RECEIVED	ATTORNEY DOCKET NO.
FL	27	6	1	$880.00	

ADDRESS

BRUCE D JOBSE
BOOKSTEIN & KUDIRKA
ONE BEACON STREET
BOSTON MA 02108

TITLE

GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

This is to certify that annexed hereto is a true copy from the records of the United States Patent and Trademark Office of the application which is identified above.

By authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

Date Certifying Officer

PATENT APPLICATION SERIAL NO. 08/721316

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

290 SB 10/22/96 08721316
1 101 750.00 CK N0003/7002

PTO-1556
(5/87)

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 1995

Application or Docket Number
08/7?? ??6

CLAIMS AS FILED - PART I

FOR	NUMBER FILED (Column 1)		NUMBER EXTRA (Column 2)	SMALL ENTITY RATE	SMALL ENTITY FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY FEE
BASIC FEE					375.00	OR		750.00
TOTAL CLAIMS	6	minus 20 =	*	x$11=		OR	x$22=	
INDEPENDENT CLAIMS	1	minus 3 =	*	x39=		OR	x78=	
MULTIPLE DEPENDENT CLAIM PRESENT				+125=		OR	+250=	
				TOTAL		OR	TOTAL	750

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

AMENDMENT A

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE	ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	ADDITIONAL FEE
Total	* 18	Minus	** 20	=	x$11=		OR	x$22=	
Independent	* 3	Minus	*** 3	=	x39=		OR	x78=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+125=		OR	+250=	
					TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE	ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	ADDITIONAL FEE
Total	*	Minus	**	=	x$11=		OR	x$22=	
Independent	*	Minus	***	=	x39=		OR	x78=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+125=		OR	+250=	
					TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE	ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	ADDITIONAL FEE
Total	*	Minus	**	=	x$11=		OR	x$22=	
Independent	*	Minus	***	=	x39=		OR	x78=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+125=		OR	+250=	
					TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

08/721316

709	227
Class	Subclass

ISSUE CLASSIFICATION

UTILITY SERIAL NUMBER 08/721316 | PATENT DATE DEC 28 1999 | PATENT NUMBER 6009469

SERIAL NUMBER	FILING DATE	CLASS	SUBCLASS	GROUP ART UNIT
08/721,316	09/25/96	~~395~~ 709	~~200~~ 227	~~2302~~ 2757

6009469

APPLICANTS: SHANE D. MATTAWAY, BOCA RATON, FL; GLENN W. HUTTON, MIAMI, FL; C... STRICKLAND, TAMARAC, FL.

CONTINUING DATA*******************
VERIFIED THIS APPLN IS A CIP OF 08/533,115 09/25/95
PROVISIONAL APPLICATION NO. 60/025,415 09/04/96
PROVISIONAL APPLICATION NO. 60/024,251 08/21/96
AHW.

CERTIFICATE MAY - 8 2001 OF CORRECTION

CERTIFICATE MAY - 8 2001 OF CORRECTION

FOREIGN/PCT APPLICATIONS**********
VERIFIED
AHW.

FOREIGN FILING LICENSE GRANTED 01/25/97

Foreign priority claimed / 35 USC 119 conditions met / Verified and Acknowledged / Examiner's Initials	AS FILED	STATE OR COUNTRY	SHEETS DRWGS.	TOTAL CLAIMS	INDEP. CLAIMS	FILING FEE RECEIVED	ATTORNEY'S DOCKET NO.
☐ yes ☒ no; ☐ yes ☐ no	→	FL	27	6	1	$980.00	

ADDRESS:
BRUCE D JOBSE
BOOKSTEIN & KUDIRKA
ONE BEACON STREET
BOSTON MA 02108

TITLE: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

U.S. DEPT. OF COMM./PAT. & TM—PTO-436L (Rev.12-94)

12-6-99 Formal Drawings (27 shts) set 8-20-99

PARTS OF APPLICATION FILED SEPARATELY [redacted]

Applications Examiner

NOTICE OF ALLOWANCE MAILED		CLAIMS ALLOWED	
6-22-99	Assistant Examiner	Total Claims 18	Print Claim 1

ISSUE FEE			DRAWING		
Amount Due $1210.00	Date Paid 8-4-99	ELLIS B. RAMIREZ PRIMARY EXAMINER / Primary Examiner	Sheets Drwg. 27	Figs. Drwg. 33	Print Fig. 1

ISSUE BATCH NUMBER U91

PREPARED FOR ISSUE

Label Area

WARNING: The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.

Form PTO-436A (Rev. 8/92)

T.D.

(FACE)

STAPLE AREA ☆U.S. GOVERNMENT PRINTING OFFICE: 1998-440-769

PATENT NUMBER

APPLICATION SERIAL NUMBER

08/721,316

APPLICANT'S NAME (PLEASE PRINT)

Mattaway et al

IF REISSUE, ORIGINAL PATENT NUMBER

INTERNATIONAL CLASSIFICATION

G	0	6	F		17/00

ORIGINAL CLASSIFICATION

CLASS	SUBCLASS
709	227

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)			

GROUP ART UNIT 2757

ASSISTANT EXAMINER (PLEASE STAMP OR PRINT FULL NAME)

PRIMARY EXAMINER (PLEASE STAMP OR PRINT FULL NAME) Ellis B. Ramirez

PTO 270
(REV. 5-91)

ISSUE CLASSIFICATION SLIP

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

SEARCHED

Class	Sub.	Date	Exmr.
~~395~~	~~200.38~~	~~3/12/98~~	GSW
~~"~~	~~200.34~~	~~3/25/98~~	
~~"~~	~~200.35~~	~~"~~	
~~"~~	~~200.48~~	~~"~~	
395	200.57	3/26/98	GSW
395	200.58		
	updated	6/10/99	Q
709	227 228	6/10/99	Q
370	352 355 357 389 395	6/10/99	Q

INTERFERENCE SEARCHED

Class	Sub.	Date	Exmr.
709	227	6/10/99	Q

SEARCH NOTES

	Date	Exmr.
Discussed Search w/ Examiner L. Barry and Prior Art Reviewed	3/25/98	GSW.
2 Internet Searches (see inside FW).	3/18/98 3/24/98	GSW
Reviewed Case for D.P.	6/10/99	Q

Note: Check for D.P.

(RIGHT OUTSIDE)

Staple Issue S ..ere

POSITION		ID NO.	DATE
CLASSIFIER		w	10-30-96
EXAMINER		277	11-25
TYPIST		502	1/25
VERIFIER		204	1-20-97
CORPS CORR.			
SPEC. HAND		4/4	1/21/97
FILE MAINT.		442	11-26-96
DRAFTING			

INDEX OF CLAIMS

Claim		Date							
Final	Original	3/27/98	[illegible]						
1	1	✓	=						
2	2.	✓	=						
3	3.	✓	=						
4	4.	✓	=						
	5	✓							
	6	✓							
5	7		=						
6	8		=						
7	9		=						
8	10		=						
9	11		=						
10	12		=						
11	13		=						
12	14		=						
13	15		=						
14	16		=						
15	17		=						
16	18.		=						
17	19		=						
18	20		=						
	21								
	22								
	23								
	24								
	25								
	26								
	27								
	28								
	29								
	30								
	31								
	32								
	33								
	34								
	35								
	36								
	37								
	38								
	39								
	40								
	41								
	42								
	43								
	44								
	45								
	46								
	47								
	48								
	49								
	50								

SYMBOLS

- ✓ .... Rejected
- = ... Allowed
- - (Through numberal) Canceled
- + ... Restricted
- N .... Non-elected
- I .... Interference
- A .... Appeal
- O .... Objected

Claim		Date							
Final	Original								
	51								
	52								
	53								
	54								
	55								
	56								
	57								
	58								
	59								
	60								
	61								
	62								
	63								
	64								
	65								
	66								
	67								
	68								
	69								
	70								
	71								
	72								
	73								
	74								
	75								
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								

UTIL SERI
SERIA
APPLICANTS
FOREIG
Foreign priority 35 USC 119 c
Verified and Ac
ADDRESS
TITLE
PARTS OF A FILED SEPAR
NOTICE OF A
ISS
Amount Due

Form PTO-436A (Rev. 8/92)

T.D.

(LEFT INSIDE)

UNITED ST[illegible]S DEPARTMENT OF COMMERCE
Patent and Trad[illegible]mark Office
Address: COMMISS[illegible]R OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO./TITLE
08/721,316	09/25/96	MATTAWAY	S

0222/1202

BRUCE D JOBSE
BOOKSTEIN & KUDIRKA
ONE BEACON STREET
BOSTON MA 02108

0000

DATE MAILED: 12/02/96

NOTICE TO FILE MISSING PARTS OF APPLICATION
Filing Date Granted

An Application Number and Filing Date have been assigned to this application. However, the items indicated below are missing. The required items and fees identified below must be timely submitted ALONG WITH THE PAYMENT OF A SURCHARGE for items 1 and 3-6 only of $ 130.00 for a ☒ large entity ☐ small entity in compliance with 37 CFR 1.27. The surcharge is set forth in 37 CFR 1.16(e). Applicant is given TWO MONTHS FROM THE DATE OF THIS NOTICE within which to file all required items and pay any fees required above to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

If all required items on this form are filed within the period set above, the total amount owed by applicant as a ☐ large entity ☐ small entity (verified statement filed), is $ 130.00 .

☐ 1. The statutory basic filing fee is:
- ☐ missing.
- ☐ insufficient.

Applicant must submit $ ________ to complete the basic filing fee and/or file a verified small entity statement claiming such status (37 CFR 1.27).

☐ 2. Additional claim fees of $ ________, including any multiple dependent claim fees, are required. *Applicant must either submit the additional claim fees or cancel additional claims for which fees are due.*

☒ 3. The oath or declaration:
- ☒ is missing.
- ☐ does not cover the newly submitted items.
- ☐ does not identify the application to which it applies.
- ☐ does not include the city and state or foreign country of applicant's residence.

An oath or declaration in compliance with 37 CFR 1. 63, including residence information and identifying the application by the above Application Number and Filing Date is required.

☐ 4. The signature(s) to the oath or declaration is/are:
- ☐ missing.
- ☐ by a person other than inventor or person qualified under 37 CFR 1.42, 1.43, or 1.47.

A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.

☐ 5. The signature of the following joint inventor(s) is missing from the oath or declaration:

____

An oath or declaration listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date, is required.

☐ 6. A $ ________ processing fee is required since your check was returned without payment (37 CFR 1.21(m)).

☐ 7. Your filing receipt was mailed in error because your check was returned without payment.

☐ 8. The application does not comply with the Sequence Rules.
See attached "Notice to Comply with Sequence Rules 37 CFR 1.821-1.825."

☐ 9. OTHER:

Direct the response and any questions about this notice to "Attention: Box Missing Parts."

A copy of this notice MUST be returned with the response. C Hohne

Customer Service Center
Initial Patent Examination Division (703) 308-1202

202 130-105 BCD #3

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

MAIL ROOM DEC 22 1996 55 PAT. & TRADEMARK OFFICE

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO./TITLE
08/721,316	09/25/96	MATTAWAY	S

0222/1202

BRUCE D JOBSE
ROOKSTEIN & KUDIRKA
ONE BEACON STREET
BOSTON MA 02108

2/2/97

0000

DATE MAILED: 12/02/96

NOTICE TO FILE MISSING PARTS OF APPLICATION
Filing Date Granted

An Application Number and Filing Date have been assigned to this application. However, the items indicated below are missing. The required items and fees identified below must be timely submitted ALONG WITH THE PAYMENT OF A SURCHARGE for items 1 and 3-6 only of $ 130.00 for a ☒ large entity ☐ small entity in compliance with 37 CFR 1.27. The surcharge is set forth in 37 CFR 1.16(e). Applicant is given TWO MONTHS FROM THE DATE OF THIS NOTICE within which to file all required items and pay any fees required above to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

If all required items on this form are filed within the period set above, the total amount owed by applicant as a ☐ large entity ☐ small entity (verified statement filed), is $ 130.00.

☐ 1. The statutory basic filing fee is:
  ☐ missing.
  ☐ insufficient.
  Applicant must submit $ ________ to complete the basic filing fee and/or file a verified small entity statement claiming such status (37 CFR 1.27).

☐ 2. Additional claim fees of $ ________, including any multiple dependent claim fees, are required.
  Applicant must either submit the additional claim fees or cancel additional claims for which fees are due.

☒ 3. The oath or declaration:
  ☒ is missing.
  ☒ does not cover the newly submitted items.
  ☐ does not identify the application to which it applies.
  ☐ does not include the city and state or foreign country of applicant's residence. BK
  An oath or declaration in compliance with 37 CFR 1. 63, including residence information and identifying the application by the above Application Number and Filing Date is required.

☐ 4. The signature(s) to the oath or declaration is/are:
  ☐ missing.
  ☐ by a person other than inventor or person qualified under 37 CFR 1.42, 1.43, or 1.47.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.

☐ 5. The signature of the following joint inventor(s) is missing from the oath or declaration:

____

An oath or declaration listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date, is required.

☐ 6. A $ ________ processing fee is required since your check was returned without payment (37 CFR 1.21(m)).

☐ 7. Your filing receipt was mailed in error because your check was returned without payment.

☐ 8. The application does not comply with the Sequence Rules.
  See attached "Notice to Comply with Sequence Rules 37 CFR 1.821-1.825."

☐ 9. OTHER: BK

Direct the response and any questions about this notice to "Attention: Box Missing Parts."

01/13/97 08721316
1 105 130.00 CK

A copy of this notice MUST be returned with the response.

Customer Service Center
Initial Patent Examination Division (703) 308-1202

MAIL ROOM DEC 22 1996 55 PAT. & TRADEMARK OFF.

N0003/7002
PATENT

Assistant Commissioner for Patents
Box Missing Parts
Washington, DC 20231

TRANSMITTAL LETTER

Sir:

Transmitted herewith for filing in the Patent Application of

Applicant:	Shane D. Mattaway, et al.
Serial No.:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

are the following papers:

X Response to Notice to File Missing Parts of Application

X Signed Declaration

X Copy of Notice to File Missing Parts of Application *Filing Date Granted*

A check in the amount of $130.00 is enclosed to cover the surcharge. The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §§1.16 and 1.17 that may be required, or credit any overpayment, to our Deposit Account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse, Esq.
Reg. No. 33,518
BOOKSTEIN & KUDIRKA, P.C.
One Beacon Street
Boston, MA 02108
(617) 367-4600

BDJ:rc

H:\BDJ\N0003\7002\MISPRTTR.WPD

PATENT
N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re The Application of: Shane D. Mattaway, et al.	)	Examiner: Not yet assigned
	)	Art Unit: Not yet assigned
Serial No. 08/721,316	)	
Filed: September 25, 1996	)	Bookstein & Kudirka, P.C.
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION	)	One Beacon Street
	)	Boston, MA 02108

CERTIFICATE OF MAILING

I hereby certify that the following Response to Notice to File Missing Parts is being deposited with the United States Postal Service as first class mail pursuant to 37 C.F.R. 1.8 in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231, Attention: Box Missing Parts, on December 17, 1996.

Rivki Cohen
Rivki Cohen

Assistant Commissioner for Patents
Washington, D.C. 20231
Attention: Box Missing Parts

Sir:

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

In response to the Notice to File Missing Parts of Application-Filing Date Granted mailed December 2, 1996, enclosed herewith is a Declaration executed by the named inventors for the above-referenced application. A check for $130.00 to cover the surcharge for this Response is enclosed.

The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §§1.16 and 1.17 that may be required, or credit any overpayment, to our Deposit Account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse, Esq.
Registration No. 33,518
BOOKSTEIN & KUDIRKA, P.C.
One Beacon Street
Boston, MA 02108
(617) 367-4600

BDJ:rc

Date: December 17, 1996

ATTORNEY'S DOCKET NO. N0003/7002

x020297

H:\BDJ\N0003\7002\RESPMISS.WPD

#3

DOCKET NUMBER: N0003/7002

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are stated below next to my name:

I believe I am an original, first and joint inventor the subject matter which is claimed and for which a patent is sought on the invention entitled **GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION** the specification of which was filed on September 25, 1996 under Attorney's Docket Number N0003/7002, now U.S. Patent Application Serial No. 08/721,316.

I hereby state that I have reviewed and understand the contents of the above identified patent application, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 C.F.R. 1.56.

I hereby claim the benefit of foreign priority under 35 U.S.C. 119 of any foreign application(s) for patent or inventor's certificate having a filing date before that of the application the priority of which is claimed:

Prior Foreign Application(s):			Priority Claimed
________	________	________	_____Yes _____No
(Number)	(Country)	(Filing Date)	

I hereby claim the benefit of United States priority under 35 U.S.C. 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in a listed prior United States application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 C.F.R. 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial #)	(Filing Date)	(Status)
08/533,115	9/25/95	pending
60/024,251	8/21/96	pending
60/025,415	9/4/96	pending

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

7

Bruce D. Jobse	Reg. No. 33,518	Paul E. Kudirka	Reg. No. 26,931
Arthur Z. Bookstein	Reg. No. 22,958	John F. Perullo	Reg. No. 36,265
Philip L. Conrad	Reg. No. 34,567	Steven G. Saunders	Reg. No. 36,265
Paul J. Cook	Reg. No. 20,280		

Send correspondence to Bruce D. Jobse, BOOKSTEIN & KUDIRKA, P.C., One Beacon Street, Boston, Massachusetts, 02108.

1-00

FULL NAME OF INVENTOR: Shane D. Mattaway

INVENTOR'S SIGNATURE: Shane D. Mattaway DATE: 12/8/96

RESIDENCE: 826 Periwinkle, Boca Raton, FL 33486
CITIZENSHIP: U.S.A.
POST OFFICE ADDRESS: 826 Periwinkle, Boca Raton, FL 33486

2-00

FULL NAME OF INVENTOR: Glenn W. Hutton

INVENTOR'S SIGNATURE: [signature] DATE: 12-2-96

RESIDENCE: 9725 Hammocks Boulevard, #206, Miami, FL 33196
CITIZENSHIP: Canada
POST OFFICE ADDRESS: 9725 Hammocks Boulevard, #206, Miami, FL 33196

3-00

FULL NAME OF INVENTOR: Craig B. Strickland

INVENTOR'S SIGNATURE: [signature] DATE: 12/10/96

RESIDENCE: 5713 NW 65th Terrace, Tamarac, FL 33321
CITIZENSHIP: ~~U.S.A.~~ Canada CBS
POST OFFICE ADDRESS: 5713 NW 65th Terrace, Tamarac, FL 33321

H:\BDJ\N0003\7002\DECL.WPD

MAIL ROOM
DEC 23 1996
PAT. & TRADEMARK OFF.

ATTORNEY'S DOCKET NO.:N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Shane D. Mattaway et al.
SERIAL NO.: 08/721,316
FILED: September 25, 1995
FOR: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
EXAMINER: --
ART UNIT: --

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 20th day of December, 1996.

Frances M. Cunningham

Frances M. Cunningham

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

Transmitted herewith for filing is/are the following document(s):

[X] Information Disclosure Statement
[X] PTO Form 1449

If the enclosed papers are considered incomplete, the Mail Room and/or the Application Branch is respectfully requested to contact the undersigned collect at (617) 367-4600, Boston, Massachusetts.

No fee is being submitted. If the fee is insufficient, the balance may be charged to the account of the undersigned, Deposit Account No. 02-3038. A duplicate of this sheet is enclosed.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse, Esq.
Reg. No.: 33,518
BOOKSTEIN & KUDIRKA, P.C.
One Beacon Street
Boston, Massachusetts 02108
Tel.: (617) 367-4600

ATTORNEY DOCKET NO.: N0003/7002
DATE: December 20, 1996
NDDH:\BDJ\N0003\7002\IDSTRANS.WPD

MAIL ROOM
DEC 23 1996
PAT. & TRADEMARK OFF.
84

0300

ATTORNEY'S DOCKET NO.: N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Shane D. Mattaway et al.
Serial No.:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	
Art Unit:	

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 20th day of December, 1996.

Frances M. Cunningham

Frances M. Cunningham

Assistant Commissioner for Patents
Washington, DC 20231

STATEMENT FILED PURSUANT TO THE DUTY OF
DISCLOSURE UNDER 37 C.F.R. §§1.56, 1.97 AND 1.98

Sir:

Pursuant to the duty of disclosure under 37 C.F.R. §§1.56, 1.97 and 1.98, the applicant requests consideration of this information disclosure statement.

Compliance with 37 C.F.R. §1.97

This information disclosure statement has been filed before the mailing date of a first office action on the merits in the above-identified application. No fee or certification is required.

Information Cited

The applicant hereby makes of record in the above-identified application the information listed on the attached form PTO-1449 (modified). The order of presentation of the references should not be construed as an indication of the relative importance of the references.

Remarks

A copy of each of the above-identified information is enclosed unless otherwise indicated on the attached form PTO-1449 (modified). It is respectfully requested that:

- The examiner consider completely the cited information, along with any other information, in reaching a determination concerning the patentability of the present claims;
- The enclosed form PTO-1449 be signed by the examiner to evidence that the cited information has been fully considered by the Patent and Trademark Office during the examination of this application;
- The citations for the information be printed on any patent which issues from this application.

By submitting this information disclosure statement, the applicant makes no representation that a search has been performed, of the extent of any search performed, or that more relevant information does not exist.

By submitting this information disclosure statement, the applicant makes no representation that the information cited in the statement is, or is considered to be, material to patentability as defined in 37 C.F.R. §1.56(b).

By submitting this information disclosure statement, the applicant makes no representation that the information cited in the statement is, or is considered to be, in fact, prior art as defined by 35 U.S.C. §102.

It is understood by applicant that the foregoing information will be considered and, to the extent deemed appropriate by the examiner, will be reflected in the examiner's communication.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse
Reg. No. 33,518
BOOKSTEIN & KUDIRKA, P.C.
One Beacon Street
Boston, Massachusetts 02108
Tel: (617) 367-4600
Attorneys for Applicant

Docket No.: N0003/7002
Date: December 20, 1996

H:\BDJ\N0003\7002\IDS.WPD

(FILE 'USPAT' ENTERED AT 15:36:24 ON 18 MAR 1998)

```
L1        219 S IP ADDRESS
L2        145 S L1 AND SERVER
L3        103 S L2 AND INTERNET
L4          6 S L3 AND TELEPHONY
L5          0 S (INTERNET AND (PHONE OR TELEPHONE OR TELEPHONY))/TI
L6          0 S (INTERNET AND (PHONE OR TELEPHONE OR TELEPHONY))/ABS
L7         12 S (INTERNET AND (PHONE OR TELEPHONE OR TELEPHONY))/AB
L8         32 S "IP ADDRESS" (3A) (SERVER OR DATABASE OR STORAGE OR COLL
ECT
L9          2 S ("IP ADDRESS" (5A) (SERVER OR DATABASE OR STORAGE OR COLLEC
L10         1 S L9 AND (TELEPHONY OR VOICE OR MULTIMEDIA OR SOUND OR TAL
K O
```

(FILE 'USPAT' ENTERED AT 18:26:56 ON 18 MAR 1998)

```
L1       1369 S IRC
L2          1 S "DYNAMIC IP ADDRESS" AND (SERVER OR DATABASE OR STORAGE)
L3          3 CHAT AND "IP ADDRESS"
```

(FILE 'USPAT' ENTERED AT 15:07:40 ON 23 MAR 1998)

```
L1         88 S 395*12/CCLS
L2          0 S L1 AND INTERNET
L3         19 S L1 AND TELEP?
L4          2 L1 AND "TELEPHONE INTERFACE"
```

(FILE 'USPAT' ENTERED AT 11:49:05 ON 24 MAR 1998)

```
L1          0 S "INTERNET TELEPHONY"
L2          7 S "NETWORK TELEPHONY"
L3       1037 S INTERNET
L4        511 S L3 AND TELEPHONE
L5         51 S L4 AND INTERNET (4A) TELEPHONE
L6          3 S L4 AND (INTERNET (4A) TELEPHONE)/AB
L7          2 L5 AND (INTERNET (W) TELEPHONE)
```

(FILE 'USPAT' ENTERED AT 14:12:11 ON 27 MAR 1998)

```
L1     103486 S INTERNET OR WEB OR WWW
L2       3531 S L1 AND (TELEPHON! OR VOICE OR TALK OR SPEAK OR SPEECH OR AU
L3        352 S L2 AND ( (ROLLING OR NEW OR DYNAMIC OR UNIQUE OR DIFFERENT
L4       3613 S L1 AND (TELEPHON! OR PHONE OR VOICE OR TALK OR SPEAK OR SPE
L5        359 S L4 AND ( (ROLLING OR NEW OR DYNAMIC OR UNIQUE OR DIFFERENT
L6        178 S L5 AND ((USER (W) INTERFACE) OR WINDOW)
L7         35 S L6 AND (IP (7A) (SERVER OR DATABASE OR "DATA BASE"))
```

Readme
VocalTec Internet Phone (TM)
Version 2.5 (Build 5) - February, 1995
==

In order to use Internet Phone, you need...

1. Windows 3.1 or higher (not NT).

2. 8MB of RAM recommended.

3. 486SX 25Mhz or faster recommended.

4. Windows compatible audio board, with speaker and microphone.

5. TCP/IP software with WINSOCK 1.1 support.

6. A SLIP/PPP, or direct Internet connection (14,400 baud minimum).

Installing the Internet Phone

1. Make sure that your microphone and speaker work properly, by recording yourself using the Microsoft's Sound Recorder. See "Preparing Your Audio Device" section, below.

2. Create a directory on your hard-disk
   e.g.: MD C:\IPHONE

3. From that directory, execute the self-extracting archive
   C:\IPHONE> IPHONE25.EXE

4. Choose File/Run and execute C:\IPHONE\ADDICONS
   A new program-manager group file will be created, with icons for Th
e
   Internet Phone and Help file

5. Double-click the Internet Phone icon.

6. The first time you run the Internet Phone Software, a Quick Tour wi
ll
   be suggested to you.

7. Start talking with the rest of the world!

About The Internet Phone and IRC

The Internet Phone uses the IRC to show the currently on-line user
s.
The actual talk is done directly between the PC's running the Intern
et
Phone, and NOT via the IRC.

Selecting an IRC server

In order to use the Internet Phone, you must be connected to an I
RC
server. It is best to select the one nearest to you, in order to g
et
the best connection.

Once you're connected to the IRC, you can call any other Internet Pho
ne
user that is connected to the IRC network. There is no need for bo
th
of you to use the same IRC server.

Please note that by "nearest" we mean over the net, but usual
ly
geographically close places have a better network connection.

The first time you connect, you can select a server from the Public
ly
Accessible Servers. It might not be the closest to you, but it wi
ll
enable you to start talking.

Later you can try and find a server better suited for you. Note th
at
many servers accept connections from specific areas. Some are limit
ed
to a country, some to a specific campus.

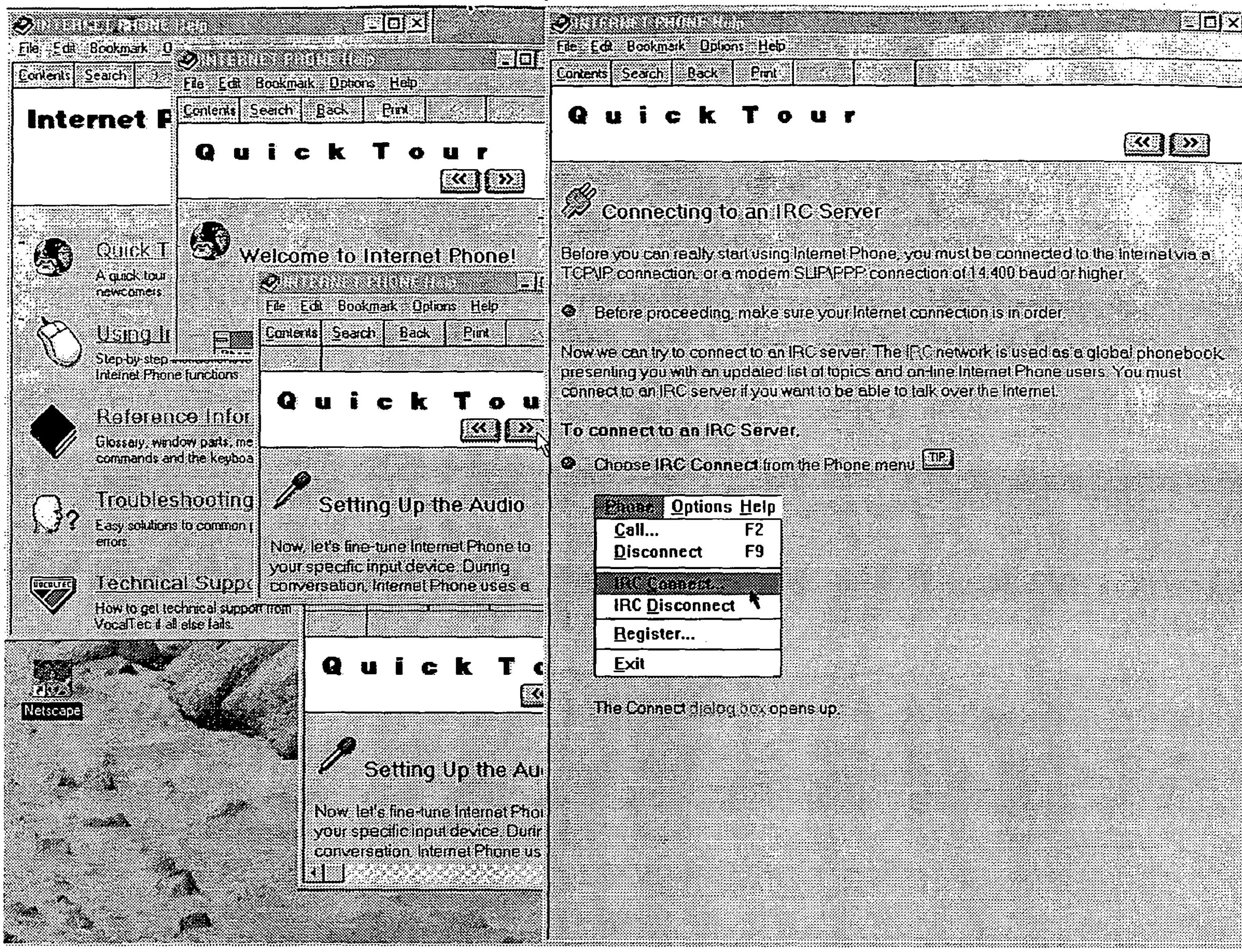
Technical Support

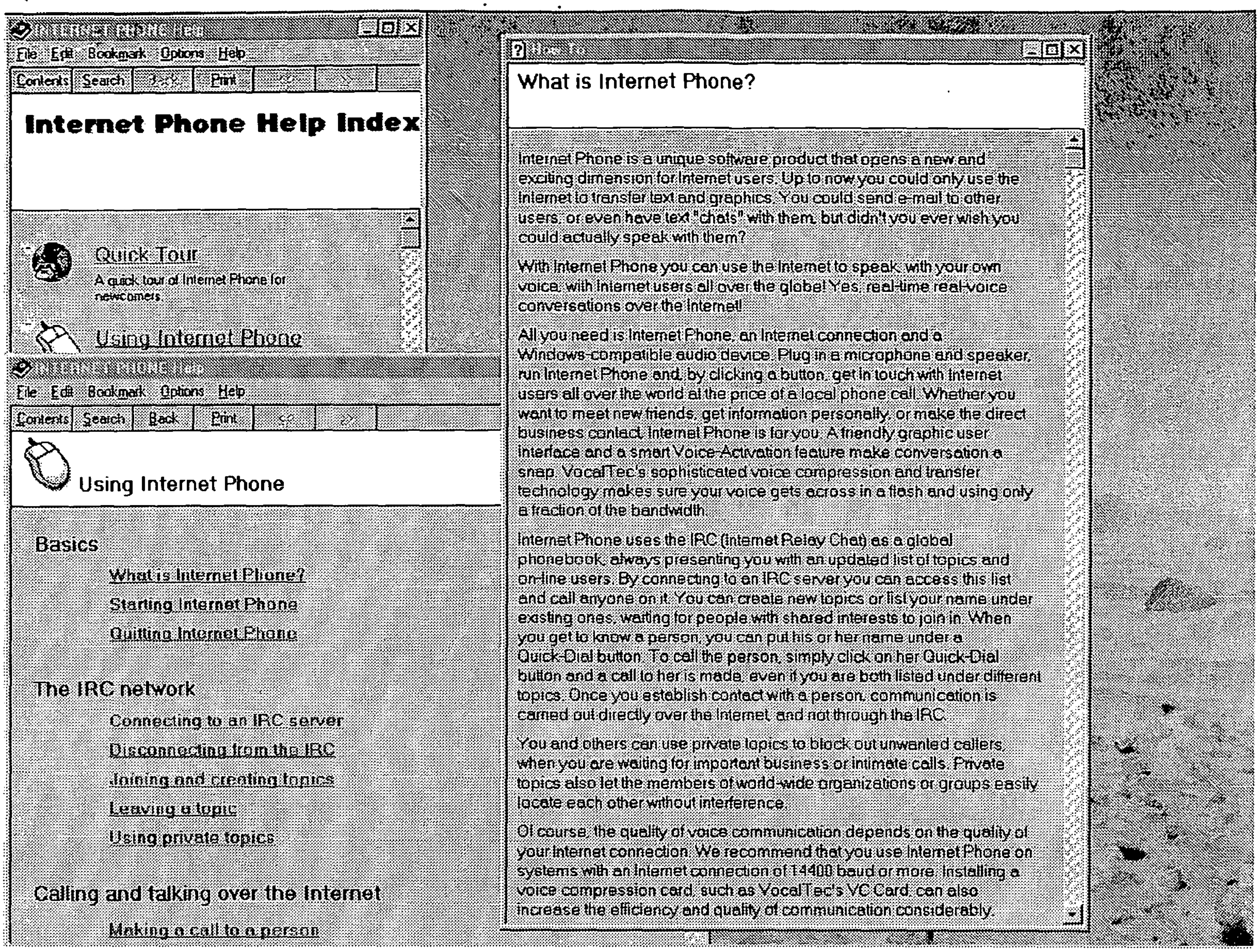
Before calling VocalTec for technical support, please do the following
:

1. Check the TroubleShooting from the Help menu in the Internet Phone.
   It contains a list of problems and solutions.

2. Select "Technical Support" from the Help menu for information on ho
w
   to contact VocalTec.

END of README.TXT


File Edit Bookmark Options Help
Contents Search Back Print
Quick Tour
Connecting to an IRC Server
Before you can really start using Internet Phone, you must be connected to the Internet via a TCP\IP connection, or a modem SLIP\PPP connection of 14,400 baud or higher.
Before proceeding, make sure your Internet connection is in order.
Now we can try to connect to an IRC server. The IRC network is used as a global phonebook presenting you with an updated list of topics and on-line Internet Phone users. You must connect to an IRC server if you want to be able to talk over the Internet.
To connect to an IRC Server.
Choose IRC Connect from the Phone menu. TIP
Phone Options Help
Call... F2
Disconnect F9
IRC Connect...
IRC Disconnect
Register...
Exit
The Connect dialog box opens up.
Internet P
Quick T
A quick tour newcomers
Using I
Step-by-step Internet Phone functions
Reference Infor
Glossary, window parts, me commands and the keyboa
Troubleshooting
Easy solutions to common errors
Technical Supp
How to get technical support from VocalTec if all else fails.
Welcome to Internet Phone!
Setting Up the Audio
Now, let's fine-tune Internet Phone to your specific input device. During conversation, Internet Phone uses a
Netscape



File Edit Bookmark Options Help

Contents Search Back Print << >>

Internet Phone Help Index

Quick Tour

A quick tour of Internet Phone for newcomers.

Using Internet Phone

File Edit Bookmark Options Help

Contents Search Back Print << >>

Using Internet Phone

Basics

What is Internet Phone?

Starting Internet Phone

Quitting Internet Phone

The IRC network

Connecting to an IRC server

Disconnecting from the IRC

Joining and creating topics

Leaving a topic

Using private topics

Calling and talking over the Internet

Making a call to a person

What is Internet Phone?

Internet Phone is a unique software product that opens a new and exciting dimension for Internet users. Up to now you could only use the Internet to transfer text and graphics. You could send e-mail to other users, or even have text "chats" with them, but didn't you ever wish you could actually speak with them?

With Internet Phone you can use the Internet to speak with your own voice with Internet users all over the globe! Yes, real-time real-voice conversations over the Internet!

All you need is Internet Phone, an Internet connection and a Windows-compatible audio device. Plug in a microphone and speaker, run Internet Phone and, by clicking a button, get in touch with Internet users all over the world at the price of a local phone call. Whether you want to meet new friends, get information personally, or make the direct business contact, Internet Phone is for you. A friendly graphic user interface and a smart Voice-Activation feature make conversation a snap. VocalTec's sophisticated voice compression and transfer technology makes sure your voice gets across in a flash and using only a fraction of the bandwidth.

Internet Phone uses the IRC (Internet Relay Chat) as a global phonebook, always presenting you with an updated list of topics and on-line users. By connecting to an IRC server you can access this list and call anyone on it. You can create new topics or list your name under existing ones, waiting for people with shared interests to join in. When you get to know a person, you can put his or her name under a Quick-Dial button. To call the person, simply click on her Quick-Dial button and a call to her is made, even if you are both listed under different topics. Once you establish contact with a person, communication is carried out directly over the Internet, and not through the IRC.

You and others can use private topics to block out unwanted callers, when you are waiting for important business or intimate calls. Private topics also let the members of world-wide organizations or groups easily locate each other without interference.

Of course, the quality of voice communication depends on the quality of your Internet connection. We recommend that you use Internet Phone on systems with an Internet connection of 14400 baud or more. Installing a voice compression card, such as VocalTec's VC Card, can also increase the efficiency and quality of communication considerably.

```
Domain Name: Q5.COM

Administrative Contact, Technical Contact, Zone Contact:
   Weinberg, Ed  (EW286)  edw@DETEL.COM
   203-333-3675
Billing Contact:
   Weinberg, Ed  (EW286)  edw@DETEL.COM
   203-333-3675

Record last updated on 19-Mar-98.
Record created on 22-Feb-96.
Database last updated on 19-Mar-98 04:11:09 EST.

Domain servers in listed order:

NS1.DETEL.COM                  165.254.238.145
NS1.GRANITECANYON.COM          205.166.226.34
NS2.GRANITECANYON.COM          208.146.254.90
NS1.RESEARCH.TROY.NY.US        206.72.196.240

 Enter a handle, name, mailbox, or other field, optionally preceded
 by a keyword, like "host diis".  Type "?" for short, 2-page
 details, "HELP" for full documentation, or hit RETURN to exit.
---> Do ^E to show search progress, ^G to abort a search or output <--
-
Whois:
```

Search | Post Message | My Deja News | Help

Article 5 of exactly 5

<< Previous Article | >> Next Article | Λ Current Results

- Help
- Author Profile
- View Thread
- Post New
- Post Reply
- Email Reply
- Bookmark
- Text Only

Subject: Re: Getting IP address of PPP-connected Mac
From: jgull@umich.edu (Jason Gull)
Date: 1995/04/03
Message-ID: <jgull-0304951005350001@pm012-11.dialip.mich.net>
Newsgroups: comp.sys.mac.comm

[Subscribe to comp.sys.mac.comm] New!

[More Headers]

Thanks for the advice. However, I'm already using MacTCPWatcher to find out *my own* IP address. It's trying to discover the IP addresses of other PPP users that is troubling me. So far the best "solution" seems to be a central location where I and my friends with whom I may wish to use Talk, NetPhone, etc. in the future can post our dynamic IPs each time we connect via PPP. Then other users can check that location and contact me.

I'm working on an AppleScript to do this. Any info, comments, advice would be appreciated. I'll post details here (and to my web page) if I ever get it going.

Jason Gull
jgull@umich.edu
http://www.umich.edu/~jgull/

In article <3lmrnv$igu@sct1.sct.fr>, Luc Saint-Elie
<lstelie@world-net.sct.fr> wrote:

> jgull@umich.edu (Jason Gull) wrote:
> >Is there *any* other way I can find out the IP address of a Mac connected
> >via MacPPP without asking the person using the machine on the other end?
> >I've tried making Talk requests to my friend's various email addresses, to
> >no avail. It just seems like the server has to have some way of figuring
> >out the address of a MacPPP-connected machine. Right? So is there any
> >way I can tap into that knowledge on the server?
>
> There are two ways (may be much more) to know that:
>
> 1- Simple way, use the "stats.." item in your ConfigPPP panel. On the
bottom right
> side of the display you will find your IP adress.

```
> 2- Best way : Use MacTCP Watcher (freeware from Peter Lewis), a really nice
> software allowing you to know EVREYTHING about your IP connection.
>
> Hope this helps

--
Jason Gull                    Liberty is always dangerous. But it is
jgull@umich.edu               the safest thing we have. - H.E.Fosdick
```

Article 8 of exactly 11

Subject: Re: Internet Phone for Mac?
From: jgull@umich.edu (Jason Gull)
Date: 1995/04/17
Message-ID: <jgull-1704950116450001@pm049-28.dialip.mich.net>
Newsgroups: comp.sys.mac.comm

[Subscribe to comp.sys.mac.comm] New!

[More Headers]

It's called **NetPhone**, and from all accounts, it's a lot better than Internet Phone (which uses an IRC **server**). **NetPhone** supports GSM (the compression scheme used by a lot of European and other cellular phones), which means it works fine over a 14.4 line, though GSM really requires a 25mhz 040 minimum.

The only problem for dial-up SLIP/PPP users is that to call, a caller needs to know the **IP address** of the receiver's machine, which changes all the time with most SLIP/PPP accounts. I've heard Internet Phone is trying to solve this using a dedicated IRC **server**. I've been trying to solve it with a script to write my current dial-up **address** to my web page, but it doesn't really work yet.

NetPhone is from emagic, and their web site is at
http://www.emagic.com
There you can download a demo version (outgoing calls limited to 90 seconds).

Jason Gull
jgull@umich.edu

In article <jazzbo-1604951234280001@onramp2-11.onr.com>, jazzbo@onr.com wrote:

> The latest issue of Wired had a blurb that said there was something akin
> to the Internet Phone available for Mac users. What is it and where can I
> get it??
>
> -Dave
>
> P.S. Have a nice day.
> --

```
> Have you ever gotten sick of hearing AT&T take credit for things that
they didn't invent?  You will.
>
>                                    -Dave Hamilton (jazzbo@onr.com)
```

<< Previous Article | >> Next Article | /\ Current Results

- Help
- Author Profile
- View Thread
- Post New
- Post Reply
- Email Reply
- Bookmark
- Text Only

IBM Technical Interchange '98 | Directories | Classifieds | Yellow Pages

About Deja News · New Users · Ad Info · Our Advertisers · How are we doing?
Home · Search · Post · My Deja News · Help

Power Search Results

11 Matches for search:

netphone ip address server [Find]

- Help
- Quick Search
- Interest Finder
- Browse Groups

	Date	Scr	Subject	Newsgroup	Author
1.	95/08/20	047	server addressed PPP account	comp.protocols.tcp-ip	Emilio C. Petri
2.	95/08/20	047	server addressed PPP account	comp.protocols.tcp-ip	Emilio C. Petri
3.	95/08/20	047	server addressed PPP account	comp.protocols.ppp	Emilio C. Petri
4.	95/08/20	047	server addressed PPP account	comp.sys.mac.comm	Emilio C. Petri
5.	95/08/21	046	Re: server addressed PPP acc	comp.sys.mac.comm	Clark Martin
6.	95/08/24	045	Re: Static vs. Dynamic IP ad	comp.sys.mac.comm	Dennis Wall
7.	95/06/28	043	PPP, Dynamic Addressing, & N	comp.sys.mac.comm	Jason Gull
8.	95/04/17	041	Re: Internet Phone for Mac?	comp.sys.mac.comm	Jason Gull
9.	95/04/03	041	Re: Getting IP address of PP	comp.sys.mac.comm	Jason Gull
10.	95/03/30	041	Re: Getting IP address of PP	comp.sys.mac.comm	Hao-lin Harry T
11.	95/07/10	034	Re: Eudora and Mailshare	comp.sys.mac.comm	T. Byfield

Individual word match counts (exact)

- address: 132081
- ip: 36509
- netphone: 225
- server: 164858

Introducing an easier way to read Usenet...
Click here for My Deja News.

Search Again: Power Search

Search for:

netphone ip address server [Find]

Example: ufo AND (sighting OR abduction OR alien)

- Help
- Quick Search
- Interest Finder
- Browse Groups

Archive: complete

Keywords matched: All

Number of matches: 25

Results format: Concise

Sorted by: Score

Group(s): comp.*

Example: alt.tv.x-files or *x-files*

Author(s):

Example: demos@dejanews.com

Subject(s):

Example: FAQ or (Frequently Asked Questions)

Date from: Jan 1 1990 **To:** Sept 12 1995

Example format: Apr 1 1997

IBM Technical Interchange '98 | Directories | Classifieds | Yellow Pages

About Deja News · New Users · Ad Info · Our Advertisers · How are we doing?
Home · Search · Post · My Deja News · Help

Netscape Conference and *CoolTalk* Meeting Room

Home
Register
Unregister
Talk Meeting Rm
Chat Rooms
Get Software
Errors / FAQ

- **Home School chat**
- **It's a BOY!** 3 12 10 1
- **Holocaust Remembrance Day Chat**

Welcome to the q5 Netscape Conference and CoolTalk® Meeting Room!
now with CHAT!
(We have **NO** connection to Netscape Communications Corporation.)

Bookmark this page. Other pages will change as this site improves!

A random user

See the people you talk to! Email us your GIF, JPEG, or BMP with a bio. No graphic? Snail mail us your picture and a bio and we will scan it in.

We have *Chat* and *Talk* meeting rooms.

Chat allows you to communicate either publicly or privately by typing to each other.

For *talk* you can use either CoolTalk or Netscape Conference.
First you register (it's free), then go to the Talk Meeting Room to see the list of people waiting for a call.
To call someone, press the *CoolTalk* ( ) or *Conference* ( ) icon next to their name.

For most of us, every time we log on to your Internet Service Provider you have a different IP address, so you must register here each time you log on to your Internet Service Provider.

Netscape Conference is a program in the suite *Netscape CommunicatorPreview Release*. You must choose to download:
"Netscape Communicator Preview Release - All Components plus Plug-ins" in order to get *Netscape Conference*.

There is a section of the Release notes which deals with Netscape Conference.

CoolTalk® is a plugin program for Netscape. It comes bundled with Netscape 3.0 and is available for many platforms including Windows 95, Windows NT, Windows 3.1, MacOS, SunOS, Solaris, HP-UX, Digital Unix, and IRIX.

If you are downloading Netscape, you must get the "plugin" version with a "P" in its name. When you select the "Desired Product:" make sure you select one which is called "standard plus components"
CoolTalk can also be downloaded from the Netscape FTP site.

MAC users *must* use a 28.8 or faster modem.

Check out the CoolTalk FAQ. It specifically addresses issues of compatable sound cards, upgrading to *Full Dupex*, and *MAC*.

We have NO connection with Netscape. While we may be able to answer simple questions, Netscape Technical Support is more knowledgable than us. **Send comments about this site to coolmaster@detel.com**

This site may be uncomprehendable without Netscape Navigator 3.0. Download Netscape Now

---

This site was created by:
Edward J. Weinberg webmaster@detel.com

Detel, Inc.
Suite 332
2490 Black Rock Tnpk
Fairfield, CT 06432

We can create one for you!

No programmers were harmed in the testing of this product.

Is your domain available?
Check out:
www.serverking.com

Home
Register
Unregister
Talk Meeting Rm
Chat Rooms
Get Software
Errors / FAQ

Talk Meeting Room

The list

Meet your friends

Visitors: 8888 19

The following people have indicated they are looking for someone to talk to using Netscape Conference or Cooltalk.

You have to press the "reload" button to see the latest list of names.

If you are waiting for a call...make sure Conference and/or Cooltalk is turned on!

To call someone, press the *CoolTalk* ( ) or *Conference* ( ) icon next to their name.

When people disconnect, they are not removed from this list, and if you disconnect and log in again you will probably have a different IP address.

While waiting for a call try our new Chat Room

Time/Date	Dial	Name/Email	City	St	Country
03/20 13:55 EST		Guenter Z.	Tacoma	WA	USA
		Kai, ruf nochmal durch!!!!!!!!!!!			
03/20 13:43 EST		LastNiceGuy	houston	tx	USA
		I'd like to try this anyone call me.			
03/20 13:35 EST		katherina		bc	canada
		waiting for last nice guy			
03/20 13:31 EST		Erin	York	PA	USA

03/20 13:20 EST		ROBNIEDSME	Tamarac	FL	USA
		USA			
03/20 13:11 EST		M. ANN		md	usa
		financial services,loans, maryland only.			
03/20 12:37 EST		Eglin M	Port Elizabeth		South Africa
		Let's talk			
03/20 12:27 EST		Rik	vitoria	ES	Brasil
		USA			
03/20 12:26 EST		Maximo	Roma		Italia
		italian			
03/20 12:04 EST		peter	montreal	que	Canada
03/20 12:01 EST		Kai Schütrumpf	Friedewald	Hessen	Germany
		Please only for Guenter!!!			
03/20 12:01 EST		ROCAL	Rochester	IN	USA
		KA9YQM			
03/20 11:03 EST		tinkoo	MUMBAI	MH	INDIA
		i can receive calls but can't call up...			
03/20 11:01 EST		Armando Gonzalez	Caracas	DF	Venezuela
		USA			
03/20 10:58 EST		ARCH-Snd Questions	will snd answer	Fl	U.S.A.
		NetConf & CT works send e-mail for info			
03/20 10:50 EST		perfect_			
		hi			
03/20 10:45 EST		Zaxxon	statesville	NC	USA
03/20 10:35 EST		bob	ellenton	fl	usa
		USA			
03/20 10:09 EST		Don	Morristown	NJ	
		My E-Mail is: Don0453@AOL.COM			
03/20 09:22 EST		hema	mumbai		india
		just testing			

03/20 09:14 EST	Daniel	vic		aust	USA
03/20 09:12 EST	Corinne			Singapore	Looking for DANIEL dear....
03/20 07:05 EST	TAZZ	Newnan	GA	USA	USA
03/20 06:52 EST	LK	Russellville	AR	USA	USA
03/20 06:38 EST	cjay	melbourne	vic	australia	waiting for mates
03/20 06:26 EST	Tbone	okinawa	ap	japan	
03/20 04:44 EST	Aleksander	San Fran	CA	ICQ#8336177	Hey any nasty ladies out there?...M25
03/20 03:29 EST	KRISHY			Malaysia	USA
03/20 02:22 EST	Lacie	Jacksonville	FL	USA	Waiting for Dave
03/20 02:22 EST	Davester	Phoenix	AZ	US	Lacie.......

Home | Add your IP

BRIAN'S MINDY McCREADY GALLERY

LinkExchange Member

Register your IP address "telephone number" for Netscape Conference and/or CoolTalk

This will add your *current* IP address and other information to the contact list.
Since your IP address will change each time you log on, you must register each time you log on.

The following information is optional, but including it will improve the chances that someone will talk to you.
Including your email address will put you on our mailing lists for updates to this site.

Register me for:
- [x] CoolTalk
- [ ] Netscape Conference

Name or Nick:	tgif
E-Mail:	george.wallace@uspto.gov
City:	arlington
State:	va
Country:	USA
Comment:	checking out the site

- [x] Remember this information so I do not have to enter it again!

Submit IP * Reset

Your IP address is: 151.200.96.2.

Home | View Submitted IPs

Cisco - Exhibit 1002 - Page 146

look for all the words

"Internet Phone" SEARCH

Before: April 1, 1995

NEW SEARCH REVISE SEARCH

Returned: 226 matches.

Breakdown: internet: 11672334, phone: 6326171 71 - 80

The Web
Usenet
Top News Sites
Businesses
People
Email Addresses
Classifieds
Domain Names
Stocks
Discussion Groups
ShareWare

71. C&I 514 Web

91% Language Arts Web Back to Student Web Welcome to C&I 514 Language Arts Web Mexican Culture Server It has Mexican recipes,songs, flags, and artists. All is in Spanish. Margaret Bruha Foreign Languages and Culture Web references The site contains a...
http://www.cae.wisc.edu/~tojek/514language.html, 5567 bytes, 08Mar95

72. Jo's Homepage

91% Jo's Bookmarks These are some of the resources that a typical K12 teacher found on the Internet: White House Tour Index - NMAA/WHC National Museum of American Art home page Adrien Rothschild - NMAA/WHC http://www.nmaa.si.edu/whc/whcgifs...
http://www.vt.com/edu/jobook.html, 13996 bytes, 20Jun94

73. Electronic Retail

91% From : David Rich, sasha@ozemail.com.au On : Thu Mar 2 06:54:37 EST 1995 In reponse to why consumers may be going off buying over the internet: Most consumers are not yet on the net. Most people do not understand what the net is, nor how it works..
http://cism.bus.utexas.edu/issues/issue2/comment11.html, 2997 bytes, 05Mar95

74. March Archives: Re: 28.8 not all that bad

91% Re: 28.8 not all that bad David Winet (dwinet@qal.berkeley.edu) Tue, 14 Mar 1995 06:40:56 -0800 (PST) Messages sorted by: [date][thread][subject][author] Next message: Roie Gat: "Re: 28.8 not all that bad" Previous message: Larry Chace: ...
http://www.indstate.edu/CU-SeeMe/devl_archives/mar_95/0259.html, 3587 bytes, 02Apr95

75. The Web Untangled

91% Introduction Known as WWW or just the Web, the World Wide Web is more a concept than a specific protocol. The Web provides computer users on the Internet with a consistent means of access to a variety of media in a simplified fashion. Access is via.
http://wvnvaxa.wvnet.edu/~roman/UNTANGLED.html, 3220 bytes, 06Jan95

76. March Archives: Re: 28.8 not all that bad

90% Re: 28.8 not all that bad rravindr@INDYVAX.IUPUI.EDU Tue, 14 Mar 1995 15:13:30 -0500 Messages sorted by: [date][thread][subject][author] Next message: Jesus Arango: "cu-seeme & iphone conference" Previous message: Dan Berrios: "Timing out..
http://www.indstate.edu/CU-SeeMe/devl_archives/mar_95/0270.html, 4071 bytes, 02Apr95

77. Hendry's first home page

90% Hendry's Homepage Hot ! Add you page here! This page is best viewed with Netscape Navigator. Download Let's Surf Cool Sites Games HK Stuffs Resources Dictionary Museums Movies, TV Softwares, Icons Download Autos News, Magazines, Computer paper What.
http://www.smart.is/link4/LINK5.HTM, 16131 bytes, 01Jan94

78. NIC-News Newsletters: NIC Newsletter v 5.10

90% NIC Newsletter v 5.10 Sheryl Erez (erez@cac.washington.edu) Tue, 23 Mar 1993 15:32:46 -0800 (PST) == || Networks & Distributed Computing || NIC - NEWS || == -- | An update on network resources for NDC staff | | Volume 5, Issue 10 Edited by Sheryl...
http://www.washington.edu/nic-news/old/text/0053.html, 7486 bytes, 06Jan95

79. (http://www.cox.smu.edu/class/mis6386/people/stort/iphone.html)

90% The Internet Phone The IPHONE is a cool program to "telephone" worldwide using the Internet. System Requirements: 386 CPU or higher Windows 3.1 or later A Sound Blaster (compatible) sound card Speakers Microphone Internet Access (SLIP, e.g. PICnet..
http://www.cox.smu.edu/class/mis6386/people/stort/iphone.html, 1841 bytes, 30Mar95

80. Spock's Other Raging Slab of Meat

90% The PolySpock Project BBS PolySpock is the direct and spiritual successor to Rathead Systems. PSP was started on a crazy whim one day by RatSnatcher and his roommate from Ohio, Special Ed (aka Gar, Adam Capell) while they were trying to figure out..
http://www.arlington.com/~tjames/pig/pspock2.html, 4992 bytes, 15Mar95

Breakdown: internet: 11672334, phone: 6326171 71 - 80

GAU 2751.

#4
4/16/98

OIPE JC44
MAR 30 1998
PATENT & TRADEMARK OFFICE

ATTORNEY'S DOCKET NO.:N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Shane D. Mattaway et al.
SERIAL NO.: 08/721,316
FILED: September 25, 1995
FOR: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
EXAMINER: --
ART UNIT: --

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 25th day of March, 1998.

Rivki Cohen

Rivki Cohen

Assistant Commissioner for Patents
Washington, DC 20231

RECEIVED
APR -2 98
GROUP 2600

Sir:

Transmitted herewith for filing is/are the following document(s):

[X] Information Disclosure Statement
[X] PTO Form 1449 and references cited

If the enclosed papers are considered incomplete, the Mail Room and/or the Application Branch is respectfully requested to contact the undersigned collect at (617) 367-4600, Boston, Massachusetts.

No fee is being submitted. If any fee is required, the balance may be charged to the account of the undersigned, Deposit Account No. 02-3038. A duplicate of this sheet is enclosed.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse, Esq.
Reg. No.: 33,518
KUDIRKA & JOBSE, LLP
One Beacon Street
Boston, Massachusetts 02108
Tel.: (617) 367-4600

ATTORNEY DOCKET NO.: **N0003/7002**
DATE: March 25, 1998
NDD
H:\BDJ\N0003\7002\IDS2TRAN.WPD

OIPE JC44
MAR 3 0 1998
PATENT & TRADEMARK OFFICE

ATTORNEY'S DOCKET NO.: N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Shane D. Mattaway et al.
Serial No.:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	
Art Unit:	

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 25th day of March, 1998.

Rivki Cohen

Rivki Cohen

Box DD
Assistant Commissioner for Patents
United States Patent and Trademark Office
Washington, DC 20231

RECEIVED
APR -2 98
GROUP 2600

STATEMENT FILED PURSUANT TO THE DUTY OF
<u>DISCLOSURE UNDER 37 C.F.R. §§1.56, 1.97 AND 1.98</u>

Sir:

Pursuant to the duty of disclosure under 37 C.F.R. §§1.56, 1.97 and 1.98, the applicant requests consideration of this information disclosure statement.

Compliance with 37 C.F.R. §1.97

This information disclosure statement has been filed before the mailing date of a first office action on the merits in the above-identified application.

No fee or certification is required.

Information Cited

The applicant hereby makes of record in the above-identified application the information listed on the attached form PTO-1449 (modified). The order of presentation of the references should not be construed as an indication of the relative importance of the references.

Remarks

A copy of each of the above-identified information is enclosed unless otherwise indicated on the attached form PTO-1449 (modified). It is respectfully requested that:

- The examiner consider completely the cited information, along with any other information, in reaching a determination concerning the patentability of the present claims;
- The enclosed form PTO-1449 be signed by the examiner to evidence that the cited information has been fully considered by the Patent and Trademark Office during the examination of this application;
- The citations for the information be printed on any patent which issues from this application.

By submitting this information disclosure statement, the applicant makes no representation that a search has been performed, of the extent of any search performed, or that more relevant information does not exist.

By submitting this information disclosure statement, the applicant makes no representation that the information cited in the statement is, or is considered to be, material to patentability as defined in 37 C.F.R. §1.56(b).

By submitting this information disclosure statement, the applicant makes no representation that the information cited in the statement is, or is considered to be, in fact, prior art as defined by 35 U.S.C. §102.

It is understood by applicant that the foregoing information will be considered and, to the extent deemed appropriate by the examiner, will be reflected in the examiner's communication.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse, Esq.
Reg. No. 33,518
KUDIRKA & JOBSE, LLP
One Beacon Street
Boston, Massachusetts 02108
Tel: (617) 367-4600
Attorneys for Applicant

Docket No.: N0003/7002

Date: March 25, 1998

H:\BDJ\N0003\7002\IDS2.WPD

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 556 012 A2**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number : **93300919.3**

(22) Date of filing : **09.02.93**

(51) Int. Cl.^{5} : **H04Q 7/00**, H04L 12/56

(30) Priority : **10.02.92 JP 23506/92**
16.09.92 JP 246855/92
10.11.92 JP 299531/92

(43) Date of publication of application :
18.08.93 Bulletin 93/33

(84) Designated Contracting States :
DE FR GB

(71) Applicant : **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
1006, Kadoma
Kadoma-shi, Osaka-fu 571 (JP)

(72) Inventor : **Wada, Hiromi**
15-10, Higashigaoka, Uzumasa
Neyagawa-shi, Osaka 572 (JP)
Inventor : **Yozawa, Takashi**
5-16-19, Shinke, Aoo
Mino-shi, Osaka 562 (JP)
Inventor : **Ohnishi, Tatsuya**
281-5, Kawahara, Aza, Sasabe
Kawanishi-shi, Hyogo 666-01 (JP)

(74) Representative : **Cummings, Sean Patrick et al**
David Keltie Associates Audrey House Ely Place
London EC1N 6SN (GB)

(54) **Migration communication control device.**

(57) Disclosed is a migration communication control device constructed to control a continuous communication between a mobile node and a node unaffected the mobile node's migration. The migration communication control device comprises a first migration control unit, a second migration control unit on the mobile node, and a third migration control unit on the partner node. The first migration control unit comprises a packet transfer unit and an address post unit. The packet transfer unit receives a packet which was destined for an outdated address of the mobile node, generates a conversion packet which holds an updated address instead of the outdated address, and then transmits the conversion packet, while an address post unit transmits an address post message which indicates the updated address to the third migration control unit. The second migration control unit comprises a migration post unit and a packet resumption unit. The migration post unit transmits to the first migration control unit a migration post message which indicates the updated address when the mobile node migrates to another network while a packet resumption unit receives the conversion packet from both the first migration control unit and the third migration control unit and resumes an original packet from the conversion packet. The third migration control unit comprises a packet conversion unit which converts a destination address of a packet into the updated address, then transmits it to the mobile node.

EP 0 556 012 A2

Jouve, 18, rue Saint-Denis, 75001 PARIS

BACKGROUND OF THE INVENTION

(1) Field of the Invention

The present invention relates to a migration communication control device that controls a communication between a mobile node and a corresponding node to enable them to communicate continuously when the former migrates by managing addresses assigned to the former each time it migrates across networks.

(2) Description of the Related Art

Recent progress in the field of electronic technology makes it possible to assemble smaller and lighter portable computers. These portable computers referred to as mobile nodes are designed so that they can migrate across networks: they are unplugged from a network and plugged in another and communicate with a stationary node. Thus, each of them is assigned a specific address to prove its identity. The address, in general, includes location information as to which network the mobile nodes are currently plugged in, and for this reason, a new address is assigned each time they migrate.

For example, the address composed of a network address unit for specifying a network in which the mobile node is currently plugged in and a node address unit for proving the mobile node's identity in the network, or the address used in a conventional network architecture such as Internet Protocol(details of which are in Internet Protocol, RFC791, Jon Postel, Sep., 1981), they must be changed every time the mobile nodes migrate.

However, once the mobile node migrates to another network, a communication with the stationary node will be terminated. This is because a packet is transmitted to its old address only to be wasted.

Thus, to enable the mobile node and stationary node to communicate continuously when the former migrates, it is necessary to control the communication by managing the steadily changing address.

To date, two address managing methods have been proposed: one by Sony Computer Science Laboratory Inc. and one by the Department of Computer Science at Columbia University.

Sony Computer Science Laboratory Inc. proposed a method using VIP(Virtual Internet Protocol), details of which are on "VIP : Lower Layer Internet Protocol", Fumio Teraoka, Yasuhiko Yokote, Mario Tokoro, Proceed of Data Processing Convention : Multimedia Communication and Distributed Processing.

In this method, each mobile node is assigned a VIP(Virtual Internet Protocol) address and a PIP(Physical Internet Protocol) address. The former is an unchanged address used in a communication application for packet transmission and reception; and the latter is an address changed for every migration to specify an update physical location of the mobil node. Data related to both addresses are held in a cache of a gateway. Under these conditions, the stationary node transmits a packet to the mobile node to the VIP address thereof, and the packet is converted into another packet addressed to the PIP address when it passes the gateway, thence transmitted to the mobile node via the gateways placed in a route onwards. These gateways collect data related to a correlation between the VIP and PIP addresses from the header of the packet upon the receipt thereof, thus updates data in the cache, and hence are able to convert other packets addressed to the VIP addresses into the packets addressed to the PIP addresses based on the correlation entered in the cache.

In this method, in short, the use of the address constituting with the VIP and PIP addresses enables the mobile node and the stationary node to communicate continuously when the former migrates.

The Department of Computer Science at Columbia University proposed a method using an Internet Protocol address of which network address unit does not specify the network which the mobile node is currently plugged in but declares itself to be the mobile node, hence a certain value is given as the network address unit to all the mobile nodes. As well, the method uses an MSS(Mobile Support Station) installed at each network to manage the IP addresses and control a packet route to the mobile node. The MSS is designed so that it collects data related to the update physical location of the mobile nodes by referring other MSSs.

Given these conditions, when the stationary node transmits a packet to the mobile node when it migrates, it first transmits the packet to a first MSS installed in its network; thence the first MSS transfers the packet to a second MSS installed in a network which the mobile node is currently plugged in; and finally the second MSS transfers the packet to the mobile node.

In this method, in short, the use of the MSS enables the mobile node and the stationary node to continue the communication when the former migrates.

In the first method, however, all the nodes must be constructed so that they understand both the VIP and PIP addresses, causing them to extend a scale functionally, otherwise making it impossible to apply this method to apparatuses employed in existing networks. In addition, the communication via the gateways reduces communication efficiency compared with direct packet transmission, because the gateways check whether they have received the packet addressed to the VIP address or PIP address each time they receive it, as well as whether or not to collect the data therefrom to update those in the cache.

In the second method, each network must have the MSS, and the communication via the MSSs makes it impossible to transmit the packet directly, thereby reducing the communication efficiency.

SUMMARY OF THE INVENTION

The present invention therefore has an object to provide a migration communication control device that is available to any apparatus employed in existing networks. Also the present invention has another object to provide a migration communication control device that enables the mobile node and stationary node to communicate continuously when the former migrates by transmitting and receiving the packet directly besides transferring the packet as has been done when the mobile node migrates across the networks.

The above objects are fulfilled by a migration communication control device constructed to control a communication between a mobile node and a partner node, the mobile node migrating across networks and obtaining an address assigned on each network while the partner node being a communication partner of the mobile node, comprising a first migration control unit, a second migration control unit, a third migration control unit, the second migration control unit being placed on the mobile node and the third migration control unit being placed on the partner node, wherein the first migration control unit comprises a packet transfer unit for receiving a packet which was destined for an outdated address of the mobile node, the outdated address assigned when the mobile node migrated to a network to which the first migration control unit is attached, generating a conversion packet which holds an updated address instead of the outdated address, and transmitting the conversion packet; and an address post unit for transmitting an address post message which indicates the updated address of the mobile node to the third migration control unit, the third migration control unit transmitting the packet received by the packet transfer unit, and the second migration control unit comprises a migration post unit for transmitting to the first migration control unit a migration post message which indicates the updated address of the mobile node when the mobile node migrates to another network; and a packet resumption unit for receiving the conversion packet from both the first migration control unit and the third migration control unit and resuming an original packet from the conversion packet, and the third migration control unit comprises a packet conversion unit for converting a destination address of a packet, the packet to be transmitted to the mobile node, into the updated address indicated by the address post message, the address post message sent by the first migration control unit, and transmitting it to the mobile node.

The migration post unit in the second migration control unit may transmit an identification key included in the migration post message, the identification key being employed to identify the mobile node.

The identification key may be an address of the mobile node assigned at one network before the network to which the mobile node is currently attached.

The identification key may be an address of the mobile node assigned before its initial migration.

The second migration control unit may be constructed to transmit to the third migration control unit the packet which has the same format as the resumed packet.

The first migration control unit may further comprise an address hold unit for holding the outdated address and the updated address by corresponding them with each other; and an address comparison unit for comparing the destination address of the received packet with the outdated address, wherein the packet transfer unit generates the conversion packet and transmits it when the address comparison unit detects that the destination address of the received packet coincides with the outdated address.

The first migration control unit may further comprise an address hold unit for holding the outdated address and the updated address by corresponding them with each other; and an address comparison unit for comparing the destination address of the packet received by the packet transfer unit with the outdated address, wherein the address post unit transmits the address post message which indicates the updated address of the mobile node to the third migration control unit, the third migration control unit transmitting the packet received by the packet transfer unit, when the address comparison unit detects that the destination address of the packet coincides with the outdated address.

The second migration control unit may further comprise an address hold unit for holding the outdated address and the updated address by corresponding them with each other; and an address comparison unit for comparing the updated address with the destination address of the packet received from one of the first migration control unit and the third migration control unit, wherein the packet resumption unit resumes the original packet from the conversion packet when the address comparison unit detects that the updated address coincides with the destination address of the packet received from one of the first migration control unit and the third migration control unit.

The third migration control unit may further comprise an address hold unit for holding the outdated address and the updated address of the mobile node by corresponding them with each other; and an address comparison unit for comparing the outdated address in the address hold unit with the destination address of the packet to be transmitted to the mobile node, wherein the packet conversion unit converts the destination address of the packet to be transmitted to the mobile node into the updated address which corresponds to the outdated address in the address hold unit when the address comparison unit detects the outdated address in the address hold unit coincides with the destination address of the packet.

There may be a plurality of the first migration control units, and the second migration control unit transmits the migration post message to at least one of the first migration control units.

The migration post unit in the second migration control unit may transmit the migration post message to the first migration control unit which is attached to the network to which the mobile node was attached before its migration, each of the first migration control units has a migration post unit for transmitting to one of the other first migration control units a migration post message to post the same address as the updated address indicated by the migration post message received from the second migration control unit, and each of the first migration control units has a migration post unit for transmitting a migration post message from one of the other first migration control units to another first migration control unit to post the same address as the updated address indicated by the received migration post message.

Each of the first migration control units and the second migration control unit may further comprise a pointer hold unit for holding pointers related to the first migration control unit to which the migration post message is transmitted, and wherein the migration post unit in each of the first migration control units and the migration post unit in the second migration control unit transmit the migration post message to each of the addresses related to each of the pointers.

Each of the pointers may be a broadcast address of the network to which one of the first migration control units is attached.

Each of the pointers may be an address which is assigned to one of the first migration control units uniquely.

Each of the pointers may be the address of the mobile node which is assigned when the mobile node is attached to the same network as is the first migration control unit, and the migration post unit in the first migration control unit and the migration post unit in the second migration control unit obtain the broadcast address of the network to which each of the first migration control units is attached with referring to the address of the mobile node, and transmits the migration post message to the obtained broadcast address.

The pointer hold unit in the second migration control unit may hold a pointer related to a first migration control unit for the latest migration, which is the first migration control unit being attached to one network before the network to which the mobile node is currently attached, and the pointer hold unit in the first migration control unit holds a pointer related to another first migration control unit attached to the same network as was the mobile node attached before migrating to the network to which the first migration control unit is attached.

The second migration control unit may further transmit to the first migration control unit the pointer by sending thereto the migration post message, the pointer to be held by the first migration control unit.

The first migration control unit may store into the pointer hold unit the pointer when it receives from the second migration control unit the migration post message by corresponding the pointer with the updated address indicated by the received migration post message.

Each of the first migration control units may further comprise an address hold unit for holding the outdated address and the updated address by corresponding them with each other, wherein a migration post message unit stores into the address hold unit the outdated address and the updated address by corresponding them with each other when it receives from the second migration control unit the migration post message, while converts the updated address in the address hold unit into the updated address indicated by the migration post message when it receives from the first migration control unit the migration post message and the outdated address indicated by the migration post message coincides with one of the updated addresses in the address hold unit.

The first migration control unit may be placed on a gateway, which connects networks.

The first migration control unit may be placed on the network as an individual node.

The migration post unit in the second migration control unit may transmit the migration post message to a home migration control unit, the home migration control unit being the first migration control unit which is attached to a network where the mobile node left for its initial migration, and the home migration control unit may further comprise a home migration post unit for transmitting a migration post message to a first migration control unit for the latest migration, the first migration control unit for the latest migration being the first migration control unit which is attached to the network where the mobile node left for the latest migration, to post the same updated address as is indicated by the migration post message received from the second migration control unit.

The first migration control unit may further comprise a migration post unit for transmitting the migration post message indicating the updated address of the mobile node to one of the other first migration control units when the conversion.packet destined for the outdated address of the mobile node was sent therefrom to the first migration control unit.

The migration post unit in the second migration control unit may transmit to the home migration control unit the migration post message where a home address and the updated address are corresponded with each other, the home address assigned when the mobile node is attached to the same network as is the home migration control unit, and each of the packet transfer unit and the address post unit in the home migration control unit may transmit the conversion packet and the address post message respectively with referring to the above home address and the updated address.

The second migration control unit may further comprise an outdated address post unit for transmitting to the first migration control unit for the latest migration an outdated address post message where the outdated address and the home address are corresponded with each other, the outdated address being assigned to the mobile node before the latest migration, the home migration post unit in the home migration control unit may transmit to the said first migration control unit for the latest migration the migration post message where the above home address and the updated address are corresponded with each other, and the packet transfer unit and the address post unit in the first migration control unit for the latest migration may transmit the conversion packet and the address post message respectively in accordance with the outdated address and the updated address, the outdated address and the updated address being corresponded with each other via the home address.

The outdated address post unit in the second migration control unit may transmit the above outdated address post message at a migration of the mobile node preceding the latest migration, and each of the migration post units in the second migration control unit and the home migration post unit in the home migration control unit may transmit the above migration post message at the latest migration of the mobile node.

The second migration control unit may further comprise a home migration control unit pointer hold unit for holding a pointer related to the home migration control unit, the migration post unit in the second migration control unit transmits the migration post message to the address related to the pointer, the home migration control unit may further comprise a pointer hold unit for the latest migration for holding a pointer related to the first migration control unit for the latest migration, and the home migration post unit in the home migration control unit may transmit the migration post message to the address related to the pointer.

Each of the above pointers may be the broadcast address of the network to which each of the first migration control units is attached.

Each of the above pointers may be the address assigned to each of the first migration control units uniquely.

The second migration control unit may further comprise a pointer obtainment unit for requesting to the first migration control unit for the latest migration the pointer related to the first migration control unit for the latest migration, and the migration post unit in the second migration control unit may post the obtained pointer to the home migration control unit together with the updated address by sending thereto the migration post message.

The migration post unit in the second migration control unit may post to the home migration control unit the pointer at the migration of the mobile node preceding the latest migration, while the migration post unit may post the above updated address at the latest migration of the mobile node.

The first migration control unit may further comprise an address post suppressing unit for suppressing transmission of the address post message from the address post unit to the third migration control unit, and the address post suppressing unit may suppress transmission of the address post message when none of the first migration control units is attached to the same network as is the mobile node.

The second migration control unit may further comprise a detect unit for detecting whether or not the first migration control unit is attached to the network to which the mobile node migrates, the migration post unit in the second migration control unit may transmit to the home migration control unit the migration post message which includes the detecting result of the above detect unit together with the updated address, the home migration post unit in the home migration control unit may transmit to the first migration control unit for the latest migration the migration post message which includes the detecting result of the above detect unit together with the updated address, and the address post suppressing unit in each of the home migration control unit and the first migration control unit for the latest migration may suppress the transmission of the address post message in accordance with the detecting result of the above detect unit.

The first migration control unit may further comprise a packet transfer suppressing unit for suppressing transfer of the packet conducted by the packet transfer unit.

The first migration control unit may further comprise an address post suppressing unit for suppressing transmission of the address post message from the address post unit to the third migration control unit, and the address post suppressing unit in the first migration control unit being attached to a network to which the mobile node is not attached, may suppress the transmission of the address post message when the packet transfer suppressing unit in the first migration control unit for the latest migration suppresses transfer of the packet.

The second migration control unit may further comprise a detect unit for detecting whether or not the packet transfer suppressing unit in the first migration control unit suppresses the transfer of the packet, the first migration control unit being attached to the network to which the mobile node migrates, and the migration post unit in the second migration control unit transmits to the home migration control unit the migration post message which includes the detecting result of the above detect unit together with the updated address, the home migration post unit in the home migration control unit may transmit to the first migration control unit for the latest migration the migration post message which includes the detecting result of the detect unit together with the updated address, and the address post suppressing unit in each of the home migration control unit and the first migration control unit for the latest migration may suppress the transmission of the address post message in accordance with the detecting result of the above detect unit.

The packet transfer suppressing unit in the first migration control unit for the latest migration may suppress the transfer of the packet conducted by the packet transfer unit, when the packet transfer suppressing unit in the first migration control unit being attached to the network to which the mobile node migrates suppresses the transfer of the packet.

The above objects may also be fulfilled by a packet transfer migration control unit in a migration communication control device, the migration communication control device being constructed to control a communication between a mobile node and a partner node, the mobile node migrating across networks and obtaining an address assigned on each network while the partner node being a communication partner of the mobile node, comprising a packet transfer unit for receiving a packet which was transmitted by the partner node to an outdated address of the mobile node, the outdated address being assigned when the mobile node migrated to a network to which the packet transfer migration control unit is attached, generating a conversion packet which holds an updated address instead of the outdated address, and transmitting the conversion packet; and an address post unit for transmitting an address post message which indicates the updated address of the mobile node to the partner node, the partner node transmitting the packet received by the packet transfer unit.

The above objects may further be fulfilled by a mobile node migration control unit in a migration communication control device, the migration communication control device being constructed to control a communication between a mobile node which migrates across networks and obtains an address assigned on each network and a partner node which is a communication partner of the mobile node, being placed on the mobile node and comprising a migration post unit for transmitting to a packet transfer migration control unit a migration post message which indicates an updated address of the mobile node when the mobile node migrates to another network, the packet transfer migration control unit for receiving a packet which was transmitted by the partner node to an outdated address of the mobile node, the outdated address assigned when the mobile node migrated to a network to which the migration control unit for packet transfer is attached, generating a conversion packet which holds the updated address instead of the outdated address, and transmitting the conversion packet; and a packet resumption unit for receiving the conversion packet from both the packet transfer migration control unit and the mobile node, and resuming an original packet from the conversion packet.

The above objects are finally fulfilled by a partner node migration control unit in a migration communication control device, the migration communication control device being constructed to control a communication between a mobile node which migrates across networks and obtains an address assigned on each network and a partner node which is a communication partner of the mobile node, being placed on the mobile node and comprising an address post message receiving unit for receiving an address post message which indicates an updated address of the mobile node from a packet transfer migration control unit, the packet transfer migration control unit transmitting an address post message which indicates the updated address of the mobile node to the partner node; and a packet conversion unit for converting a destination address of a packet, the packet to be transmitted to the mobile node, into the updated address indicated by the address post message, and transmitting it to the mobile node.

According to the above construction, the migration communication control device of the present invention transfers and converts the packet using the address assigned to the mobile node each time it migrates across networks, obviating particular addresses or devices such as the VIP address used conventionally. For this reason, the migration communication control device of the present invention can be applied to the existing partner node and mobile node so that they can communicate continuously by transferring the packet. Moreover, it is advantageous that the migration communication control device of the present invention is not necessarily applied to all the nodes to enhance communication efficiency; the present invention can be applied only to where necessary on the existing networks. More precisely, when any existing partner node communicates with the mobile node when it migrates, the packet can be transmitted directly from the mobile nodes to the existing partner node; and it can be transferred via the first migration control unit from the existing partner node to the mobile node, thereby enhancing communication efficiency.

Furthermore, when the partner node employs the migration communication control device of the present invention, communication efficiency is further enhanced thanks to the direct packet transmission and reception made possible by posting the update address of the mobile node from the first migration control unit to the third migration control unit.

Also, the devices such as MSS or a gateway employing the VIP are not necessarily installed at every network to which the mobile node migrates. To be precise, according to the present invention, the continuous communication is implemented even when the mobile node migrates to a network at which no special devices including above ones are installed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and the other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings which illustrate a specific embodiment of the invention. In the drawings:

FIG. 1 is a block diagram depicting a construction of a migration communication control device in a first embodiment of the present invention;

FIG. 2 is a block diagram depicting a detailed construction of the migration communication control device employed as a mobile node in the first embodiment of the present invention;

FIG. 3 is a block diagram depicting a detailed construction of the migration communication control device employed as a gateway in the first embodiment of the present invention;

FIG. 4 is a block diagram showing a detailed construction of the migration communication control device employed as a stationary node in the first embodiment of the present invention;

FIG. 5 is a block diagram showing a detailed construction of the migration communication control device employed as an individual node in the first embodiment of the present invention;

FIG. 6 is an illustration showing a first example of a network to which the migration communication control devices in FIG. 2, 3, 4 are attached;

FIG. 7 is an illustration showing a second example of the network to which the migration communication control devices in FIG. 2, 3, 4 are attached;

FIG. 8 is an illustration showing a third example of the network to which the migration communication control devices in FIG. 2, 3, 4 are attached;

FIG. 9 is an illustration showing a fourth example of the network to which the migration communication control devices in FIG. 2, 3, 4 are attached;

FIG. 10 is an illustration showing (a) data in a data hold unit 1 in the mobile node (b) data in a data hold unit 1 in the migration communication control devices each employed as the gateway, the stationary node, and the individual node.

FIG. 11 is an illustration showing a format of a packet in the first embodiment of the present invention;

FIG. 12 is an illustration showing a format of a packet in the first embodiment of the present invention;

FIG. 13 is an illustration showing a content of the data hold unit 1 in the migration communication control device employed as the gateway;

FIG. 14 is an illustration showing a content of the data hold unit 1 in the migration communication control device employed as the individual node;

FIG. 15 is an illustration showing an example of a network to which the migration communication control device is attached in a second embodiment of the present invention;

FIG. 16 is a detailed block diagram depicting a home migration communication control device in the second embodiment of the present invention;

FIG. 17 is an illustration showing a content of a home mobile host list hold unit in the second embodiment of the present invention;

FIG. 18 is a detailed block diagram depicting the visitor migration communication control device in the second embodiment of the present invention;

FIG. 19 is an illustration showing a content of a visitor mobile host list hold unit in the second embodiment of the present invention;

FIG. 20 is a detailed block diagram depicting a migration address unit in the second embodiment of the present invention;

FIG. 21 is an illustration showing a content of an address hold unit in the migration address unit in the second embodiment of the present invention;

FIG. 22 is a detailed block diagram depicting a migration address unit in the second embodiment of the present invention;

FIG. 23 is an illustration showing a content of the address hold unit in the migration address unit in the second embodiment of the present invention;

FIG. 24 is an illustration showing a format of a data packet in the second embodiment of the present invention;

FIG. 25 is an illustration showing a format of a packet transfer message in the second embodiment of the present invention;

FIG. 26 is an illustration showing a flow of a data packet transmitted between devices in the second embodiment of the present invention;

FIG. 27 is an illustration showing a communication sequence in FIG. 26;

FIG. 28 is an illustration showing a construction of each data packet in FIG. 26;

FIG. 29 is an illustration showing a change in the content of each hold unit in FIG. 26;

FIG. 30 is an illustration showing a flow of each data packet transmitted between devices at an operation example in the second embodiment of the present invention;

FIG. 31 is an illustration showing a communication sequence in FIG. 30;

FIG. 32 is an illustration showing a construction of each data packet in FIG. 30;

FIG. 33 is an illustration showing a change in the address hold unit in each device in FIG. 33;

FIG. 34 is an illustration showing a flow of a data packet transmitted between devices at an operation example in the second embodiment of the present invention;

FIG. 35 is an illustration showing the communication sequence in FIG. 34;

FIG. 36 is an illustration showing a construction of each data packet in FIG. 34;

FIG. 37 is an illustration showing a change in the address hold unit in each device in FIG. 34;

FIG. 38 is an illustration showing a flow of each data packet transmitted between devices at an operation example in the second embodiment of the present invention;

FIG. 39 is an illustration showing a communication sequence in FIG. 38;

FIG. 40 is an illustration showing a construction of each data packet in FIG. 38;

FIG. 41 is an illustration showing a change in the address hold unit in each device in FIG. 38;

FIG. 42 is an illustration showing a flow of each data packet transmitted between devices in the second embodiment of the present invention;

FIG. 43 is an illustration showing a flow of each data packet transmitted between devices in the second embodiment of the present invention;

FIG. 44 is an illustration showing a flow of each data packet transmitted between devices in the second embodiment of the present invention; and

FIG. 45 is an illustration showing a flow of each data packet transmitted between devices in the second embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[Embodiment 1]

A construction of a migration communication control device in a first embodiment of the present invention is described hereunder with referring to FIGs. Hereinafter, the mobile node and partner node in the related art as well as in the summary of the invention are referred to as a mobile host and a stationary host, respectively.

FIG. 1 is an illustration showing the construction of the migration communication control device comprising a data hold unit 1, an application unit 2, a migration address unit 3, and a communication control unit 4.

The data hold unit 1 holds a couple of addresses of a mobile host by corresponding them. Each of the addresses in the data hold unit 1 is assigned before and after a migration of the mobile host.

The application unit 2 checks a connection as well as monitors a timer. The unit 2 is relevant for a higher layer in OSI model, which includes an application layer. For example, the unit 2 operates as TCP at TCP/IP (Transmission Control Protocol/Internet Protocol) or a layer which is higher than TCP.

The migration address unit 3 processes a migration address with referring to data in the data hold unit 1. The concrete operation of the migration address unit 3 varies depending on a type of the migration communication control device comprising the unit 3, and this will be described in detail later.

The communication control unit 4 controls the communication. The unit 4 is relevant for a lower layer in the OSI model. For example, the unit 4 operates as a layer which is lower than IP at TCP.

The application unit 2 and the communication control unit 4 are the same units as ones implemented on a general host. Besides the unit 2 and 4, the migration communication device in the first embodiment of the present invention includes the data hold unit 1 and the migration address unit 3; thereby implements an operation unique to this case. That is, the data hold unit 1 and the migration address processing unit 3 are attached to the mobile host which migrates across networks, or a stationary host which is attached to a network fixedly (for example, a gateway or a server); otherwise, they operate alone. Each device comprising the unit 1 and 3 supports a continuous communication unaffected by migration of the mobile host besides providing its own function.

The data hold unit 1 and the mobile address unit 3, which are included in the devices attached to the network, are described in FIGs. 2, 3, 4, 5. FIG. 2 shows a migration communication control device where the unit 1 and the unit 3 are attached to the mobile host which migrates across networks; FIG. 3 shows a migration communication control device where the unit 1 and the unit 3 are attached to a gateway which connects the networks; FIG. 4 shows a migration communication control device where the unit 1 and the unit 3 are attached to the stationary host, which is the communication partner of the mobile host; and FIG. 5 shows a migration communication control device attached to the network itself.

The migration communication control device in FIG. 2 (hereinafter referred to as a mobile host) further includes the application unit 2, the communication control unit 4, and an address obtainment unit 25, besides the data hold unit 1 and the migration address unit 3.

Each of the application unit 2 and the communication control unit 4 operates as the above; while the unit 2 together with the unit 4 operate as a conventional stationary host.

The address obtainment unit 25 obtains an address of the mobile host assigned when it has migrated to another network. Although other options can be considered, such as employing a manual setting by an operator or communicating with a server computer which administrates addresses of the network, it is supposed here that the address is obtained in accordance with an instruction of a system administrator or the operator. The address obtainment unit 25 is also possessed by a general host and will not be described in detail.

The addresses held in the data hold unit 1 are obtained by the address obtainment unit 25.

The migration address unit 3 (enclosed with a broken line) consists of a response message transmission unit 20, a marked packet conversion unit 21, a migration address setting unit 26, a migration post transmission unit 27, a reception packet unit 28, and a marked packet resumption unit 29.

The response message transmission unit 20 transmits the packet which responds to the received packet if the response is needed.

The marked packet conversion unit 21 converts a packet received from the response message transmission unit 20 as well as the application unit 2 into a marked packet by converting the address of the received packet and marking the packet.

The migration address setting unit 26 stores the address obtained by the address obtainment unit 25 into the data hold unit 1. The address obtained by the unit 25 is the address of the mobile host assigned after the migration, and the unit 26 stores it into unit 1 by corresponding it to the address of the mobile host assigned before the migration.

The migration post transmission unit 27 posts via the communication control unit 4 that the address obtained by the unit 25 is held in the data hold unit 1 together with the correspondence between a couple addresses each of which assigned before and after the migration.

The reception packet unit 28 detects whether or not the received packet is marked, and sends the unmarked packet to the application unit 2 while sending the marked packet to the marketed packet resumption unit 29.

The marked packet resumption unit 29 resumes the marked packet.

The migration communication control device in FIG. 3 (hereinafter referred to as a gateway) further includes the application unit 2 and the communication control unit 4 besides the data hold unit 1 and the migration address unit 3 (enclosed with a broken line).

Each of the application unit 2 and the communication control unit 4 operates described the above, and the unit 2 together with the unit 4 operate as a conventional gateway.

The data hold unit 1 holds the correspondence between a couple of the addresses of the mobile host each of which assigned before and after migration.

The migration address unit 3 consists of a reception packet unit 35, a migration post information unit 36, an address comparison unit 37, an address conversion post transmission unit 38, and a marked packet conversion unit 39.

The reception packet unit 35 detects whether or not the received packet is the packet comprising a migration post message, which is transmitted by the mobile host. The unit 35 then sends the migration post message to the migration post information unit 36 while sending the other packets to the address comparison unit 37.

In accordance with the migration post message received from the reception packet unit 35, the migration post information unit 36 stores in the data hold unit 1 the correspondence between a couple of the addresses of the mobile host each of which assigned before and after the migration. The unit 36 also sends the migration post message to the address conversion post transmission unit 38.

The address comparison unit 37 detects whether or not the destination address of the packet received from the reception packet unit 35 coincides with the address of the mobile host assigned before migration, which is held in the data hold unit 1. When they coincide with each other, the unit 37 further sends to the marked packet conversion unit 39 the address assigned after the migration, which corresponds to the address which coincides with the destination address, as well as the packet received from the reception packet unit 35. On the other hand, when they do not coincided with each other, the unit 37 implements a function of a gateway by sending the packet to the application unit 2.

The address conversion post transmission unit 38 transmits to the destination address of the above packet received from the reception packet unit 35 an address conversion post message to inform that the address of the mobile host changes when the address comparison unit 37 detects a coincidence. Also the unit 38 transmits the address conversion post message to the network which satisfies the following two conditions: (1) the network where the address assigned before the migration, which is held in the data hold unit 1, is other than 0 (2) the migration communication control device employs as the gateway is not attached to the network. When the address conversion post message is transmitted to the network, which satisfies the above conditions, its destination address is a broadcast address of the network. The broadcast address consists of a network part and a host part, and every bit of the host part is 1.

The marked packet conversion unit 39 generates a marked packet when the address comparison unit 37 detects a coincidence. The unit 39 generates it by marking a general packet after converting the destination address of the packet. Then, the unit 39 transmits it.

The migration communication control device in FIG. 4 (hereinafter referred to as a stationary host) further includes the application unit 2 and the communication control unit 4 besides the data hold unit 1 and the migration address unit 3 (enclosed with a broken line).

Each of the application unit 2 and the communication control unit 4 operates as described the above, and the unit 2 together with the unit 4 operate as a conventional stationary host (not migrate).

The data hold unit 1 holds the correspondence between a couple of the addresses of the mobile host each of which assigned before and after the migration.

The migration address unit 3 consists of a reception packet unit 45, a marked packet resumption unit 46, an address conversion post information unit 47, an address comparison unit 48, and a marked packet conversion unit 49.

The reception packet unit 45 detects whether the received packet is the packet comprising the address conversion post message, the marked packet, or the other packets. The address conversion post message is transmitted by the gateway. Then the unit 45 sends the address conversion post message to the address conversion post information unit 47, the marked packet to the marked packet resumption unit 46, and the other packets to the application unit 2.

The marked packet resumption unit 46 resumes the unmarked packet from the marked packet, which is received from the reception packet unit 45.

The address conversion post information unit 47 obtains from the packet comprising the address conversions post message, which is received from the reception packet unit 45, the correspondence between the address of the mobile host assigned before the migration and the one assigned after the migration, and stores it into the data hold unit 1.

The address comparison unit 48 detects whether or not destination address of the packet received from the application unit 2 coincides with the address of the mobile host assigned before migration, which is held in the data hold unit 1. When they coincide with each other, the unit 48 further sends to the marked packet conversion unit 49 the address assigned after the migration, which corresponds to the address which coincides with the destination address, as well as the packet received from the application unit 2. On the other hand, when they do not coincided with each other, the unit 48 sends the packet to the communication control unit 4.

The marked packet conversion unit 49 generates a marked packet when the address comparison unit 37 detects a coincidence. The unit 49 generates it by marking a general packet after converting the destination address of the packet. Then, the unit 49 transmits it.

The migration communication control device in FIG. 5, which is attached to the network by itself, consists of the data hold unit 1, the migration address unit 3 (enclosed with a broken line), and the communication control unit 4.

The data hold unit 1 holds the correspondence between a couple of the addresses of the mobile host each of which assigned before and after the migration.

The migration address unit 3 consists of the reception packet unit 35, the migration post information unit 36, the address comparison unit 37, the address conversion post transmission unit 38, and the marked packet conversion unit 39. The units integrating the migration address unit 3 operate substantially same as equivalent units integrating the gateway in FIG. 3 except the following.

In FIG. 3 the address conversion post transmission unit 38 transmits the address conversion post message to the network satisfying both of the two conditions, which are described in the above; whereas, the address conversion post transmission unit 38 in FIG. 5 transmits the address conversion post message to the broadcast address of the network as long as the network satisfies the first condition, that is it transmits the address conversion post message to the network when the address assigned before the migration, which is held in the data hold unit 1, is other than 0.

FIG. 6 shows a first example of a network to which the migration communication control device as the mobile host in FIG. 2, the migration communication control device as the gateway in FIG. 3, and migration communication control device as the stationary host in FIG. 4 are attached. In the figure numeral 11 denotes a mobile host in FIG. 2, which migrates from a network A to a network B and obtains an address α assigned on the network A as well as an address β assigned on the network B.

Numeral 12 denotes a stationary host in FIG. 3, which is attached to the network B and obtains an address γ assigned thereon.

Numeral 12' denotes a stationary host in FIG. 3, which is attached to the network A and obtains an address γ' assigned thereon.

Numeral 13 denotes a gateway in FIG. 3, which has an address g. The gateway 13 is attached to both the network A and the network B.

The address on each network is assigned by a system administrator.

FIG. 7 shows a second example of a network to which the mobile host in FIG. 2, the gateway in FIG. 3, and the stationary host in FIG. 4 are attached. The stationary host is not illustrated in FIG. 7 since its location does not affect the communication with the mobile host.

In the figure the mobile host 11 migrates across network 1-4, and obtains an address m, m', m'', m''' assigned on each network respectively.

The network 5 as well as each of the network 1-4 (hereinafter referred to as the net 5, and the net 1-4 respectively) are connected with each other by a gateway 1-4, as shown in the figure.

A gateway 1-4 (hereinafter referred to as gw 1-gw 4) is the migration communication control device employed as the gateway in FIG. 3.

FIG. 8 shows a third example of the network to which the mobile host in FIG. 2, the gateway in FIG. 3, and the stationary host in FIG. 4 are attached. Construction of this network is substantially same as the second example of the network in FIG. 6 although operation thereof is different from the second example, which will be described later.

FIG. 9 shows a fourth example of the network to which the mobile host in FIG. 2, the migration communication control device in FIG. 5, the stationary host in FIG. 4 are attached. The migration communication control device as the stationary host will not be described here.

In the figure, numeral 11 denotes the mobile host which migrates across the network 1-4 and obtains the address m, m', m", m"' assigned on each network respectively.

The network 5 as well as each of the network 1-4 (hereinafter referred to as the net 5, and the net 1-4 respectively) are connected with each other by a gw 1-4, as shown in the figure.

Each of the migration communication control unit 1-4 (hereinafter referred to as S1-S4) is relevant for the one in the FIG. 5.

An address used in the first embodiment of the present invention is described hereunder. Each address consists of a network part, which is assigned on each network and shared by every host attached to that network, as well as a host part, which is assigned to each host uniquely.

A broadcast address is a special kind of address, which can be divided into two types. The first one is the broadcast address used as the destination address in transmitting a packet from a network to another network, such as the broadcast address where every bit of the host part is 1. When the first type of the broadcast address is used as the destination address of the packet, the packet is transferred by the gateway to the network directed by the network part of the broadcast address. The other one is used in transmitting a packet within a network, such as the broadcast address where every bit of both the host part and the network part is 1. When the second type of the broadcast address is used as the destination address of the packet, the packet is transmitted to all the devices attached to the network, which includes the broadcast address. However, the gateway does not transfer the packet to any other network.

Operations of the migration communication control device in the first embodiment of the present invention are described hereunder with referring to drawings.

(operation example in FIG. 6)

In FIG. 6, when the mobile host migrates from the network A to the network B, the migration communication control device is operated as follows.

In a first operation, the mobile host and the gateway operate when the mobile host migrates across networks.

In a second operation, the stationary host transmits a packet to an address of the mobile host which was assigned before the migration.

In a third operation, the stationary host transmits the packet to an address of the mobile host which has been assigned after the migration.

In a fourth operation, the mobile host receives the packet which is transmitted by the stationary host.

In a fifth operation, the mobile host sends a response message to the stationary host.

(first operation in FIG. 6)

In FIG. 6 the mobile host 11 attached to the network A (enclosed with a broken line) migrates to the network B to complete ongoing communication with the stationary host 12, which is attached to the network B. When migrating to the network B, the address obtainment unit 25 in the mobile host 11 (FIG. 2) obtains the address β assigned on the network B.

Immediately after obtaining the address β, the address obtainment unit 25 gives the address β to the migration address setting unit 26 and the migration post transmission unit 27. The migration address setting unit 26 stores the address β into the data hold unit 1 by corresponding it to the address α, which is the address assigned before the migration. FIG. 10 (a) shows the content of the data hold unit 1. The migration post transmission unit 27 gives to the gateway 13 via the communication control unit 4 a packet comprising migration post message and the correspondence between the address α and the address β, so that the gateway 13 will know that the mobile host 11 has migrated to the network B. The mobile host 11 can transmit the packet both before and after the migration. In FIG. 6 a packet 51 is transmitted before the migration, and its format is shown in FIG. 11 (a). As shown in FIG. 11 (a), the packet 51 consists of a destination address 91, a source address 92, and data 93. The data 93 further comprise a message type 98, an address before migration 94, and an address after migration 95.

Receiving from the communication control unit 4 the packet 51, the gate way 13 sends it to the reception packet unit 35, the unit 4 and the unit 35 being in FIG. 3. From the message type 98 in FIG. 11 (a), the gateway 13 identifies the packet 51 with the migration post message, and gives the packet 51 to the migration post information unit 36. The migration post information unit 36 obtains from the data 93 in the data packet 51 the address before migration α and the address after the migration β; then stores them into the data hold unit 1 by corresponding them with each other. The content of the data in the data hold unit 1 is shown in FIG. 10 (b).

Additionally, the destination address 91 of the packet in FIG. 11 (a), can be the broadcast address of the network A, where the network part names the network A and every bit of the host part is 1. When the broadcast address is employed, every stationary host attached to the network A, including the gate way 13, receives the correspondence of the addresses each of which assigned before and after the migration. In this case communication control unit 4 in the stationary host 12' receives the data packet 51, and gives it to the reception packet unit 45, the unit 4 and the unit 45 in FIG. 4. From the message type 98 in FIG. 11 (a), the reception packet unit 45 identifies the packet 51 with the migration post message, and gives the packet 51 to the address conversion post information unit 47. The unit 47 obtains from the data 93 in the data packet 51 the address before migration α and the address after the migration β and stores them into the data hold unit 1 by corresponding them with each other. Once those addresses are stored in the data hold unit 1, the stationary host 12' can transmit a packet to the address assigned after the migration instead of transmitting it to the address before the migration, the same to other stationary hosts attached to the network A.

(second operation in FIG. 6)

In the second operation, the stationary host 12 transmits a packet to the address assigned before the migration after the mobile host 11 migrates to the network B and obtains the address β assigned on the network B. It is supposed that the mobile host 11 transmits the packet 51, which comprises the migration post message, to the gateway 13 rather than to the broadcast address of the network A.

The stationary host 12, which is not notified that the mobile host 11 has migrated to the network B, transmits the packet to the address α of the mobile host, which was assigned before the migration. A packet 52 in FIG. 6 is transmitted by the stationary host 12 to the address α of the mobile host 11, and its format is shown in FIG. 11 (f). The packet 52 is received by the gateway 13. Because the gateway 13 is located between the source address of the packet 52 and the address of the mobile host α assigned before the migration, and also it is attached to the network A, to which the mobile host 11 was attached before the migration.

The gateway 13 employs its devices in FIG. 3 to implement its functions including reception of the packet. That is, the communication control unit 4 in the gateway 13 receives the packet 52, and sends it to the reception packet unit 35 in the migration address unit 3. The reception packet unit 35 identifies the packet 52 with a general packet and gives it to the address comparison unit 37. The unit 37 compares the destination address α of the packet 52 with the address before the migration, which is held in the data hold unit 1; then detects whether or not they are coincide with each other. When the destination address of the received packet does not coincide with the address assigned before the migration, the address comparison unit 37 sends the packet to the application unit 2. On the other hand, when they coincide with each other, the address comparison unit 37 obtains from the data hold unit 1 the address β of the mobile host assigned after the migration, which corresponds to the address α; then sends it both to the address conversion post transmission unit 38 and the marked packet conversion unit 39.

As is described the above, the packet 52 is transmitted to the address α of the mobile host 11 by the stationary host 12. Therefore, the address conversion post transmission unit 38 notifies the stationary host 12 that the address of the mobile host 11 has changed by transmitting thereto the packet 53. FIG. 11 (b) shows the packet 53. Simultaneously, the marked packet conversion unit 39 converts the packet 52 into the packet 53 by rewriting the destination address of the packet 52 to the address β assigned after the migration, returning thereto the previous destination address of the packet 52 as additional information, and marking to show that its destination address has changed; then sends the packet to the communication control unit 4. Thereby, the packet 52, which is converted into the marked packet 52', is transferred from the address α of the mobile host 11 assigned before the migration to the address β assigned after the migration. FIG. 12 (e) shows the packet 52'.

Receiving the packet 53 from the communication control unit 4 in the stationary host 12, it sends its packet 53 to the reception packet unit 45, the unit 4 and the unit 45 being in FIG. 4. From the message type 98 in FIG. 11 (b), the reception packet unit 45 identifies the packet 53 with the address conversion post message, and gives the packet 53 to the address conversion post information unit 47. The address conversion post information unit 47 obtains from the data 93 in the data packet 53 the address before migration α and the address after the migration β; then stores them into the data hold unit 1 by corresponding them with each other. Thereby, the stationary host 12 obtains the address of the mobile host 11 assigned after the migration, so that a direct communication between the stationary host 12 and the mobile host 11 is implemented.

In the second operation the migration communication control device comprising the units in FIG. 4 is employed as the stationary host 12. However, a conventional stationary host, which is not constructed as the migration communication control device can also be communication partner of the mobile host if it is attached to a network. Therefore, hereunder a communication between the mobile host 11 and the convention stationary host is described.

When the conventional stationary host transmits a packet to the address of the mobile host 11 assigned before the migration after the mobile host 11 has migrated to another network, the gateway 13 transfers the packet to the address of the mobile host 11 assigned after the migration as well as sends to the stationary host the packet 53 comprising the address conversion post message in FIG. 11 (c). This operation is same as the above.

However, when receiving the packet 53, the stationary host disposes it since it does not support the address conversion post message and judges the packet 53 is not a required packet. Thus, the conventional stationary host cannot utilize the packet 53 to detect the address of the mobile host assigned after the migration nor hold the correspondence of the addresses each assigned before and after the migration.

Therefore, the stationary host gives the packet only to the address of the mobile host 11 assigned before the migration. Then, the gateway transfers the packet to the address of the mobile host 11 assigned after the migration, and the mobile host 11 receives the packet. The message from the mobile host 11, such as the response message, is transmitted to the stationary host directly, so that it is received by the stationary host without fail.

Thus, the conventional stationary host transmits a packet to the mobile host indirectly and receives a packet from the mobile host directly. Continuous communication unaffected by the mobile host's migration can be implemented, even when the conventional stationary host is employed.

(third operation in FIG. 6)

In the third operation, the stationary host 12 transmits the packet to the address β of the mobile host 11 assigned after the migration with referring to the correspondence of the addresses each assigned before and after the migration, which is held in the data hold unit 1. The third operation is described hereunder with referring to FIG. 4.

The stationary host 12 employs its devices in FIG. 4 to implement conversion of the destination address and the transmission of the packet, both of which integrate the third operation. That is, application unit 2 sends to the address comparison unit 48 the packet 54, whose destination address is the address α of the mobile host 11 assigned before the migration. FIG. 11 (f) shows a format of the packet 54. Then, the comparison unit 48 obtains the destination address of the packet 54 and detects whether or not it coincides with the address before the migration, which is held in the data hold unit 1.

The comparison unit 48 sends the packet 54 to the communication control unit 4 when the above addresses do not coincide with each other while it sends the packet 54 to the marked packet conversion unit 49 when the above addresses coincide with each other. In the third operation the coincidence is detected since the corresponded between the address α and the address β is stored in the data hold unit 1. Therefore, the packet 54 is sent to the marked packet conversion unit 49. Then the marked packet conversion unit 49 obtains from the data hold unit 1 the address β of the mobile host assigned after the migration, which corresponds to the address α as well as converts the packet 54 into the packet 54' by converting the destination address α into the address β, returning thereto the original destination address α as additional information, and marking the packet 54 to show that its destination address has changed; then sends the packet 54' to the communication control unit 4. FIG. 11 (c) shows a format of the packet 54'. Since the destination address of the packet 54' is an updated address of the mobile host 11, the packet 54' is given to the mobile host 11 without fail.

(fourth operation in FIG. 6)

In the fourth operation, the mobile host 11 receives the marked packet 54' and obtains the original unmarked packet 54 by resuming the packet 54'. This operation is described hereunder with referring to FIG. 2.

The mobile host 11 employs its devices in FIG. 2 to implement its operation. That is, the communication control unit 4 receives the packet 54' and sends it to the reception packet unit 28. The reception packet unit 28 detects that the received packet 54' is marked, and sends it to the marked packet resumption unit 29. The unit 29 obtains the original destination address α, which is held in the additional information 97, and replaces the current destination address β of the packet 54' with the address α. Then it sends the packet 54' to the application unit 2. Thus, the mobile host 11 can receive the packet destined for its outdated address.

(fifth operation in FIG. 6)

In the fifth operation, the mobile host 11 sends to the stationary host 12 a packet comprising a response message (hereinafter referred to as a response packet) or a packet excluding the response message (hereinafter referred to as a non-response packet). A type of the received packet determines whether or not it is responded with the response packet.

When the packet 54' is responded with a response packet, the mobile host 11 employs its devices in FIG. 2 to send the response packet. That is, the response message transmission unit 20 builds the response packet, and sends it to the marked packet conversion unit 21 together with the destination address α of the packet 54'.

The mobile host 12 also employs its devices to send the non-response packet 55. That is, the application unit 2 gives the address α assigned before the migration and the non-response packet to the marked packet conversion unit 21. The unit 21 sends the received packet to the stationary host 12 via the communication control unit 4 without marking it. FIG. 11 (e) shows the packet sent by the unit 21 to the stationary host 12.

The communication control unit 4 in the stationary host 4 receives the packet 55, and gives it to the reception packet unit 45. The unit 45 detects that the packet 55 is the non-response packet, so that it gives the packet 55 to the application unit 2. Thus, the stationary host and the mobile host implement a continuous communication unaffected by mobile host's migration. Although the migration communication control device is employed as the stationary host 12 in this embodiment, the conventional host can also be employed to transmit the non-response packet.

In the above, the unmarked response packet and the unmarked non-response packet are sent to the mobile stationary host 12. On the other hand, hereunder the operation of the mobile host 11 at conversion of the response packet and the non-response packet into the marked ones is described. This will be employed effectively in a communication between mobile hosts.

Receiving the unmarked packet from the application unit 2, the marked packet conversion unit 21 generates a packet 55' where the destination address and the source address are the address γ of the stationary host 12 and the address β assigned after the migration respectively. Also in generating the packet 55', the application unit 2 gives to the received packet the address α assigned before the migration as additional information as well as marks the received packet to indicate that the destination address has converted. FIG. 11 (d) shows a format of the packet 55'. Then the application unit 2 sends the packet 55' to the stationary host 12 via the communication control unit 4.

The communication control unit 4 in the stationary host 12 receives the packet 55', and sends it to the reception packet unit 45. Detecting the packet 55' is the marked packet, the reception packet unit 45 sends it to the marked packet resumption unit 46. The unit 46 resumes the packet 55' into the packet 55 by unmarking it and replacing the source address thereof with the address α assigned before the migration, which is held as the additional information. A format of the packet 55 is shown in FIG. 11 (e). Thus, the stationary host and the mobile host implement a continuous communication unaffected by mobile host's migration.

(operation example in FIG. 7)

In FIG. 7, when the mobile host migrates across the network 1, 2, 3, and 4, and obtains a temporary address assigned on each network, the newest address of the mobile host is transmitted to the stationary host, which operates as communication partner.

(migration from network 1 to network 2)

The address of the mobile host is m when it is attached to the network 1. When migrating from the network 1 to the network 2, the mobile host 11 replaces its address with m' assigned on the network 2. Then the mobile host 11 notifies the migration communication control device attached to the network 1 that it has migrated to the network 2 by sending thereto a packet comprising a migration post message. In FIG. 7 the migration communication control device gw 1, gw 2 attached to the network 1 receive the migration post packet 61, and store it into its own data hold unit 1. The operation in FIG. 7 is substantially same as the operation in FIG. 6 except that in FIG. 7 the packet 61 holds the address of the mobile host assigned before the last migration besides the correspondence of the addresses each assigned before and after the current migration. The address assigned before the last migration makes the gws prepare for further migration of the mobile host, which will be described later. A format of the packet 61 is shown in FIG. 12 (a). Since the migration from the network 1 to the network 2 is the first migration in FIG. 7, the packet 61 holds 0 at the address assigned before the last migration.

The gw 1 and the gw 2 store in the data hold unit 1 the correspondence of the addresses each assigned before and after the migration, as well as the address assigned before the last migration. As shown in FIG. 13 (a), m-m' and 0 are stored in the data hold unit 1 of each of the gw 1 and the gw 2.

Then, the gw 1 and the gw 2 detects from 0 at the address assigned before the last migration that no migration had been conducted before the current migration.

The broadcast address of the network 1 can be employed as the destination address of the migration post packet 61. If the packet is destined for the broadcast address, every host attached to the network 1, which includes the gw 1 and the gw 2, will hold the correspondence of the addresses each of which assigned before and after the migration as well as the address assigned before the last migration. Thereby, the hosts attached to the network 1 can communicated with the mobile host directly.

(migration from network 2 to network 3)

When migrating from the network 2 to the network 3, the mobile host 11 obtains m" at the address assigned after the migration. Then the mobile host 11 notifies the gw 2 and a gw 3, both of which are attached to the network 2, that the mobile host 11 has migrated to the network 3 by transmitting thereto a packet comprising the migration post message, referred to as a packet 62 in FIG. 7. FIG. 12 (b) shows a format of the packet 62, which is transmitted to the gw 2. The broadcast address of the network 2 can be employed as the destination address of the packet 62. When the packet 62 is transmitted to the broadcast address of the network 2, every host attached to the network 2, which includes the gw 2 and the gw 3, holds the correspondence of the addresses each assigned before and after the migration.

The gw 2 employs its devices in FIG. 3 to process the packet 62. That is, receiving the packet 62, the gw 2 sends it to the migration post information unit 36 via the communication control unit 4 and the reception packet unit 35, then refers to the data hold unit 1 where m→m' and 0 are still held at the address correspondence and at the address assigned before the last migration respectively. The migration post information post unit 36 obtains from the packet 62 m'-m" as the newly assigned correspondence between the addresses each of which assigned before and after the current migration, the migration from the network 2 to the network 3. Then, it detects whether or not the address m' coincides with the address held in the data hold unit 1 as the address assigned after the last migration. Since the unit 36 detects the coincidence, it replaces the address m' in the unit 1 with the address m" as well as replaces the correspondence m-m' with the correspondence m-m".

Also the migration post information unit 36 sends to the data hold unit 1 the address m assigned before the last migration together with the address correspondence m'-m" obtained from the current migration. Now the data hold unit 1 in the gw 2 holds the address m at the address assigned before the last migration and the address correspondence m'-m" at the correspondence of the addresses each of which assigned before and after the migration as well as the address 0 at the address assigned before the last migration as well as the address correspondence m-m' at the correspondence of the addresses each of which assigned before and after the migration. After updating as well as adding the addresses in the data hold unit 1, the migration post information unit 36 sends to the address conversions post transmission unit 38 m'-m" as the newly obtained correspondence of the addresses before and after the current migration.

The address conversion post transmission unit 38 detects the network satisfying the following conditions with referring to the data hold unit 1 and then transmits the address conversion post message to the broadcast address of the detected network. That is, the address conversion post message is transmitted to the network where the address assigned before the migration, which is held in the data hold unit 1, is other than 0 as well as the migration communication control device employed as the gateway is not attached. Although in the migration from the network 2 to the network 3, the data hold unit 1 holds m at the address assigned before the last migration, the gw 2 is attached to the network 1; therefore, the unit 38 does not transmit the address conversion post to the network 1.

The packet 62 is also received by gw 3. When receiving the packet 62, the gw 3 employs its own devices in FIG. 3 to process the packet 62, which is substantially same as does the gw 2 except the following. That is, the address conversion post transmission unit 38 of the gw 3 detects that the gw 3 is not attached to the network 1. Also it is detected that the mobile host 11, attached to the network 1, has the address m as the address assigned before the last migration. Therefore, the unit 38 of the gw 3 transmits to the broadcast address of the network 1 a packet comprising the address conversion post message, which is referred to as a packet 63. FIG. 12 (c) shows the packet 63.

The packet 63 is received by the gw 2, the gw 1, both of which are attached to the network 1. Although it is also received by the stationary host 11, this will not be described here. Obtaining the current address correspondence m'-m" from the packet 63, where m' coincides with the address which has been held in the hold unit 1 at the address obtained after the migration, the gw 1 changes the m-m' in the data hold unit 1 into the m-m" by replacing m' with m" as the address assigned after migration.

On the other hand, the data hold unit 1 of the gw 2 had gained from the packet 62 the above information before receiving the packet 63. Therefore the content of the unit 1 of the gw 2 does not change across reception of the packet 63. This is because the gws of the present invention locate on a gateway, which connects a couple of networks. Due to its location, each gw receives packets from two networks. However, actually the packet 62 is destined for the network 2 and the packet 63 is destined for the network 1. Therefore, even though the gw 2, which are attached to both the network 1 and the network 2, receives both the packet 62 and 63 by the gw 2, this will not cause any problem in the communication between the stationary host 12 and the mobile host 11.

FIG. 13 (b) shows the content of the data hold unit 1 in each of the gws.

(migration from network 3 to network 4)

When migrating from the network 3 to the network 4, the mobile host 11 obtains m‴ as the address assigned after the migration. Then the mobile host 11 sends to the gw 3 and a gw 4, both of which are attached to the network 3, a packet comprising the migration post message. The packet received by the gw 3 is referred to as a packet 64. The broadcast address of the network 3 can be employed as the destination address of the packet 64. When the packet 64 is destined for the broadcast address of the network 3, every host attached to the network 2, which includes the gw 3 and the gw 4, obtains from the packet the correspondence of the addresses each of which assigned before and after the migration from the network 3 to the network 4.

The gw 3 employs its devices in FIG. 3 to process the packet 64. That is, receiving the packet 64, the gw 3 converts the content of the data hold unit 1 by replacing the address correspondence m-m" with m-m‴, newly holding m"-m‴ obtained from the packet 64 as well as the address m' assigned before the last migration. Then, the address conversion post transmission unit 38 of the gw 3 transmits the address conversion post message to the network satisfying the following condition. That is, the address conversion post message is transmitted to the network where the address assigned before the migration, which is held in the data hold unit 1, is other than 0 as well as the gw 3 it self is not attached. The packet including the address conversion post message is referred to a packet 65, and the packet is transmitted to the broadcast address of the network 1. FIG. 7 (c) shows the packet 65.

The packet 64 is also received by gw 4. When receiving the packet 64, the gw 4 renews the content of the data hold unit 1 by replacing m'-m" with m'-m‴ as well as newly holding the address m' as the address assigned before the last migration. Further, the address conversion post transmission unit 38 of the gw 4 detects that the gw 4 is not attached to the network 2 which has the address other than 0 at the address assigned before the last migration; therefore, the unit 38 of the gw 4 transmits a packet comprising the address conversion post message, which is referred to as a packet 66, to the broadcast address of the network 2. FIG. 7 (c) shows the packet 66.

Receiving the packet 65, 65, the gw 2 and the gw 1 renew the content of its data hold unit 1, which is substantially the same as the above.

The gw 3 and the gw 2 receives the same information twice since the former receives the packet 64 and 65 while the latter receives the packet 65 and 66. This is because gws of the present invention locate on a gateway and receives packets from a couple of networks, which is described the above.

FIG. 13 (c) shows the content of the data hold unit 1 in each of the gws. Thus, according to the gws of the present invention, the packet transmitted to any of the addresses m, m', m" is transferred by the gws to the updated address of the mobile host, the gws also notify the stationary host of the updated address.

For example, when the stationary host is not notified of the updated address of the mobile host and transmits a packet to the address m', the packet is received by the gw 2 and the gw 3, both of which are attached to the network 2. Then, the gw 2 and the gw 3 transfers the packet to the updated address of the mobile host as well as notifies the stationary host of the updated address. Thereby, the stationary host obtains the updated address of the mobile host, so that it will be able to communicate with the mobile host directly. The packet destined for the address m' is received by both the gw 2 and the gw 3, since they are attached to the network 2. Thus, the mobile host receives the same packet twice, once from the gw 2 and the other time from the gw 3, and the stationary host receives the same message twice; however, the repeated packet or the message can be simply ignored, so that this will not cause any problem in the communication between the stationary host and the mobile host. The repeated packet or the message is observed when the two gws are attached to each network in FIG. 7; whereas it is not observed when only one migration communication control device is attached to each network, which will be described later at the operation in FIG. 9.

(operation example in FIG. 8)

In FIG. 6, FIG. 7, the stationary host transmits the data packet to the outdated address after mobile host notifies the gws that it has migrated to another network. Then the gws transmit the address conversion post message to the stationary host. However, in FIG. 8 the gws convert the destination address of data the packet from the outdated address into the updated address assigned after the migration instead of transmitting the address conversion post message.

A packet 71, 72 in FIG. 8 are substantially same as the packet 51, 52 in FIG. 6. The operation conducted before the packet 72 is transmitted by the stationary host 12 and is received by the gateway 13 is substantially same as the first operation in FIG. 6. The operation which follows reception of the packet 72 is described hereunder with referring to FIG. 3.

The gate way 13 employs its units in FIG. 3 to process the packet 72. The communication control unit 4 receives the packet 72 and gives it to the reception packet unit 35 in the migration address unit 3. Detecting that the packet 72 is a general packet, the reception packet unit 35 sends it to the address comparison unit 37. The address comparison unit 37 detects whether or not the destination address of the packet 72 coincides with the address in the data hold unit 1 at the address assigned before the migration.

When no coincides is found, the address comparison unit 37 gives the packet 72 to the application unit 2. On the other hand, a coincidence is found, the address assigned after the migration, which corresponds with the address identical to the destination address of the packet 72, is obtained from the data hold unit 1, and is sent to the marked packet conversion unit 39 together with the packet 72. The marked packet conversion unit 39 generates a packet 72' where the destination address of the packet 72 is replaced with the address assigned after the migration, which is sent by the address comparison unit 37, the destination address of the packet 72 is added as additional address, and a mark is set to indicate that the destination address has converted. Then the packet 72' is sent to the communication control unit 4. FIG. 12 (e) shows a format of the packet 72', where identical numerals denotes the same units in FIG. 11. The packet 72' is sent to the mobile host 11 without fail since its destination address is the updated address thereof.

(operation example in FIG. 9)

In FIG. 9, the mobile host migrates across network 1, 2, 3, and 4. In FIG. 7 the gw 1-gw 4 are employed as the migration communication control devices; whereas in FIG. 9 the gw 1-gw 4 are employed simply as gateways to connect networks, and also another migration communication control device is attached to each network. The operation of the migration communication control device, which is connected to the network alone, at processing the migration post message or the address conversion post message is substantially same as one of the gw 1-gw 4 in FIG. 7. The flow of the migration post message and the address migration post message are mainly described hereunder.

(migration from network 1 to network 2)

When migrating from the network 1 to the network 2, the mobile host 11 sends a packet comprising the migration post message to the migration communication control device, which is attached to the network 1. In FIG. 9 (a) a migration post packet 81 is transmitted to a migration communication control device S1, which is attached to the network 1. The destination address of the packet 81 can be the broadcast address of the network 1.

The device S1 processes the packet 81 by employing its devices in FIG. 3. Receiving the packet 81, the device S1 stores into the data hold unit 1 the correspondence of the addresses each assigned before and after the migration as well as the address assigned before the last migration. The migration post information unit 36 transmits the packet 81 to the address conversion post transmission unit 38; however, since the unit 38 detects that the address assigned before the last migration is 0, it does not transmit the address conversion post message to any network. The content of the data hold unit 1 in the S1-S4 are shown in FIG. 14 (a).

(migration from network 2 to network 3)

When migrating from the network 2 to the network 3, the mobile host 11 notifies the S2, which is attached to the network 2, that it has migrated to the network 3 by transmitting thereto the packet comprising the migration post message, which is referred to as a packet 82 in FIG. 9 (b).

The S2 employs its devices in FIG. 3 to process the packet 82. That is, it converts the content of the data hold unit 1 by renewing and adding new information, and finally holds in the unit 1 the address m'-m" at the correspondence of the addresses each of which assigned before and after the migration as well as the address m assigned before the last migration. Then, the migration post information unit 36 gives the newly obtained correspondence m'-m" to the address conversion post transmission unit 38.

The address conversion post transmission unit 38 detects whether or not the address assigned before the last migration, which is held in the data hold unit 1, is 0. If the address is not 0, the unit 38 transmits the address conversion post message to the broadcast address of the network which includes the detected address. In FIG. 9 (b) the address m is held at the address assigned before the last migration, so that the unit 38 transmits the packet 83 to the broadcast address of the network 1.

When receiving the packet 83, the migration communication control device S1, which is attached to the network 1, renews the content of the data hold unit 1 by newly holding the address correspondence m-m" as well as the address 0 at the address assigned before the last migration. Detecting 0 at the address assigned before the last migration, the address conversion post transmission unit 38 does not transmit the address conversion post to any network. The content of the data hold unit 1 in the S1-S4 are shown in FIG. 14 (b).

(migration from network 3 to network 4)

When migrating from the network 3 to the network 4, the mobile host 11 notifies the communication migration control device S3, which is attached to the network 3, that it has migrated to the network 4 by transmitting thereto a packet comprising the migration post message, referred to as a packet 84 in FIG. 9 (c).

The migration communication control device S3 employs its devices in FIG. 3 to process the packet 84. That is, it newly holds into the data hold unit 1 the address correspondence m''-m''' as well as the address m' assigned before the last migration. Then, the address conversion post transmission unit 38 in the S3 transmits a packet comprising the address conversion post message, referred to a packet 85 in FIG. 9 (c), to the broadcast address of the network 2 since the address m' is held at the address assigned before the last migration in the data host unit 1.

When receiving the packet 85, the migration communication control device S2 employs its devices in FIG. 3 to process it. That is, it newly holds into the data hold unit 1 the address correspondence m'-m'' as well as the address m assigned before the last migration. Then, the address conversion post transmission unit 38 in the S2 transmits a packet comprising the address conversion post message, referred to a packet 86 in FIG. 9 (c), to the broadcast address of the network 2 since the address m is held at the address assigned before the last migration in the data hold unit 1.

When receiving the packet 86, the migration communication control device S1 employs its devices in FIG. 3 to process it. That is, it newly holds into the data hold unit 1 the address correspondence m-m''' as well as the address 0 at the address assigned before the last migration. The address conversion post transmission unit 38 in the S1 does transmit the address conversion post since 0 is detected at the address assigned before the last migration. The content of the data hold unit 1 in each of the S1-S4 are shown in FIG. 14 (c). Thus, according to the migration communication control device S1-S4 of the present invention, the S1-S4 are notified of the updated address of the mobile host at every migration, so that the packet transmitted to any of the addresses m, m', m'' is transferred thereby to the updated address of the mobile host. The S1-S4 also notify the stationary host of the updated address of the mobile host.

The operation in FIG. 9 differs from the operation in FIG. 7 in that each network has just one communication migration control device (one of the S1-S4), so that the migration post and the address conversion transmitted to S1-S4 are not duplicated.

In the format shown in FIG. 11 and 12, the mark 96 or the message type 93 indicates kind of packet. That is, mark 96 indicates whether or not the packet is marked while the message type 93 indicates whether it is the packet comprising the migration post message, the packet comprising the address conversion post message, and the general packet. Further, a protocol type can also be employed to indicate which migration communication control device is employed. For example, when TCP/IP is employed, the protocol number at the IP header thereof distinguishes the packet employed in the embodiment from other packets. That is, when the protocol number in the packet is identical with the one, which has been assigned to the protocol number field, the packet is the one employed in the embodiment.

In the first embodiment of the present invention, a nonvolatile storage can be employed as the data hold unit 1 of the mobile host. If so, the communication can be resumed even after the host or the gateway is turned off as well as after the system is reset.

Also even when the stationary host employs the nonvolatile storage as the data hold unit 1, it can resume the communication, which has interrupted by the switch off or the system reset, rather fast since it obtains from another host the updated address of the mobile host instead of receiving from the gateway the address conversion post message which shows the updated address.

For example, it is supposed in FIG. 7 that the mobile host 11 migrates from the network 1 to the network 4. The data hold unit 1 of the migration communication device holds the address correspondence m-m''' since it has communicated with the mobile host, which is attached to the network 4, at least once. According to the migration communication control device in the embodiment described the above, the packet is transferred from the outdated address to the updated address of the mobile host and the stationary host is notified of the updated address; therefore, even when the address information in the data hold unit is lost by switch off thereof, the stationary host will obtain the updated address. Restart of the communication can also be implemented by employing a specific host such as a server. That is, the server may be constructed to obtain the updated address of the mobile host at every migration, and give it to the stationary host whenever requested. In this case a packet comprising the address inquiry should be generated beforehand.

Also in the fifth operation in FIG. 6, the mobile host 11 employs the application unit 2 and sends to the marked packet conversion unit 21 the address assigned before the migration when transmitting the non-response address to the stationary host after it has migrated to another network. Instead of sending the non-response address, the application unit 2 can transmit a connection identifier to the marked packet conversion unit 21. In this case the data hold unit of the migration communication control device, employed as the mobile host, holds a correspondence between the connection identifier and the address that had been assigned when the connection was established instead of holding the correspondence between the correspondence of the addresses each assigned before and after the migration. Then, the unit 21 obtains the source address of the packet by detecting the address which corresponds to the identifier, which is held in the data hold unit 1.

As is described the above, the mobile host can employ the broadcast address of the network when transmitting the migration post to the migration communication control devices. When the broadcast address is employed, every host attached to the network, to which the migration communication control device is also attached, obtains the updated address of the mobile host. This implements a direct communication between the mobile host and the stationary host, which improves efficiency of the communication.

The address assigned before the last migration, which is held in the hold unit 1, can be replaced with the broadcast address assigned to the network to which the mobile host is attached before the last migration. If the broadcast address is employed, the gateway employed as the migration communication control device (gws) or the migration communication control device (Ss) needs to include the broadcast address in the address conversion post message. In this case both devices can obtain the broadcast address from the data hold unit; therefore, the operation thereof at requesting the broadcast address will be eliminated.

When storage capacity of the data hold unit 1 is limited, the data hold unit 1 holds only the useful data by disposing the unuseful data, which is least recently retrieved therefrom by the address comparison unit.

[Embodiment 2]

In FIG. 15 network A, B, and C are connected in a line via gateways 143 and 143', the gateway 143 placing between the network A and B while the gateway 143' placing between the network B and C.

A home migration communication control device 101 including a migration address unit 144 is attached to the network A; a visitor migration communication control device 109 including a migration address unit 145 is attached to the network B; and a visitor migration communication control device 109' including a migration address unit 145' is attached to the network C. A mobile host 146 including a migration address unit 115 is attached to the network A as its home network, and a stationary host 151 including a migration address unit 125 is also attached to the network A.

The mobile host 146 migrates across the network A, B, and C. It has a home address α assigned when it is attached to the network A, as well as other addresses assigned depending on where it migrates, such as a temporary address β on the network B and a temporary address γ on the network C.

Also each of the home migration communication control device 101, the visitor migration communication control device 109, 109' which are identical in its construction and the stationary host 151 has an address Ha, Va, Va', and Sa respectively assigned on the network.

Detailed function of the above devices 101, 109, 109', 146, and 151 is described hereunder, in which like components are labeled with like reference numerals.

[home migration communication control device 101]

When the mobile host 146 migrates from the home network to another network, it is assigned the temporary address. However if the stationary host 151 is not notified of that migration, it transmits an original data packet (hereinafter referred to as a noncapsulated data packet) to the home address α of the mobile host 146. When the noncapsulated data packet is destined for the outdated address of the home mobile host 146, the home migration communication control device 101 transfers that noncapsulated data packet from there to the updated address, that is the temporary address β or γ of the mobile host. Then, the device 101 posts to the stationary host 151 the temporary address β or γ here, so that the stationary host 151 will be able to communicate directly with the mobile host. The device 101 also posts the same information to the visitor migration communication control device 109, 109', so that the devices 109, 109' will implement the same function with the home migration communication control device 101.

As shown in FIG. 16 the home migration communication control device 101 consists of the migration address unit 144 and a communication control unit 108. The migration address unit 144 further comprises a home mobile host (MH) list hold unit 102, a packet transfer unit 103, a mobile host (MH) transfer unit 104, an address inquiry unit 105, a packet monitoring unit 106, an address post unit 107.

Next the function of each component integrating the device 101 will be described. The communication control unit 108 mainly controls the communication of protocols located in lower layers including a physical layer, such as the protocol lower than IP.

The address post unit 107 receives from the mobile host 146 an data packet including an address post message. The address post message is generated when the mobile host 146 migrates to the network B or C, and posts the temporary address β or γ of the mobile host to the device 101. The unit 107 sends the address post message to the mobile host transfer unit 104 as well as sends a response message to the mobile host 146. FIG. 28 (3) is an example of the address post message, which includes the home address α as well as the temporary address β or γ of the mobile host 146, a value of an autonomous flag F, and a broadcast address Bba, Cba on the network B, C. The autonomous flag F will be described later. FIG. 28 (4) is an example of the response message.

A mobile host transfer unit 104 stores the address post message into the home mobile host list hold unit

102, notifies the visitor migration communication control device 109 or 109' of the migration of the mobile host 146 by sending thereto a mobile host transfer message, and receives the data packet including the response. Further, according to a direction given by the packet transfer unit 103, the unit 104 transmits the mobile host transfer message both to the stationary host 151 and the device 109 or 109'. The unit 103 gives the direction when the value of the autonomous flag F is 1.

FIG. 32 (3) and FIG. 36 (5) are examples of the mobile host transfer message including the home address α, the temporary address β or γ, and the autonomous flag F. Since the mobile host transfer message is sent to the stationary host 151 is sent only when the autonomous flag F is 1; therefore, it does not necessarily include the value of the flag F. However, the identical message is sent both to the stationary host 151 and the visitor migration communication control device 109, 109' in this embodiment to simplify the construction of the mobile host transfer unit 104. FIG 32 (4) is an example of the response message.

As shown in FIG. 17, the home mobile host list hold unit 102 holds the home address α, the temporary address β, γ, the value of the autonomous flag F, and the broadcast address Bba, Cba on the network B, C, all of which are obtained from the mobile host transfer unit 104.

The packet monitoring unit 106 receives the packet destined for the home address α of the mobile host 146, then sends it to the packet transfer unit 103 when the stationary host 151 transmits the packet to the home address α of the mobile host 146 after the mobile host 146 has migrated to another network.

The packet transfer unit 103 has a payload including the noncapsulated data packet and the packet transfer message informing the transfer of the noncapsulated data packet, generates another data packet, and sends it to the temporary address β, γ of the mobile host 146. FIG. 32 (2) is an example of the packet transfer message. As is described the above, the packet transfer unit 103 directs the mobile host transfer unit 104 to transmit the mobile host transfer message to the stationary host 151 only when the autonomous flag in the home mobile host list hold unit 102 shows the value of 1. The operation conducted when the flag F is 1 will be described later.

When the stationary host 151 has problems in communicating with the mobile host 146 such as receiving the unusual mobile host transfer message, the address inquiry unit 105 is employed to solve the problems. That is, receiving from the stationary host 151 an address inquiry message, the address inquiry unit 105 transmits to the stationary host 151 a data packet which responds to the address inquiry by showing the address to be used in the communication. The address inquiry message includes a type field 132, a flag field 133, a sequence field 134, and a home address field 138, each of which having value 5, 1, a certain number, and α respectively; while the response message includes a temporary address field 139 filled with the temporary address β, γ as well as the flag field with 2, besides the type field 132, the sequence field 134, and the home address field 138 filled with the same values in the address inquiry message.

[visitor migration communication control device 109]

The visitor migration communication control device 109 implements the same function with the home migration communication control device 101. That is, when the stationary host 151 transmits an encapsulated data packet to the temporary address β of the mobile host 146, which is the updated address thereof since the mobile host has migrated to the network C, the visitor migration communication control device 109 transfers that encapsulated data packet from the temporary address β to temporary address γ. Then, the device 109 posts to the stationary host 151 the temporary address γ, so that the stationary host 151 will be able to communicate directly with the mobile host 146. However, whether or not the device 109 provides the above packet transfer service will be determined in accordance with a processing load put on the device 109 or with a initial setting given by a system operator; thus, the packet transfer service of the device 109 is not necessarily an obligation.

As shown in FIG. 18, the visitor migration communication control device 109 consists of the migration address unit 145 and the communication control unit 108. The migration address unit 145 further comprises the packet monitoring unit 106, a visitor mobile host list hold unit 110, a packet transfer unit 111, a mobile host transfer unit 112, a mobile host visit unit 113, and an autonomous support unit 114. The unit 106 and the unit 108 function the same as those in the home migration communication control device 101.

Receiving an autonomous packet transfer support check message inquiring if the visitor migration communication control device 109 provides the packet transfer service, the autonomous support unit 114 responds to it with the response message where the autonomous flag F shows 1 when the device 109 provides that service or 0 when it does not provide that service. FIG. 28 (1) is an example of the autonomous packet transfer support check message, while FIG. 28 (2) is an example of the response message including the autonomous flag F and the broadcast address Bba.

Receiving from the mobile host 146 the mobile host visit message which informs that the mobile host 146 has migrated to the network B, the mobile host unit 113 responds it with the response message after storing the mobile host visit message into the visitor mobile host list hold unit 110. The mobile host visit message includes the home address α and the temporary address β of the mobile host 146. FIG. 28 (5) is the format of the mobile host visit message, while the FIG. 28 (6) is the format of the response message.

Receiving from the mobile host transfer unit 104 in the device 101 the mobile transfer message informing that the mobile host 146 has migrated to the network C, the mobile host transfer unit 112 stores in the visitor mobile host list hold unit 110 the updated temporary address γ of the mobile host 146 and the value of the autonomous flag F by corresponding them to the home address α. The unit 112 also transmits to the stationary host 151 the mobile host transfer message in accordance with the direction from the packet transfer unit 111, as does the mobile host transfer unit 104 in the device 101.

As shown in FIG. 19, the visitor mobile host list hold unit 110 holds the home address α and the temporary address β on the network B, which are obtained from the mobile host 146 via the mobile host visit unit 113, as well as the temporary address γ and value on the autonomous flag F, which are obtained from the home migration communication control device 101 via the mobile host transfer unit 112.

The packet transfer unit 111, as does the packet transfer unit 103 in the home migration communication control device 101, transmits to the temporary address γ the data packet including the transfer message as well as orders the mobile host transfer unit 112 to transmit the mobile host transfer message.

[mobile host 146]

As shown in FIG. 20, the mobile host 146 includes the migration address unit 115, an address obtainment unit 116, the communication control unit 108, and an application processing unit 124 which mainly controls the communication of protocols located in higher layers including an application layer, such as TCP or layers located higher than it.

The migration address unit 115 comprises the a packet transmission unit 117, a transfer packet reception unit 118, an address hold unit 119, a migration unit 120, an autonomous support unit 121, an address post unit 122, a mobile host visit unit 123.

The migration address unit 115 comprising the above units is employed in transfer of data to the temporary address β or γ when the mobile host 146 migrates to the network B or C. Also receiving the data packet destined for the temporary address β or γ including the packet transfer message and the noncapsulated data packet, the device 115 transmits the noncapsulated data to the application processing unit 124.

In accordance with the order given by the application processing unit 124 when the mobile host migrates to the network B, C, the migration unit 120 controls the address obtainment unit 116, the autonomous support unit 121, the address post unit 122, the mobile host visit unit 123, and the address hold unit 119.

Directed by the migration processing unit 120, the address obtainment unit 116 obtains the temporary address β, γ of the mobile host 146 assigned when it migrates to the network B, C respectively. BOOTP in "Bill Croft and John Gilmore, BOOTSTRAP PROTOCOL RFC951, Sep., 1985" is an example of obtaining the temporary address; besides employing the BOOTP, the operator may input the temporary address β, γ assigned by a system administrator of the network B, C.

Directed by the migration unit 120, the autonomous support unit 121 sends the autonomous packet transfer support check message to inquire if the visitor migration communication control device 109, 109' attached to the network B, C provides the packet transfer service and receives the response message to the inquiry. The autonomous packet transfer support check message is also sent to obtain the broadcast address Bba and Cba on the network B and C respectively.

Directed by the migration unit 120, the address post unit 122 sends the address post message to notify the home migration communication control device 101 of the temporary address β, γ. The address post message also informs whether or not the device 109, 109' provides the packet transfer service as well as the broadcast address Bba, Cba on the network B, C. If the response message from the visitor migration communication control device 109, 109' has the value 1 of the autonomous flag F, the mobile host visit unit 123 transmits to the visitor migration communication control device 109, 109' the mobile host visit message including the home address α as well as the temporary address β, γ respectively.

As shown in FIG. 21, the address hold unit 119 previously holds the home address α of the mobile host 146 and the broadcast address Aba on the network A. Now, the unit 119 newly holds the temporary address β or γ obtained from the address obtainment unit 116 via the migration unit 120 and the broadcast address Bba or Cba obtained from the autonomous support unit 121 via the migration unit 120.

When the mobile host 146 is attached to the network A and receiving a data packet destined for the home address α, the transfer packet reception unit 118 sends data etc. in the noncapsulated data packet to the application processing unit 124. On the other hand, when the mobile host 146 is attached to the network B and receiving a data packet destined for the temporary address β, the data packet including the packet transfer message and the noncapsulated data packet destined for α, the unit 118 sends to the application processing unit 124 data etc. in the noncapsulated data. Thus, the application processing unit 124 receives the data without being affected by the migration of the mobile across the networks.

Receiving the data to be transmitted and the instruction from the application processing unit 124, the packet transmission unit 117 generates a noncapsulated data packet whose destination address is the home address α and transmits it.

[stationary host 151]

As shown in FIG. 22, the stationary host 151 comprises the migration address unit 125 and the application processing unit 161 which mainly controls the communication of a protocol located in higher layers including application layer, such as TCP or layers located higher than the TCP and the communication control unit 108.

The migration address unit 125 comprises a transfer packet transmission unit 126, a packet reception unit 127, an address hold unit 128, an address inquiry unit 129, and the mobile host transfer unit 130.

The migration address unit 125 comprising the above units generates a noncapsulated data packet and sends it to the home address α when it is not notified that the mobile host 146 migrate to the network B or C and obtained the temporary address β or γ respectively. The unit 125 also generates an encapsulated data packet including as a payload the noncapsulated data packet and a data transfer message, which informs transfer of the noncapsulated data packet and sends it to the temporary address β, γ, when it is notified of the migration.

Receiving from the home migration communication control device 101 and the visitor migration communication control device 109, 109' the data packet including the mobile host transfer message which informs the migration of the mobile host 146, the mobile host transfer unit 130 stores into the address hold unit 128 the home address α and the temporary address β or γ of the mobile host 146 assigned on the network B or C respectively.

As shown in FIG. 23, the address hold unit 128 holds the home address α, the temporary address β or γ by corresponding them.

Directed by the application unit 161, the transfer packet transmission unit 126 generates a data packet destined for the home address α, and transmits it. However, if the address hold unit 128 holds the temporary address β or γ besides the home address α, the unit 126 generates an encapsulated data packet destined for the temporary address β or γ, which includes as a payload a noncapsulated data packet and a packet transfer message, which informs transfer of the noncapsulated data packet, and transmits it.

As is described the above, both the home migration communication control device 101 and the visitor migration communication control device 109, 109' generate the encapsulated data packet including the packet transfer message and the noncapsulated data and transmits it to the current temporary address of the mobile host 146. Owing to the device 101 or 109, 109', the stationary host 151 is able to transmit to the mobile host 146 both the noncapsulated data packet destined for the home address α and the encapsulated data packet destined for the temporary address β or γ without failure even when the address hold unit 128 fails to hold the current temporary address β or γ and the stationary host 151 transmits the data packet to the outdated address of the mobile host 146.

The packet reception unit 127 receives a data packet which is sent from the mobile host 146 and has Sa as its destination address, and sends the data etc. in it to the application unit 161.

When the address inquiry unit 129 has problems such as that it received an illegal mobile host transfer message or that it cannot communicate with the mobile host 146 successfully, it transmits a data packet including an address inquiry message in order to inquire of the host migration communication control device 101 the address which is currently used to communicate with the mobile host 146.

[construction of data packet]

As shown in FIG. 24 (a), (b), (c), there are three kinds of data packets, each data packet 210, 220, 230, includes each of header 211, 221, 231 and payload 212, 222, 232 respectively.

The header 211 of the data packet 210 includes a destination address 201, and a source address 202. Also the payload 212 consists of a transmission data 203.

The header 221 of the data packet 220 includes the destination address 201 and the source address 202. Also the payload 222 consists of a message 204.

The header 231 of the data packet 230 includes the destination address 201 and the source address 202. Also the payload 232 consists of the message 204, which is employed as the packet transfer message, and a noncapsulated data packet 210. Also each header 211, 221, 231 includes information showing presence or absence of the message 204 as a protocol number etc.

The message 204 includes some of the fields in FIG. 25 in accordance with its type.

The type of the message 204 is indicated in the message type field 132. Besides the above types, the message 204 is also employed as an echo message for examining whether or not a host employs an appropriate operation in accordance with the message.

A flag field 133 indicates whether or not the message 204 is a response. When the message 204 is not the response, the field 133 further indicates whether or not the message 204 requests a response.

A sequence field 134 gives a single number both to the request message and its response message, thereby the request message and the response message are corresponded.

An autonomous flag field 135 contains a value of the autonomous flag F indicating whether or not the visitor migration communication control device 109,109' provide the packet transfer service.

A counter field 136 contains a counter indicating the number of the visitor migration communication control devices employed to transfer the encapsulated data packet consisting of the packet transfer message and the noncapsulated data packet. The visitor migration communication control device increments the counter in the received message packet by 1, and gives it to the message to be transmitted. When the incremented number is greater than the predetermined number, the received message packet is disposed.

A status field 137 of the response message indicates presence or absence of an error in a transmission/reception of the data packet. For example, it indicates an error in authentication information, which will be described later, or the address inquiry message which cannot or should not be responded.

A home address field 138, a temporary address field 139, and a broadcast address field 140 indicates the home address as well as the temporary address of the mobile host 146 or the broadcast address on its home network or on the network it migrates. However, what the broadcast address field 140 indicates depends on type of the message 204. Whether the message 204 is the request or the response also devices the content of the broadcast address field 140.

The authentication information field 141 indicates if a source address coincides with the sender's address.

[outline of communication operation]

The home migration communication control device 101 and the visitor migration communication control device 109,109' is basically employed to transfer the data packet transmitted by the stationary host 151 as well as post to the stationary host 151 the updated temporary address of the mobile host 146. Understanding of such operations will be helped by the following two points.

1. Transfer of the data packet and posting of the updated temporary address are conducted only when the mobile host 146 migrates from its home network to another network. The home network refers to the one to which the home migration communication control device is attached.

2. Posting of the updated temporary address is conducted only when the autonomous flag F is 1, which indicates the visitor migration communication control device 109, attached to the same network as is the mobile host 146, provides the packet transfer service. Otherwise, the data packet transmitted by the stationary host 151 to the posted temporary address will not be received by the mobile host 146 when the mobile host 146 migrates to another network.

[communication operation 1]

An example of the communication operation is described hereunder. In the communication operation 1 the visitor migration communication control device 109,109' provides the packet transfer service when the mobile host 146 migrates from the network A to the network B, further from the network B to the network C.

[migration from network A to network B]

The operation at the migration of the mobile host 146 from the network A to the network B is described with referring to FIGs. 26-29. FIG. 26 shows a flow of the data packet transmitted between the devices; FIG. 27 shows a communication sequence of the data packet; FIG. 28 shows construction of each data packet; and FIG. 29 shows the content of the address hold unit 119 etc.

When the mobile host 146 is attached to the network A, the home mobile host list hold unit 102 in the home migration communication control device 101 holds the home address α both as the home address and the temporary address of the mobile host 146. Thereby the home migration communication control device 101 detects that the mobile host 146 is attached to the network A.

The address hold unit 119 in the mobile host 146 holds the home address α and the broadcast address Aba on the network A.

When the mobile host 146 migrates to the network B, the application unit 124 orders the operation of the migration unit 120 in accordance with the instruction given by the operator. The temporary address β is assigned to the mobile host 146 on the network B, and the address obtainment unit 116 obtains it. The migration unit 120 stores into the address hold unit 119 the temporary address β together with the home address α and the broadcast address Aba.

(1) The autonomous support unit 121 transmits to the visitor migration communication control device 109, which is attached to the network B, the data packet including the autonomous packet transfer support check message 147 which holds the home address α and the temporary address β. The destination address of the data packet is the broadcast address shared by every network, such as an address where every bit is 1. The message 147 does not necessarily hold the home address α and the temporary address β although

they can be used in checking the security of the network if it does. Also the message 147 holding the home address α and the temporary address γ can take the place of a mobile host visit message 146, which will be described later.

(2) The autonomous support unit 114 in the visitor migration communication control device 109 responds to the autonomous support unit 121 with the response message 147R where broadcast address Bba is set and the autonomous flag F in the autonomous flag field 135 indicates 1 to inform that the device 109 provides the packet transfer service.

The mobile host 146 transmits the data packet to the visitor migration communication control device 109. The broadcast address Bba is employed as the destination address of the data packet and it is set in the response message 147R; however, this is not an obligation.

That is, when the response message 147R does not hold the broadcast address Bba, the following means can be employed. First, the broadcast address shared by every network can be employed, which is described in the above. Second, the source address, which is set in the header of the data packet comprising the response message 147R, can be employed. Third, a so called name service can be employed, where a server device on the network system informs the broadcast address Bba. Finally, when the address assigned to each of the devices, which are attached to the network, consists of the network address being unique for the network and a device address being unique for the devices, and the broadcast address on each network consists of such network address and the device address where the value of every bit is 1, the network address Bba can be generated by employing the network address included in the temporary address β of the mobile host 146.

(3) The address post unit 122 transmits to the home migration communication control device 101 the address post message 148. The message 148 includes the value 1 of the autonomous flag F, which is obtained from the response message, home address α, the temporary address β on the network B, and the broadcast address Bba, and the broadcast address Aba is the destination address of the address post message 148.

When the address post unit 107 in the home migration communication control device 101 receives the address post message 148, the mobile host transfer unit 104 stores in the home mobile host list hold unit 102 the temporary address β, the value 1 of the autonomous flag 1, and the broadcast address Bba by corresponding them to the home address α. Since the home address α had been stored as the temporary address before the temporary address β was stored, the mobile host transfer unit 104 knows that the mobile host 146 has migrated from the network A to the network B; therefore, it does not transmit the mobile host transfer message to the visitor migration communication control device 109,109'. That is, the data packet transmitted by the stationary host 151 to the home address α of the mobile host 146 is received by the home migration communication control device 101 and transferred thereby to the temporary address β; therefore, the visitor migration communication control device 109,109' is not employed here.

(4) The address post unit 107 notifies the address post unit 122 that it has received the address post message 148 by sending the response message 148R.

(5) Since the visitor migration communication control device 109 provides the packet transfer service, the mobile host visit unit 123 transmits to the visitor migration communication control device 109 the mobile host visit message 149 including the home address α and the temporary address β, so that the device 109 is notified that the mobile host 146 has migrated to the network B. The mobile host visit message 149 is destined for the broadcast address Bba.

The mobile host visit unit 113 in the visitor migration communication control device 109 receives the mobile host visit message 149 and stores into the visitor mobile host list hold unit 110 the home address α as well as the temporary address β. The temporary address β is stored also as the updated temporary address of the mobile host 146, which will be assigned when the mobile host 146 migrates from the network B to another network; thereby, the visitor migration communication control device 109 detects that the mobile host is currently attached to the network B.

(6) The mobile host visit unit 113 notifies the mobile host visit unit 123 by sending the response message 149R that it has received the mobile host visit message 149.

[communication between the stationary host 151 and the mobile host 146 on the network B]

The operation at the communication between the stationary host 151 and the mobile host 146 when the mobile host is attached to the network B is described hereunder with referring to FIGs. 30-33, which are relevant for FIGs.26-29.

(1) The application unit 161 in the stationary host 151 directs the transmission of the noncapsulated data packet, whose destination is the home address α, despite the migration of the mobile host 146. Immediately after the mobile host 146

migrates to the network B, that is, when the address hold unit 128 does not hold the home address α and the temporary address β, the transfer packet transmission unit 126 is not notified of the migration; therefore, it generates the noncapsulated data packet 152 and transmits it to the home address α in accordance with the direction from the application unit 151.

The noncapsulated data packet 152 is not received by the mobile host 146, which is not attached to the network A, but by the packet monitoring unit 106 in the home migration communication control device 101 since the home mobile host list hold unit 102 in the device 101 holds the home address α as well as the temporary address β, which coincides with the destination address of the noncapsulated data packet 152.

(2) The packet transfer unit 103 in the home migration communication control device 101 generates an encapsulated data packet including the noncapsulated data packet 152, which is received by the packet monitoring unit 106, and the packet transfer message 153, which informs the transfer of the noncapsulated data packet 152; and transmits it to the temporary address β. The packet transfer message 153 includes the value 0 in the field 133, which indicates that no response is requested, as well as the value 0 on the counter in the field 136, which indicates that the packet transfer message is the first message added to the noncapsulated data packet 152. As is described, no response is requested by the packet transfer message 153. That is, the application unit 161 of the stationary host 151 and the application unit of the mobile host 146, rather than the home migration communication control device 101 and the migration address unit 115, confirm that the mobile host 146 receives the noncapsulated data packet 152.

The transfer packet reception unit 118 in the mobile host 146 receives the encapsulated data packet including the packet transfer message 153 and the noncapsulated data packet 152, since it is destined for the temporary address β, which is held in the address hold unit 119. The unit 118 then detects that the destination address of the noncapsulated data packet 152 is the home address α, and sends the data etc. in the noncapsulated data packet 152 to the application unit 124.

Thus, the communication between the application unit 124 and the application unit 161 is not affected by the migration of the mobile host 146.

(3) The packet transfer unit 103 transmits the encapsulated data packet including the data packet transfer message. It also directs, after detecting that the autonomous flag F indicates 1, the mobile host transfer unit 104 to transmit to the stationary host 151 the data packet including the mobile host transfer message 154 where the home address α and the temporary address β are set. Finally, the unit 104 transmits the data packet to the stationary host 151.

The mobile host transfer unit 130 in the stationary host 151 receives the mobile host transfer message and stores into the address hold unit 128 the home address α and the temporary address β.

(4) The mobile host transfer unit 130 responds to the mobile host transfer unit 104 with the response message 154R.

(5) When the application unit 161 directs the transmission of the noncapsulated data packet to the home address α after the address hold unit 128 holds the home address α and the temporary address β, the transfer packet transmission unit 126 first generates a noncapsulated data packet destined for the home address α, then generates an encapsulated data packet including it and a packet transfer message 155. The encapsulated data packet is then transmitted to the temporary address β. Thus, once the home migration communication control device 101 notifies the stationary host 151 of the home address α and the temporary address β, the stationary host 151 is able to transmit the data packet to the temporary address β of the mobile host 146, and the home migration communication control device 101 is not employed.

On the other hand, when data is transmitted from the mobile host 146 to the stationary host 151, the Sa is employed as the destination address α and the home address is employed as the source address; and the noncapsulated data packet is transmitted from the address α to the address Sa.

Thus, even when all the noncapsulated data transmitted by the stationary host 151 is destined for the home address α, the home migration communication device 101 transfers the data to the updated temporary address of the mobile host; thereby, the communication between the mobile host 146 and the stationary host 151 is implemented, and the conventional device can be employed as the stationary host 151, which broadens a practicability of the network system.

Whereas, when the network system checks the original source address of the data packet or a transfer path of the data packet, the transmission unit may be built in the mobile host 146 like the transfer packet transmission unit 126 in the stationary host 151, and also the reception unit may be built in the stationary host 151 like the transfer packet reception unit 118 in the mobile host 146; and the encapsulated data packet including the packet transfer message and the noncapsulated data packet may be transmitted therebetween.

[migration from network B to network C]

The operation at the migration of the mobile host 146 from the network B to the network C is described hereunder with referring to FIGs. 34-37, relevant for FIGs. 26-29.

(1)-(4) The operation related to transmission of an autonomous packet transfer support check message 147', a response message 147R', an address post message 148', and a response message 148' between the mobile host 146 and the visitor migration communication control device 109' is substantially same as the operation related to transmission of messages between the mobile host 146 and the visitor migration communication control device 109, which is conducted when the mobile host 146 migrates to the network B. However, the operation at the migration from the network A to the network B and the operation at the migration from the network B and the network C are different from each other in part of the operation of the home migration communication control device 101 conducted after it responds to the received address post message 148' with the response message 148R.

(5) When the address post unit 107 receives the address post message 148', the mobile host transfer unit 104 in the home migration communication control device 101 detects that the mobile host been attached to the network B before migrating to the network C since the temporary address β has been stored as the temporary address. Then, the mobile host transfer unit 104 sends to the visitor migration communication control device 109 the data packet including both the home address α and the temporary address γ, so that the device 109 transfers the data packet transmitted by the stationary host 151 from the temporary address β to the temporary address γ. The data packet received by the visitor migration communication control device is destined for the broadcast address Bba.

In accordance with the address post message 148', the mobile host transfer unit 104 stores into the home move host list hold unit 102 the temporary address γ, the value 1 of the autonomous flag F, and the broadcast address Cba by corresponding them to the home address α.

Receiving the data packet including the mobile host transfer message 150, the mobile host transfer unit 112 in the visitor migration communication control device 109 stores into the visitor mobile host list hold unit 110 the temporary address γ newly assigned to the mobile host 146 and the value 1 of the autonomous flag F by corresponding them to the home address α.

(6) The mobile host transfer unit 112 notifies the mobile host transfer unit 104 that it has received the mobile host transfer message 150 by sending thereto the response message 150R.

(7), (8) The transmission of a mobile host visit message 149' and a response message 149R' between the mobile host 146 and the visitor migration communication control device 109', which is conducted when the device 109' provides the packet transfer service, is substantially same as the transmission of messages between the mobile host 146 and the visitor migration communication control device 109, which is conducted when the mobile host 146 migrates to the network B.

[communication between mobile host 146 attached to network C and stationary host 151]

Transmission of the data packet from the stationary host 151 to the mobile host 146 when the mobile host is attached to the network C is described with referring to FIG. 38-41, which are relevant for FIG. 26-29.

The transmission is substantially same as the transmission between the stationary host 151 and the mobile host 146 when the mobile host 146 is attached to the network B, except that the visitor migration communication control device 109 instead of the home migration communication control device 101 is employed.

(1) When the stationary host 151 is not notified that the mobile host 146 has migrated from the network B to the network C, the stationary host 151 generates the encapsulated data packet including the noncapsulated data packet, which is destined for the home address α, and the packet transfer message 156; then transmits it to the temporary address β. This is substantially the same as (5) in the communication between the stationary host 151 and the mobile host 146 attached the network B.

The data packet transmitted by the stationary host is not received by the mobile host 146 since the mobile host is not attached to the network B. The data packet is received by the packet monitoring unit 106 in the visitor migration communication control device 109 since the visitor mobile host list hold list unit thereof holds the temporary address β besides the temporary address γ.

(2) The visitor migration communication control device 109 transmits to the temporary address γ of the mobile host 146 the data packet including the packet transfer message 157, which is substantially same as (2) in the communication between the stationary host 151 and the mobile host 146 on the network B except a difference described hereunder.

The home mobile host migration communication control device 101 receives the noncapsulated data packet 152 and generates an encapsulated data packet comprising the received noncapsulated data packet 152 and the packet transfer message 153. On the other hand, the visitor migration communication control device 109 receives the encapsulated data packet comprising the packet transfer message 156 and the packet transfer unit 111 converts the data packet by changing the destination address from the temporary address β into the temporary address γ as well as converting the packet transfer message 156 into the packet transfer message 157, whose value on the counter is incremented by 1.

(3)-(5) The visitor migration communication control device 109, the stationary host 151, and the mobile host 146 on the network C operate substantially same as the home migration communication control device 101, the stationary host 151, and the mobile host 146 on the network B, which is described the above in (3)-(5); thereby the mobile host transfer message 158 and the response message 158R are transmitted, and the data packet including the packet transfer message 160 is transmitted by the stationary host 151 to the mobile host 146 attached to the network C.

If the stationary host 151 does not transmit any data packet to the mobile host 146, which is attached to the network B, the stationary host is not notified of either the temporary address β or the temporary address γ; therefore, the stationary host 151 transmits the data packet to the home address α even when the mobile host 146 has migrated from the network B to the network C. When this occurs, the home migration communication control device 101, as does the visitor migration communication device 109, transfers the data packet from the home address α to the temporary address γ; then notifies the stationary host 151 of the updated temporary address γ of the mobile host 146 so that the stationary host 151 will be able to directly transmit the data packet, which comprises the packet transfer message, to the mobile host 146 attached to the network C.

Further, when the mobile host 146 migrates to the network, to which the visitor migration communication control device is attached to provide the packet transfer service, the stationary host 151 may transmit the data packet destined for any of the addresses α, β, or γ. When the data packet is transmitted to the home address α or the temporary address γ, the home migration communication control device 101 or the visitor migration communication control device 109', which is notified of the updated temporary address of the mobile host 146, transfers the data packet to the updated temporary address; then it notifies the stationary host 151 of the updated temporary address of the mobile host.

When the data packet is transmitted to the temporary address β of the mobile host 146, the visitor migration communication control device 109 receives it. Since the device 109 is notified of only the temporary address γ, it transmits the data packet comprising the packet transfer message to the temporary address γ as well as transmits the mobile host transfer message to notify the stationary host 151 of the temporary address γ. The visitor migration communication control device 109' receives the data packet comprising the packet transfer message, which is destined for the temporary address γ, and transmits it to the updated temporary address of the mobile host 146; then transmits the mobile host transfer message to notify the stationary host 151 of the updated temporary address. Also the visitor migration communication control device 109' obtains the address of the visitor migration communication control device 109 from the source address of data packet transmitted thereby, and transmits the mobile host transfer message to the device 109. Thus, the visitor migration communication control device 109' obtains the updated temporary address of the mobile host 146, and transfers the data packet to the mobile host 146 as well as notifies stationary host 151 of the obtained updated temporary address.

[communication operation 2]

Another example of the communication operation is described hereunder. In the communication operation 2 the visitor migration communication control device 109 does not provide the packet transfer service when the mobile host 146 migrates from the network A to the network B, further from the network B to the network C.

As shown in FIG. 42, when the device 109 does not provide the packet transfer service, the autonomous packet transfer support check message 181, transmitted by the mobile host 146 which has migrated from the network A to the network B, is responded with the response message 181R where the autonomous flag F in the autonomous flag field 135 indicates 0. Thereby, the autonomous flag field 135 in the address post message 182, which is transmitted by the mobile host 146 to the home migration communication control device 101, obtains the value 0, and the value 0 is held in the home mobile host list hold unit 102 in the device 101. The mobile host 146 does not transmit the mobile host visit message to the visitor migration communication control device 109.

As shown in FIG. 43, receiving from the stationary host 151 the noncapsulated data packet 183, which is destined for the home address α, the home migration communication control device generates the encapsulated data packet comprising the received noncapsulated data packet 183 and the packet transfer message 184, and transmits it to the temporary address β, as is in the communication operation 1.

However, recognizing the value 0 on the autonomous flag F, which is held in the home mobile host list hold unit 102, the device 101 does not transmit to the stationary host 151 the mobile host transfer message including the temporary address β. Therefore, every data packet transmitted by the stationary host 151 is destined for the home address α, and it is transferred to the mobile host 146 by the home migration communication control device 101. Thus, the stationary host 151 is not notified of the temporary address β since the data packet transmitted to the address other than the home address α is not transferred by the device 109; therefore it is not received by the mobile host 146 when it departs the network B to migrate to the network C.

When the visitor migration communication control device 109', which is attached to the network, provides the packet transfer service, the home migration communication control device 101 notifies the stationary host 151 of the temporary address γ when it transmits the noncapsulated data to the home address α, so that the stationary host 151 is able to directly transmit the data packet comprising the noncapsulated data packet and the packet transfer message to the mobile host 146 on the network C.

When the visitor migration communication control device 109 does not provide the packet transfer service, the home migration communication control device 101 does not necessarily notify the device 109 of the temporary address γ of the mobile host 146 assigned when it has migrated from the network B to the network C. However, the construction of the device 101 will be simplified if it conducts the same operation either or not the packet transfer service is provided since the visitor migration communication control device 109 ignores the mobile host transfer message.

Also the device 109 may respond to the autonomous packet transfer support check message 181 only when it provides the data packet transfer service; therefore, the presence or absence of the response message 181R indicates to the mobile host 146 whether or not the data packet transfer service is provided. In the above operation the value 0 of the autonomous F also indicates that the packet transfer service is not provided, whereas absence of the response message to the message 181 can indicate the absence of the packet transfer service, which will simplify construction of mobile host 146.

[communication operation 3]

The final example of the communication operation is described hereunder. In the communication operation 3 the visitor migration communication control device 109' does not provide the packet transfer service while the visitor migration communication control device 109 does.

As shown in FIG. 44, when the packet transfer service is not provided by the visitor migration communication control device 109', the mobile host 146 transmits to the home migration communication control device 101 the address post message 182' where the value 0 is set at the autonomous flag F. Then, the home migration communication control device 101 transmits to the device 109 the mobile host transfer message 185 by setting the value 0 at the autonomous flag F.

When detecting the value 0 at the autonomous flag F, the visitor migration communication control device 109 ceases to provide the packet transfer service.

As shown in FIG. 45, even after cease of the data packet transfer service, the stationary host 151 may transmit to the temporary address the data packet comprising the noncapsulated data packet and the packet transfer message 186.

When this happens, the visitor migration communication control device 109 obtains the noncapsulated data packet 187 from the received encapsulated data packet and transmits it to its destination address, the home address α. The noncapsulated data packet 187 is then received by the home migration communication control device 101, which is attached to the network A. Finally, the home migration communication control device 101 transfers the noncapsulated data packet 187 together with the packet transfer message 188 to the temporary address γ of mobile host 146, which is attached to the network C.

The visitor migration communication control device 109 notifies the stationary host 151 that the mobile host 146 is attached to the network A instead of the network C by sending the mobile host transfer message 189 where the home address α is set in the temporary address field 139. Then, the stationary host 151 transmits the noncapsulated data packet 187 to the home address α, and it is transferred by the home migration communication control device 101, which is employed to take the place of the visitor migration communication control device 109. As another option, the device 109 may send the mobile host transfer message 189 where the invalid address is set, such as the address where every bit is 1. Then, the home migration communication control device 101 may notify the stationary host 151 of the home address α in accordance with the address inquiry obtained from the stationary host 151.

The operation described the above will be employed when the visitor migration communication control device 109 ceases to provide the packet transfer service operation regardless whether or not the device 109' provides the packet transfer service.

On the other hand, the visitor migration communication device 109 may restart the packet transfer service even when the device 109' ceases to provide the service.

In this case, the home migration communication control device 101 needs to provide the visitor migration communication control device 109 with the updated temporary address at every migration of the mobile host 146 unless the mobile host migrates to the network to which another visitor migration communication control device is attached and provides the packet transfer service. To realized it, for example, when the value of the autonomous flag F in the address post message is 0 to indicate that the device 109' does not provide the packet transfer service, the broadcast address Bba as the destination address of the mobile host transfer message, which is transmitted to the device 109, will not be renewed.

Additionally, the broadcast address as the destination address of the data packet, which is transmitted by the mobile host 146, can be replaced with the address Ha, Va, Va', each of which is unique to each device. The address unique to each device will be obtained by detecting the source address of the data packet received from each device, or by employing a so called name service.

Also in the second embodiment, the home migration communication control device 101 detects whether or not the mobile host 146 is attached to the same network from what is held as the temporary address in the address hold unit; to be precise, whether or not the home address α is held as the temporary address. However, this can also be detected by knowing in which table the temporary address is held. For example, when the device 101 and the mobile host 146 are attached to the same network, the first table holds the addresses, such as the home address α; whereas, the second table holds the addresses when the device 101 and the mobile host 146 are attached to the different network from each other. Value of the autonomous flag F, 0 or 1, can also be utilized in the same way.

Further, the home migration communication control device 101 and the visitor migration communication control device 109, 109' may be employed as a host such as the mobile host 146 or the stationary host 151.

Finally, the home migration communication control device 101, the visitor migration communication control device 109, the mobile host 146, and the stationary host 156 may be constructed identically and can be replaced with each other.

Although in the embodiment the application unit 124 starts its operation before being notified of updated temporary address β; therefore it always transmits the data packet to the home address α of the mobile host 146, it can transmit the data to the temporary address β if is starts its operation after obtaining the temporary address β.

Although the present invention has been fully described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless otherwise such changes and modifications depart from the scope of the present invention, they should be constructed as being included therein.

Claims

1. A migration communication control device constructed to control a communication between a mobile node and a partner node, the mobile node migrating across networks and obtaining an address assigned on each network while the partner node being a communication partner of the mobile node, comprising a first migration control unit, a second migration control unit, a third migration control unit, the second migration control unit being placed on the mobile node and the third migration control unit being placed on the partner node,

   wherein the first migration control unit comprises:

   packet transfer means for receiving a packet which was destined for an outdated address of the mobile node, the outdated address assigned when the mobile node migrated to a network to which the first migration control unit is attached, generating a conversion packet which holds an updated address instead of the outdated address, and transmitting the conversion packet; and

   address post means for transmitting an address post message which indicates the updated address of the mobile node to the third migration control unit, the third migration control unit transmitting the packet received by the packet transfer means, and

   the second migration control unit comprises:

   migration post means for transmitting to the first migration control unit a migration post message which indicates the updated address of the mobile node when the mobile node migrates to another network; and

   packet resumption means for receiving the conversion packet from both the first migration control unit and the third migration control unit and resuming an original packet from the conversion packet, and

   the third migration control unit comprises:

   packet conversion means for converting a destination address of a packet, the packet to be transmitted to the mobile node, into the updated address indicated by the address post message, the address post message sent by the first migration control unit, and transmitting it to the mobile node.

2. The migration communication control device of Claim 1, wherein the migration post means in the second migration control unit transmits an identification key included in the migration post message, the identification key being employed to identify the mobile node.

3. The migration communication control device of Claim 2, wherein the identification key is an address of the mobile node assigned at one network before the network to which the mobile node is currently attached.

4. The migration communication control device of Claim 2, wherein the identification key is an address of the mobile node assigned before its initial migration.

5. The migration communication control device of Claim 1; wherein the second migration control unit is constructed to transmit to the third migration control unit the packet which has the same format as the resumed packet.

6. The migration communication control device of Claim 1, wherein the first migration control unit further comprises:
address hold means for holding the outdated address and the updated address by corresponding them with each other; and
address comparison means for comparing the destination address of the received packet with the outdated address, wherein
the packet transfer means generates the conversion packet and transmits it when the address comparison means detects that the destination address of the received packet coincides with the outdated address.

7. The migration communication control device of Claim 1, wherein the first migration control unit further comprises:
address hold means for holding the outdated address and the updated address by corresponding them with each other; and
address comparison means for comparing the destination address of the packet received by the packet transfer means with the outdated address, wherein
the address post means transmits the address post message which indicates the updated address of the mobile node to the third migration control unit, the third migration control unit transmitting the packet received by the packet transfer means, when the address comparison means detects that the destination address of the packet coincides with the outdated address.

8. The migration communication control device of Claim 1, wherein the second migration control unit further comprises:
address hold means for holding the outdated address and the updated address by corresponding them with each other; and
address comparison means for comparing the updated address with the destination address of the packet received from one of the first migration control unit and the third migration control unit, wherein
the packet resumption means resumes the original packet from the conversion packet when the address comparison means detects that the updated address coincides with the destination address of the packet received from one of the first migration control unit and the third migration control unit.

9. The migration communication control device of Claim 1, wherein the third migration control unit further comprises:
address hold means for holding the outdated address and the updated address of the mobile node by corresponding them with each other; and
address comparison means for comparing the outdated address in the address hold means with the destination address of the packet to be transmitted to the mobile node, wherein
the packet conversion means converts the destination address of the packet to be transmitted to the mobile node into the updated address which corresponds to the outdated address in the address hold means when the address comparison means detects the outdated address in the address hold means coincides with the destination address of the packet.

10. The migration communication control device of Claim 1, wherein there are a plurality of the first migration control units, and the second migration control unit transmits the migration post message to at least one of the first migration control units.

11. The migration communication control device of Claim 10, wherein the migration post means in the second migration control unit transmits the migration post message to the first migration control unit which is attached to the network to which the mobile node was attached before its migration,
each of the first migration control units has migration post means for transmitting to one of the other first migration control units a migration post message to post the same address as the

updated address indicated by the migration post message received from the second migration control unit, and

each of the first migration control units has migration post means for transmitting a migration post message from one of the other first migration control units to another first migration control unit to post the same address as the updated address indicated by the received migration post message.

12. The migration communication control device of Claim 11, wherein each of the first migration control units and the second migration control unit further comprise pointer hold means for holding pointers related to the first migration control unit to which the migration post message is transmitted, and wherein

the migration post means in each of the first migration control units and the migration post means in the second migration control unit transmit the migration post message to each of the addresses related to each of the pointers.

13. The migration communication control device of Claim 12, wherein each of the pointers is a broadcast address of the network to which one of the first migration control units is attached.

14. The migration communication control device of Claim 12, wherein each of the pointers is an address which is assigned to one of the first migration control units uniquely.

15. The migration communication control device of claim 12, wherein each of the pointers is the address of the mobile node which is assigned when the mobile node is attached to the same network as is the first migration control unit, and

the migration post means in the first migration control unit and the migration post means in the second migration control unit obtain the broadcast address of the network to which each of the first migration control units is attached with referring to the address of the mobile node, and transmits the migration post message to the obtained broadcast address.

16. The migration communication control device of Claim 12, wherein the pointer hold means in the second migration control unit holds a pointer related to a first migration control unit for the latest migration, which is the first migration control unit being attached to one network before the network to which the mobile node is currently attached, and

the pointer hold means in the first migration control unit holds a pointer related to another first migration control unit attached to the same network as was the mobile node attached before migrating to the network to which the first migration control unit is attached.

17. The migration communication control device of Claim 12, wherein the second migration control unit further transmits to the first migration control unit the pointer by sending thereto the migration post message, the pointer to be held by the first migration control unit.

18. The migration communication control device of Claim 17, wherein the first migration control unit stores into the pointer hold means the pointer when it receives from the second migration control unit the migration post message by corresponding the pointer with the updated address indicated by the received migration post message.

19. The migration communication control device of Claim 11, wherein each of the first migration control units further comprises:

address hold means for holding the outdated address and the updated address by corresponding them with each other, wherein

migration post message means stores into the address hold means the outdated address and the updated address by corresponding them with each other when it receives from the second migration control unit the migration post message, while converts the updated address in the address hold means into the updated address indicated by the migration post message when it receives from the first migration control unit the migration post message and the outdated address indicated by the migration post message coincides with one of the updated addresses in the address hold means.

20. The migration communication control device of Claim 1, wherein the first migration control unit is placed on a gateway, which connects networks.

21. The migration communication control device of Claim 1, wherein the first migration control unit is placed on the network as an individual node.

22. The migration communication control device of Claim 10, wherein the migration post means in the second migration control unit transmits the migration post message to a home migration control unit, the home migration control unit being the first migration control unit which is attached to a network where the mobile node left for its initial migration, and

the home migration control unit further

comprises home migration post means for transmitting a migration post message to a first migration control unit for the latest migration, the first migration control unit for the latest migration being the first migration control unit which is attached to the network where the mobile node left for the latest migration, to post the same updated address as is indicated by the migration post message received from the second migration control unit.

23. The migration communication control device of Claim 22, wherein the first migration control unit further comprises migration post means for transmitting the migration post message indicating the updated address of the mobile node to one of the other first migration control units when the conversion packet destined for the outdated address of the mobile node was sent therefrom to the first migration control unit.

24. The migration communication control device of Claim 22, wherein the migration post means in the second migration control unit transmits to the home migration control unit the migration post message where a home address and the updated address are corresponded with each other, the home address assigned when the mobile node is attached to the same network as is the home migration control unit,

and each of the packet transfer means and the address post means in the home migration control unit transmits the conversion packet and the address post message respectively with referring to the above home address and the updated address.

25. The migration communication control device of Claim 24, wherein the second migration control unit further comprises an outdated address post means for transmitting to the first migration control unit for the latest migration an outdated address post message where the outdated address and the home address are corresponded with each other, the outdated address being assigned to the mobile node before the latest migration,

the home migration post means in the home migration control unit transmits to the said first migration control unit for the latest migration the migration post message where the above home address and the updated address are corresponded with each other, and

the packet transfer means and the address post means in the first migration control unit for the latest migration transmit the conversion packet and the address post message respectively in accordance with the outdated address and the updated address, the outdated address and the updated address being corresponded with each other via the home address.

26. The migration communication control device of the Claim 25, wherein the outdated address post means in the second migration control unit transmits the above outdated address post message at a migration of the mobile node preceding the latest migration, and

each of the migration post means in the second migration control unit and the home migration post means in the home migration control unit transmits the above migration post message at the latest migration of the mobile node.

27. The migration communication control device of Claim 22, wherein the second migration control unit further comprises home migration control unit pointer hold means for holding a pointer related to the home migration control unit,

the migration post means in the second migration control unit transmits the migration post message to the address related to the pointer,

the home migration control unit further comprises pointer hold means for the latest migration for holding a pointer related to the first migration control unit for the latest migration, and

the home migration post means in the home migration control unit transmits the migration post message to the address related to the pointer.

28. The migration communication control device of Claim 27, wherein each of the above pointers is the broadcast address of the network to which each of the first migration control units is attached.

29. The migration communication control device of Claim 27, wherein each of the above pointers is the address assigned to each of the first migration control units uniquely.

30. The migration communication control device of Claim 27, wherein the second migration control unit further comprises pointer obtainment means for requesting to the first migration control unit for the latest migration the pointer related to the first migration control unit for the latest migration, and

the migration post means in the second migration control unit posts the obtained pointer to the home migration control unit together with the updated address by sending thereto the migration post message.

31. The migration communication control device of Claim 30, wherein the migration post means in the second migration control unit posts to the home migration control unit the pointer at the migration of the mobile node preceding the latest migration, while the migration post means posts the above updated address at the latest migration of the mobile node.

32. The migration communication control device of Claim 22, wherein the first migration control unit further comprises address post suppressing means for suppressing transmission of the address post message from the address post means to the third migration control unit, and

the address post suppressing means suppresses transmission of the address post message when none of the first migration control units is attached to the same network as is the mobile node.

33. The migration communication control device of Claim 32, wherein the second migration control unit further comprises detect means for detecting whether or not the first migration control unit is attached to the network to which the mobile node migrates,

the migration post means in the second migration control unit transmits to the home migration control unit the migration post message which includes the detecting result of the above detect means together with the updated address,

the home migration post means in the home migration control unit transmits to the first migration control unit for the latest migration the migration post message which includes the detecting result of the above detect means together with the updated address, and

the address post suppressing means in each of the home migration control unit and the first migration control unit for the latest migration suppress the transmission of the address post message in accordance with the detecting result of the above detect means.

34. The migration communication control device of Claim 22, wherein the first migration control unit further comprises packet transfer suppressing means for suppressing transfer of the packet conducted by the packet transfer means.

35. The migration communication control device of Claim 34, wherein the first migration control unit further comprises address post suppressing means for suppressing transmission of the address post message from the address post means to the third migration control unit, and the address post suppressing means in the first migration control unit being attached to a network to which the mobile node is not attached, suppresses the transmission of the address post message when the packet transfer suppressing means in the first migration control unit for the latest migration suppresses transfer of the packet.

36. The migration communication control device of Claim 35, wherein the second migration control unit further comprises detect means for detecting whether or not the packet transfer suppressing means in the first migration control means suppresses the transfer of the packet, the first migration control means being attached to the network to which the mobile node migrates, and

the migration post means in the second migration control unit transmits to the home migration control unit the migration post message which includes the detecting result of the above detect means together with the updated address,

the home migration post means in the home migration control unit transmits to the first migration control unit for the latest migration the migration post message which includes the detecting result of the detect means together with the updated address, and

the address post suppressing means in each of the home migration control unit and the first migration control unit for the latest migration suppresses the transmission of the address post message in accordance with the detecting result of the above detect means.

37. The communication control device of Claim 36, wherein the packet transfer suppressing means in the first migration control unit for the latest migration suppresses the transfer of the packet conducted by the packet transfer means, when the packet transfer suppressing means in the first migration control unit being attached to the network to which the mobile node migrates suppresses the transfer of the packet.

38. A packet transfer migration control unit in a migration communication control device, the migration communication control device being constructed to control a communication between a mobile node and a partner node, the mobile node migrating across networks and obtaining an address assigned on each network while the partner node being a communication partner of the mobile node, comprising:

packet transfer means for receiving a packet which was transmitted by the partner node to an outdated address of the mobile node, the outdated address being assigned when the mobile node migrated to a network to which the packet transfer migration control unit is attached, generating a conversion packet which holds an updated address instead of the outdated address, and transmitting the conversion packet;

and

address post means for transmitting an address post message which indicates the updated address of the mobile node to the partner node, the partner node transmitting the packet received by the packet transfer means.

39. A mobile node migration control unit in a migration communication control device, the migration communication control device being constructed to control a communication between a mobile node which migrates across networks and obtains an address assigned on each network and a partner node which is a communication partner of the mobile node, being placed on the mobile node and comprising:

migration post means for transmitting to a packet transfer migration control unit a migration post message which indicates an updated address of the mobile node when the mobile node migrates to another network, the packet transfer migration control unit for receiving a packet which was transmitted by the partner node to an outdated address of the mobile node, the outdated address assigned when the mobile node migrated to a network to which the migration control unit for packet transfer is attached, generating a conversion packet which holds the updated address instead of the outdated address, and transmitting the conversion packet; and

packet resumption means for receiving the conversion packet from both the packet transfer migration control unit and the mobile node, and resuming an original packet from the conversion packet.

40. A partner node migration control unit in a migration communication control device, the migration communication control device being constructed to control a communication between a mobile node which migrates across networks and obtains an address assigned on each network and a partner node which is a communication partner of the mobile node, being placed on the mobile node and comprising:

address post message receiving means for receiving an address post message which indicates an updated address of the mobile node from a packet transfer migration control unit, the packet transfer migration control unit transmitting an address post message which indicates the updated address of the mobile node to the partner node; and

packet conversion means for converting a destination address of a packet, the packet to be transmitted to the mobile node, into the updated address indicated by the address post message, and transmitting it to the mobile node.

FIG. 1

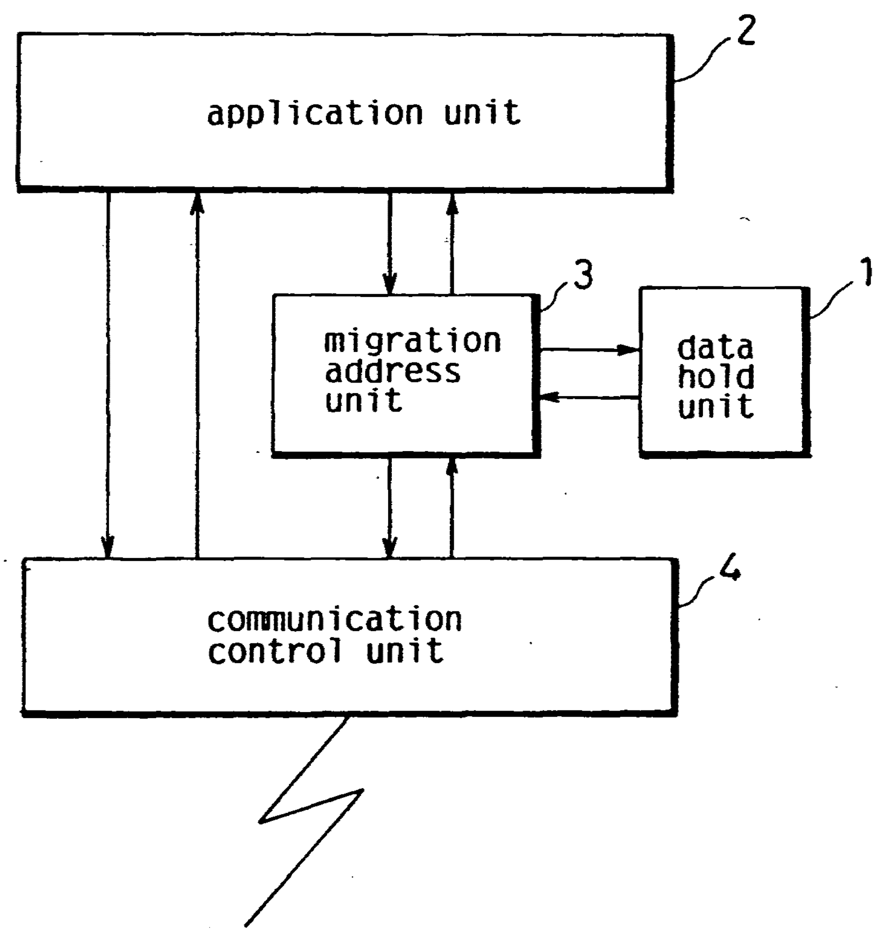

2
application unit
3
migration address unit
1
data hold unit
4
communication control unit

FIG. 2

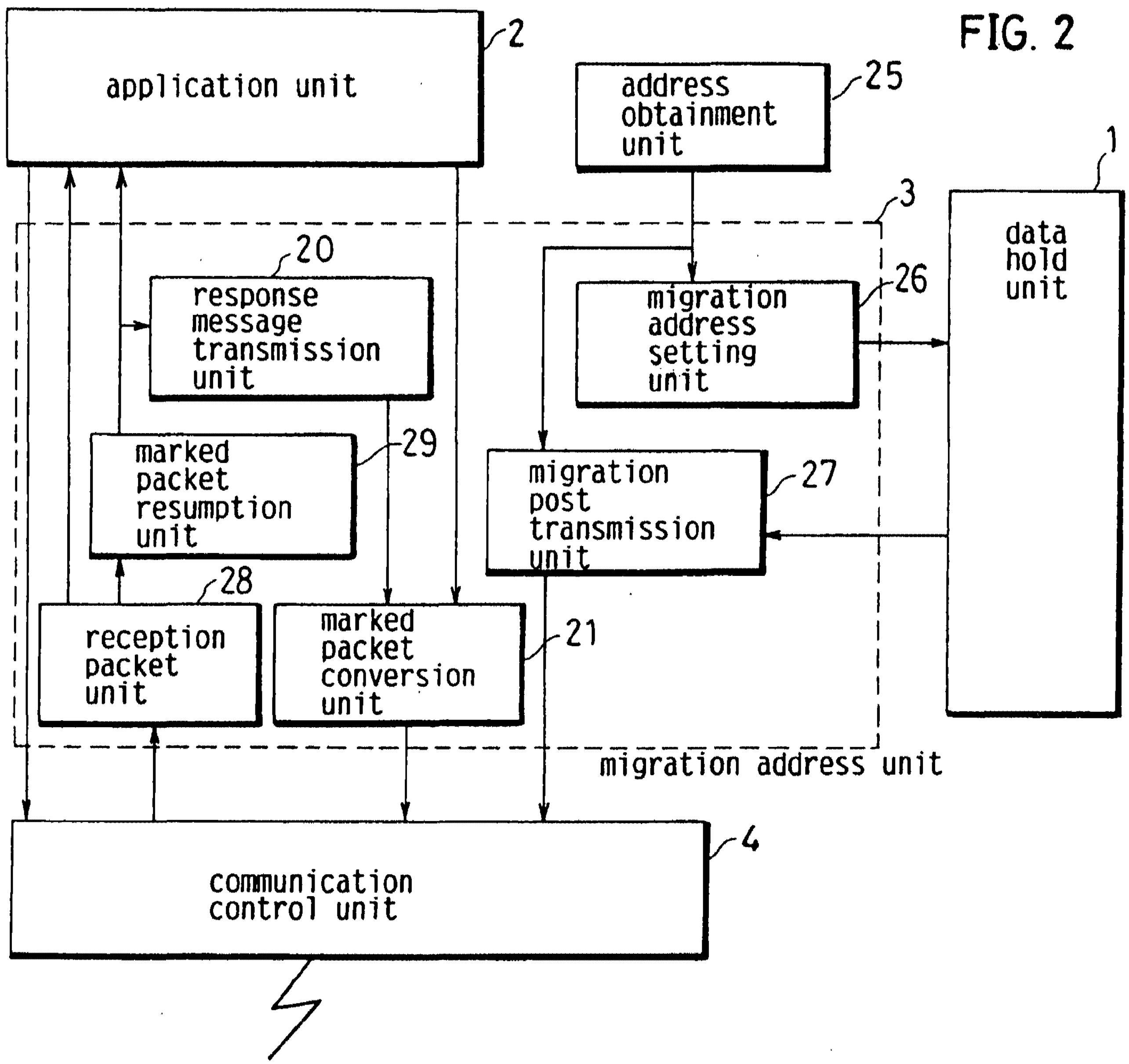

application unit
2
address obtainment unit
25
1
3
data hold unit
20
response message transmission unit
migration address setting unit
26
marked packet resumption unit
29
migration post transmission unit
27
28
reception packet unit
marked packet conversion unit
21
migration address unit
communication control unit
4

FIG. 3

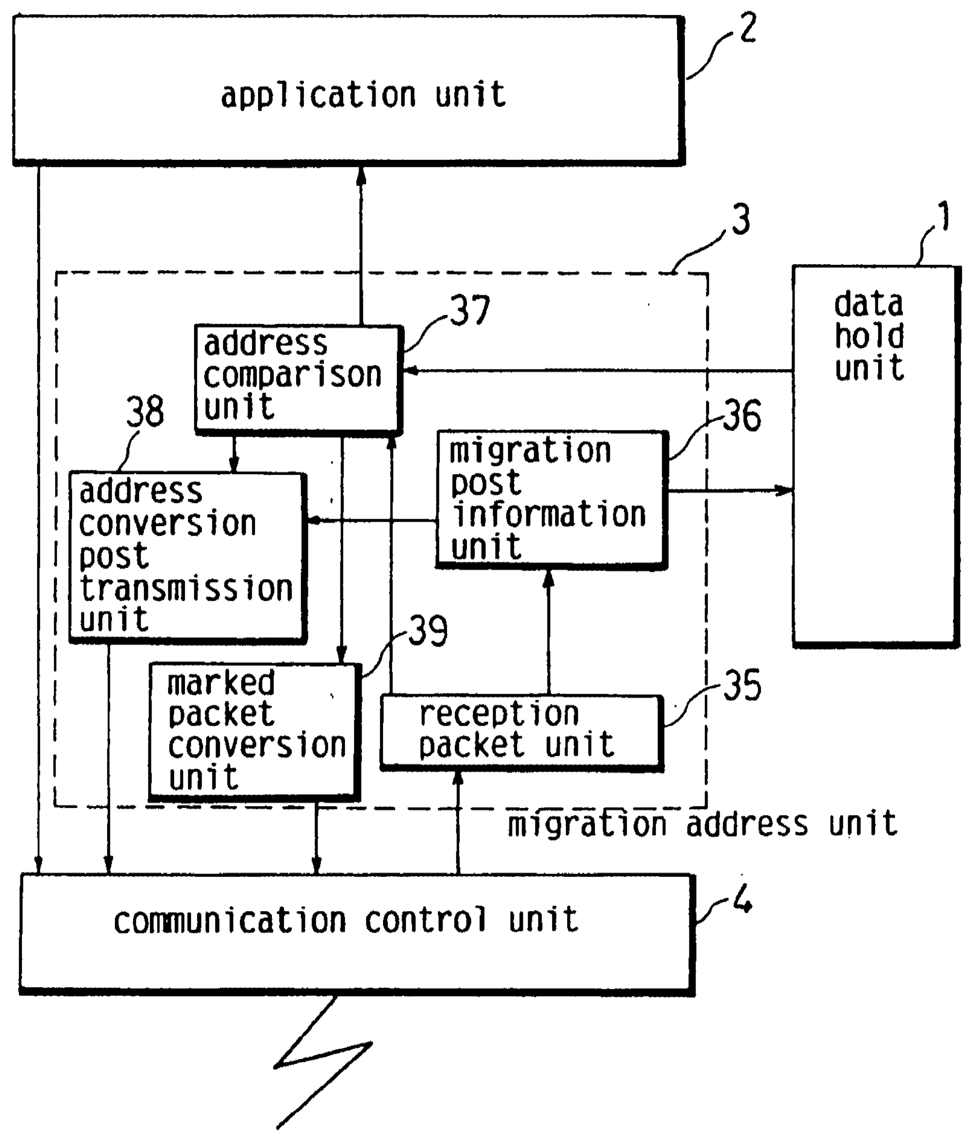

application unit
2
3
1
data hold unit
37
address comparison unit
38
address conversion post transmission unit
36
migration post information unit
39
marked packet conversion unit
35
reception packet unit
migration address unit
communication control unit
4

FIG. 4

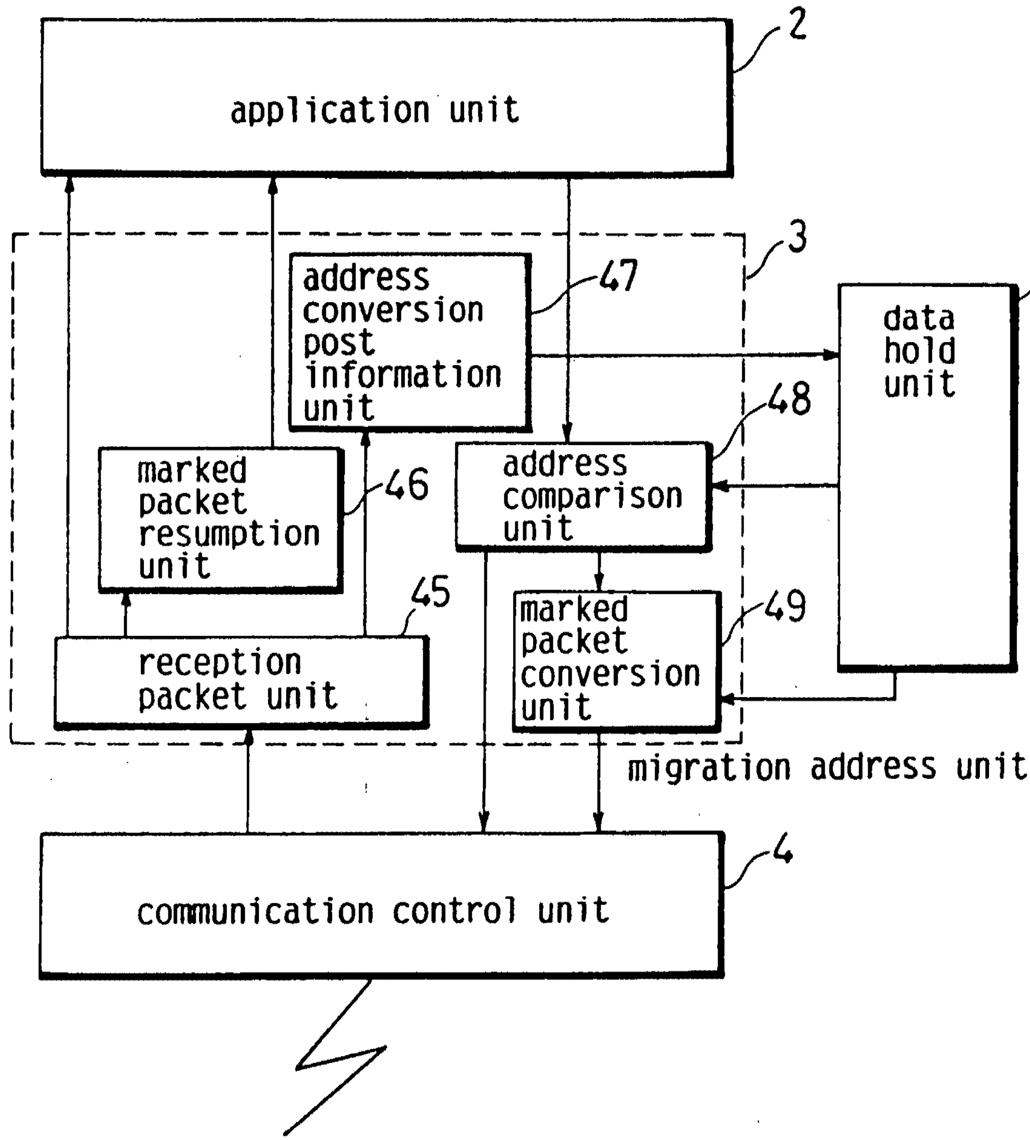

2
application unit
3
1
address conversion post information unit
47
data hold unit
48
address comparison unit
marked packet resumption unit
46
45
marked packet conversion unit
49
reception packet unit
migration address unit
4
communication control unit

FIG. 5

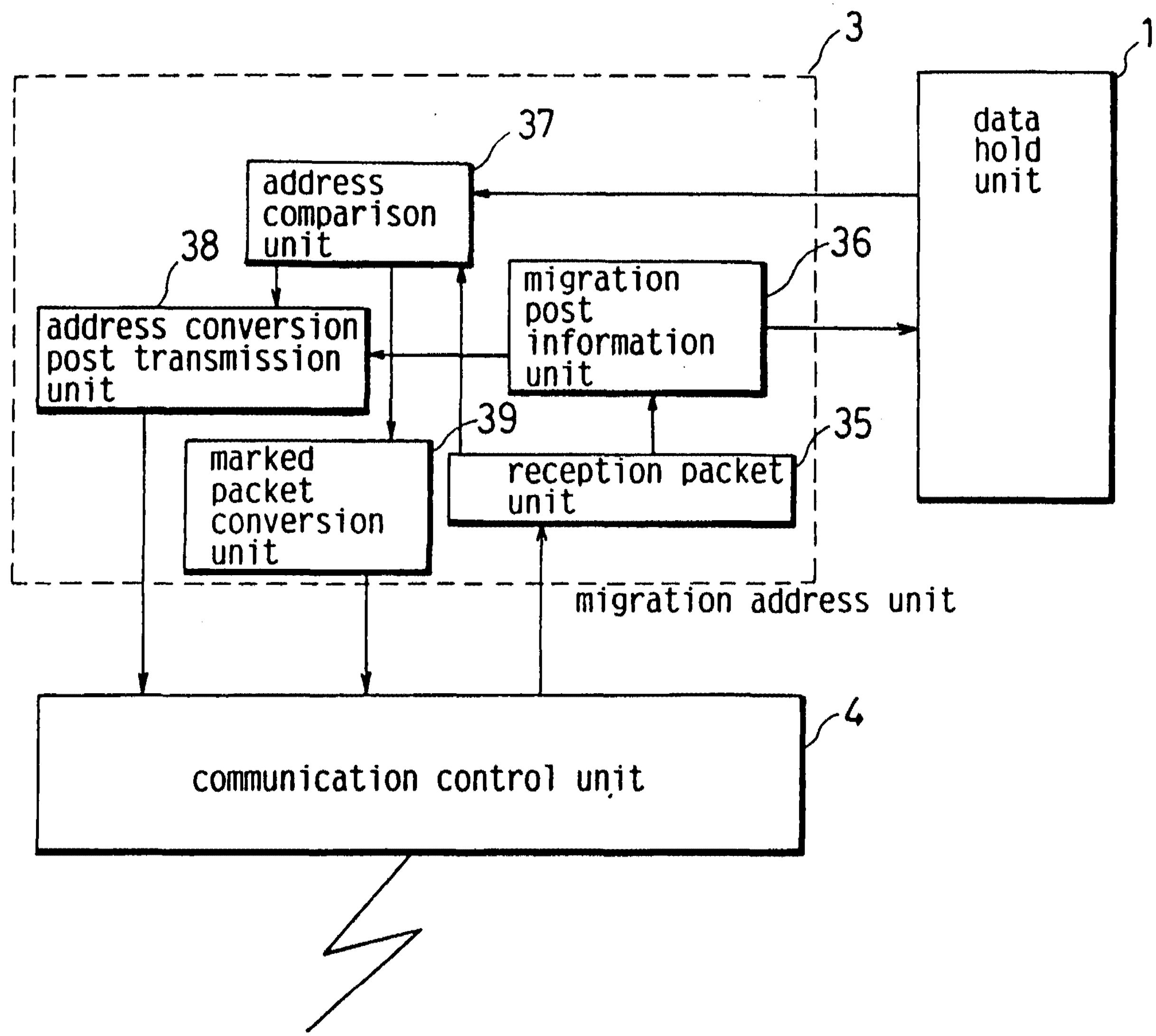

3
1
data hold unit
37
address comparison unit
38
36
address conversion post transmission unit
migration post information unit
39
35
marked packet conversion unit
reception packet unit
migration address unit
4
communication control unit

FIG. 6

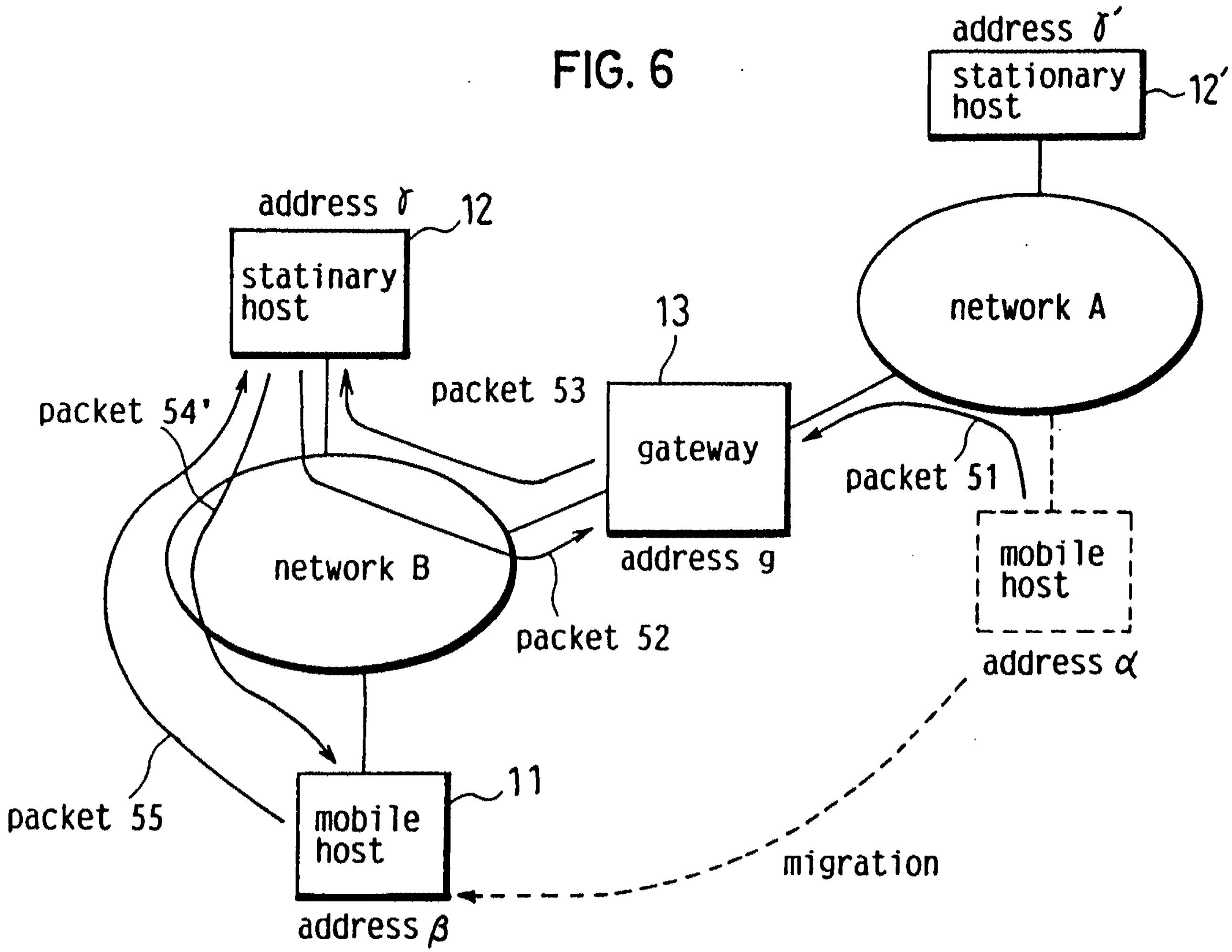
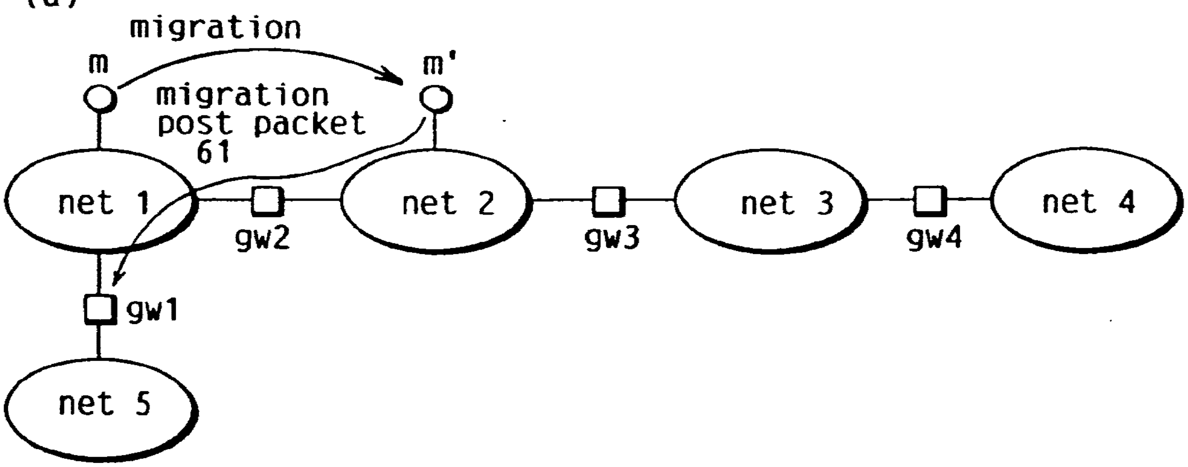
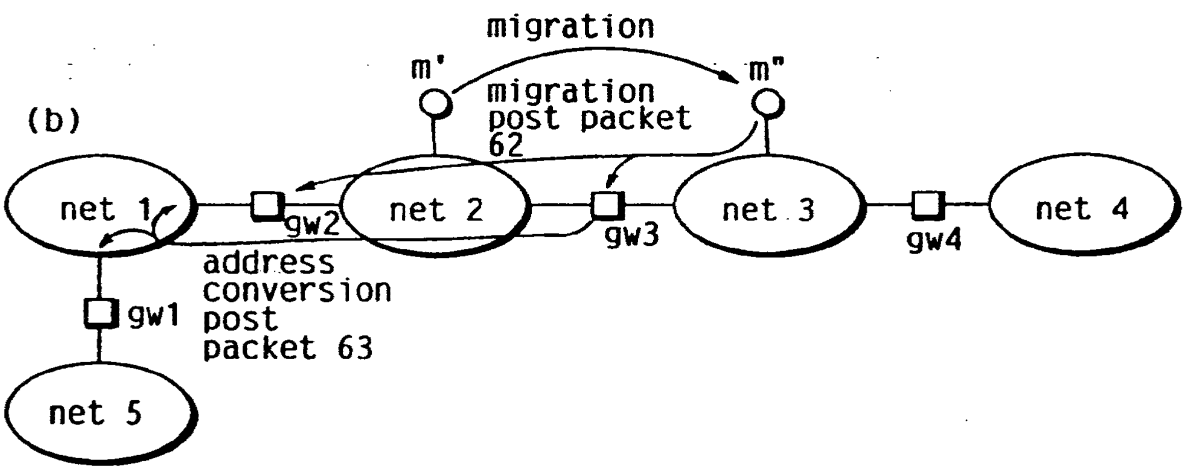

address γ'
stationary host
12'
address γ
12
statinary host
13
packet 53
gateway
network A
packet 54'
packet 51
network B
address g
mobile host
packet 52
address α
11
packet 55
mobile host
migration
address β

FIG. 7

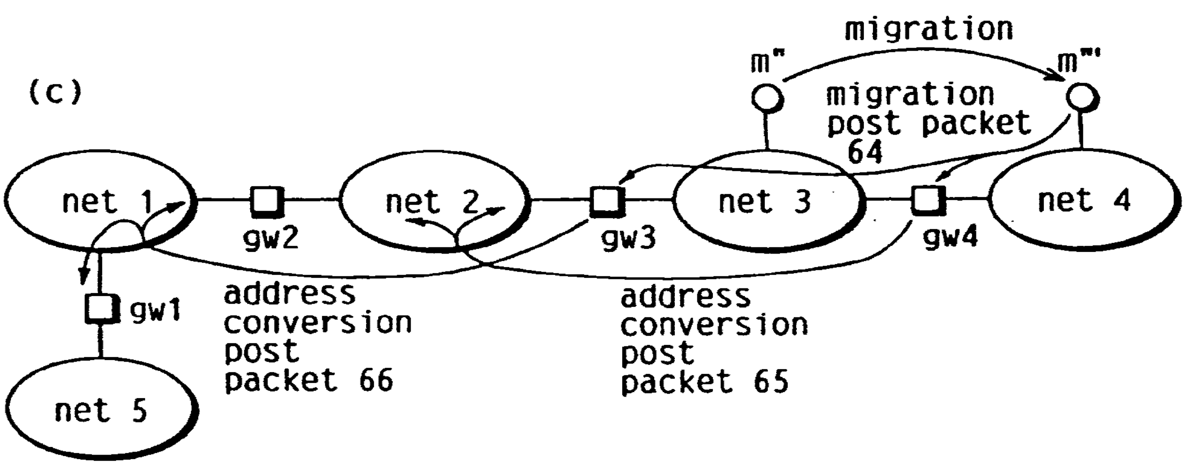
(a)


migration
m
m'
migration
post packet
61
net 1
gw2
net 2
gw3
net 3
gw4
net 4
gw1
net 5

(b)


migration
m'
m"
migration
post packet
62
net 1
gw2
net 2
gw3
net 3
gw4
net 4
address
conversion
post
packet 63
gw1
net 5

(c)


migration
m"
m"'
migration
post packet
64
net 1
gw2
net 2
gw3
net 3
gw4
net 4
gw1
address
conversion
post
packet 66
address
conversion
post
packet 65
net 5

EP 0 556 012 A2

42

FIG. 8

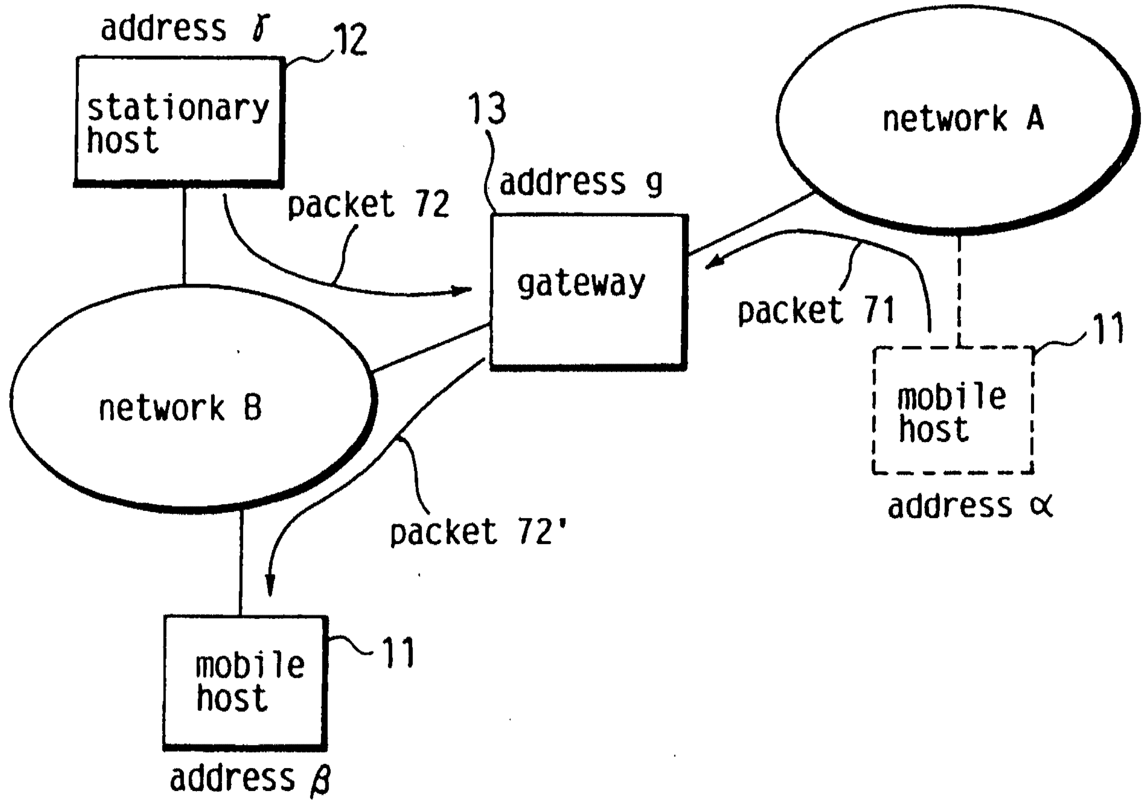


FIG. 9

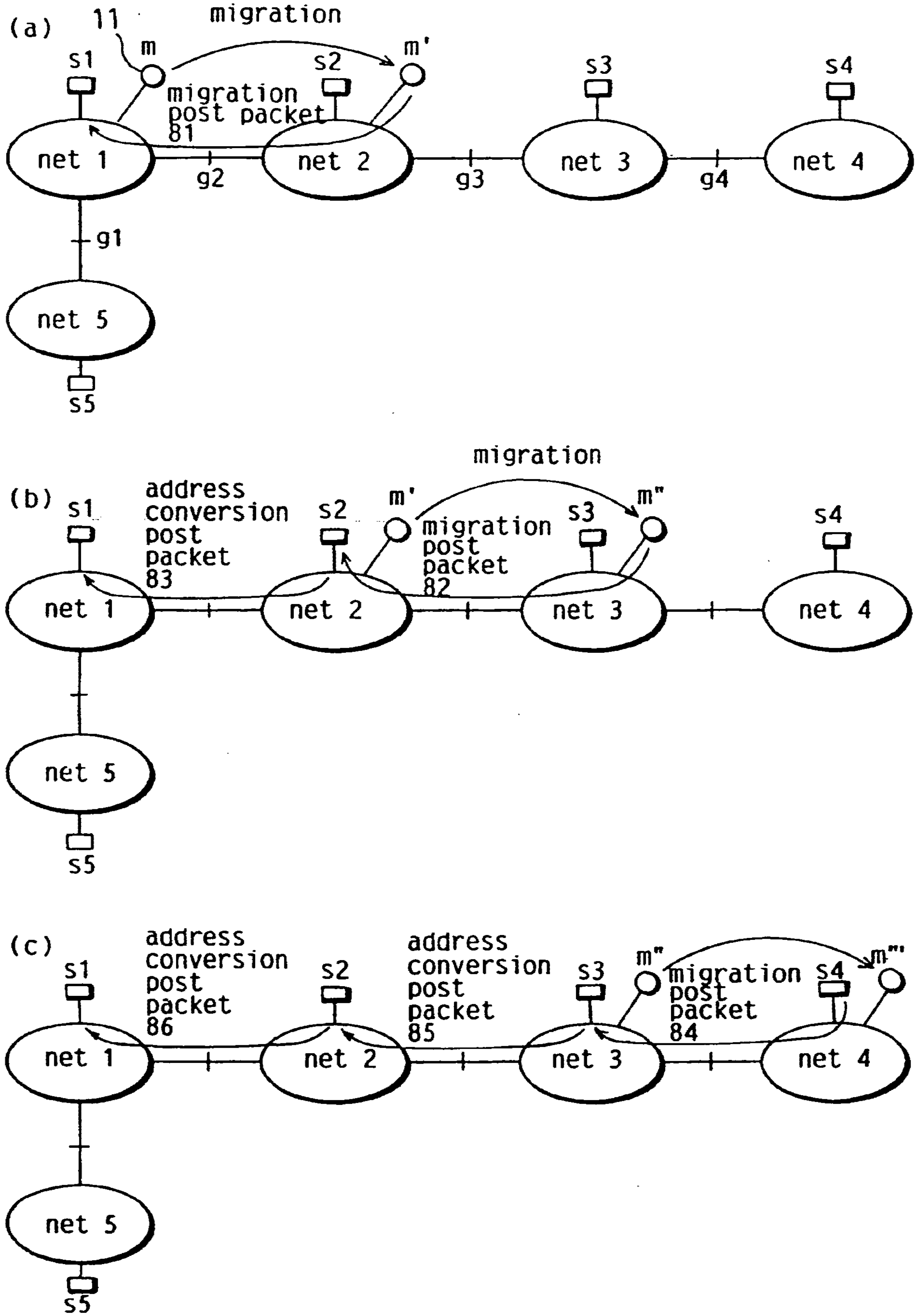

(a)
11
migration
m
m'
s1
s2
s3
s4
migration
post packet
81
net 1
net 2
net 3
net 4
g2
g3
g4
g1
net 5
s5
(b)
migration
address
conversion
post
packet
83
m'
m"
migration
post
packet
82
(c)
address
conversion
post
packet
86
address
conversion
post
packet
85
m"
m"'
migration
post
packet
84

FIG. 10

(a)

address before migration	address after migration
address α	address β

(b)

address before migration	address after migration
address α	address β
address X	address Y

FIG. 11

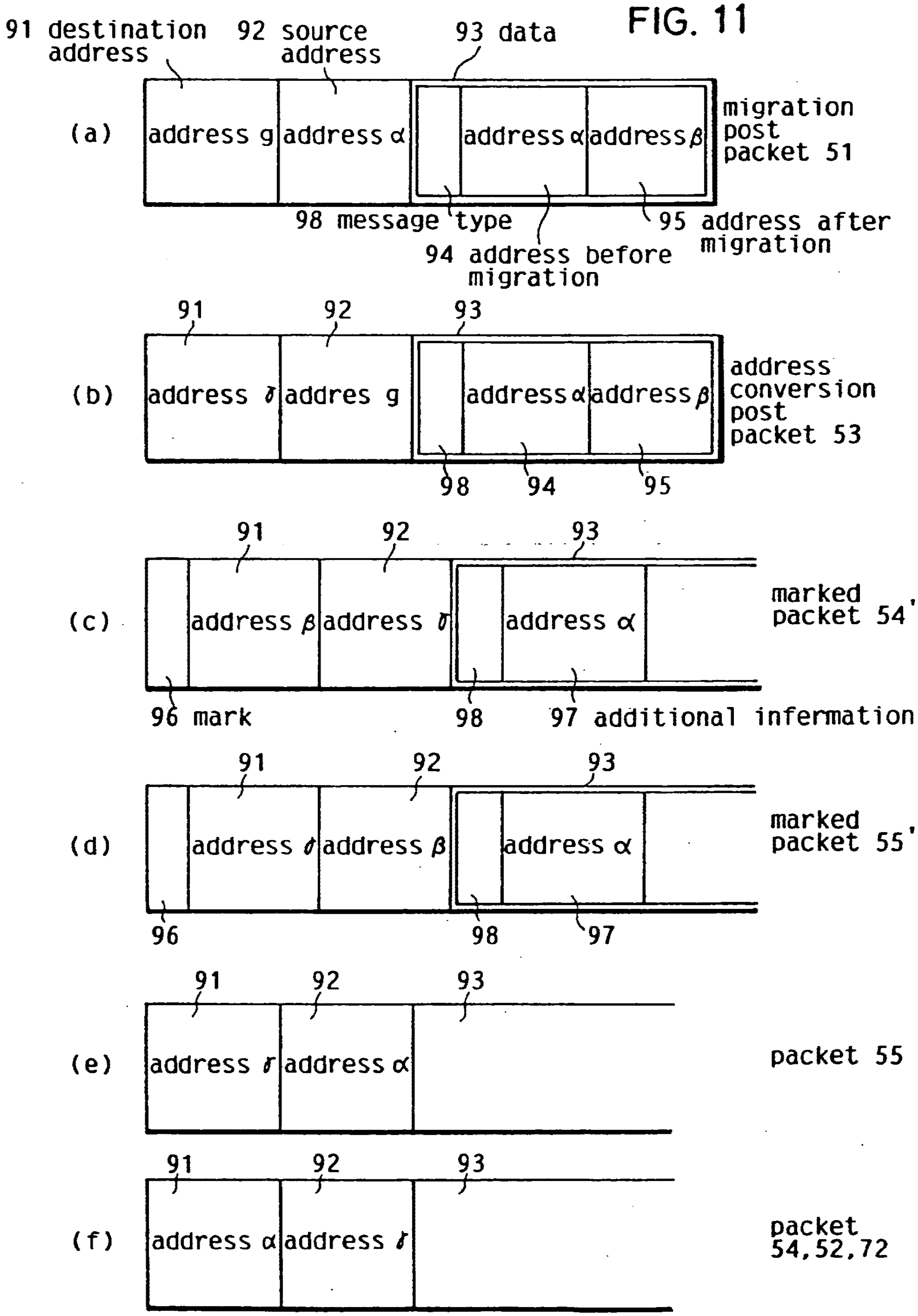

91 destination address
92 source address
93 data
(a)
address g
address α
address α
address β
migration post packet 51
98 message type
94 address before migration
95 address after migration
91
92
93
(b)
address γ
addres g
address α
address β
address conversion post packet 53
98
94
95
91
92
93
(c)
address β
address γ
address α
marked packet 54'
96 mark
98
97 additional infermation
91
92
93
(d)
address γ
address β
address α
marked packet 55'
96
98
97
91
92
93
(e)
address γ
address α
packet 55
91
92
93
(f)
address α
address γ
packet 54,52,72

FIG. 12

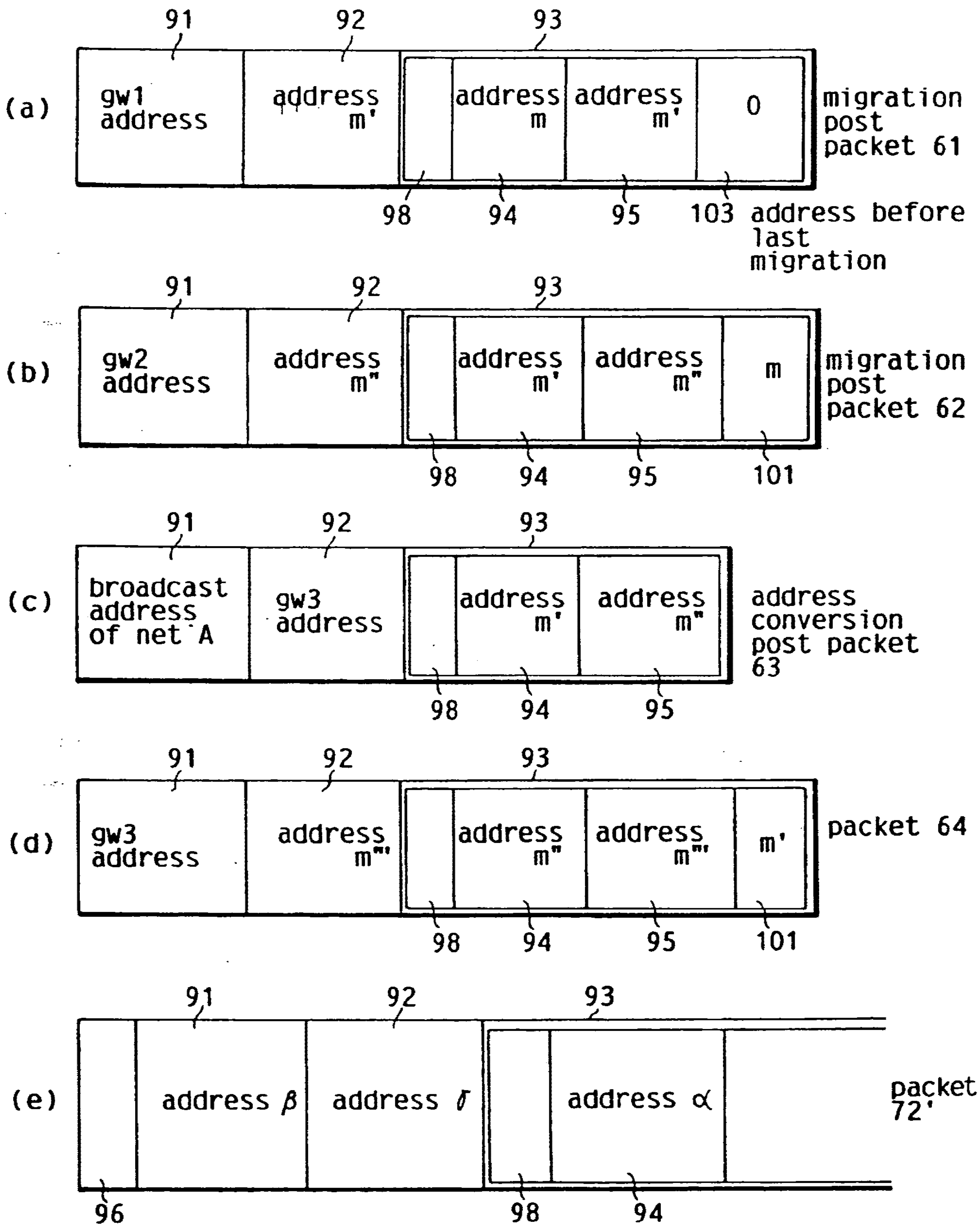

(a)
91
92
93
gw1 address
address m'
address m
address m'
0
migration post packet 61
98
94
95
103 address before last migration
(b)
91
92
93
gw2 address
address m"
address m'
address m"
m
migration post packet 62
98
94
95
101
(c)
91
92
93
broadcast address of net A
gw3 address
address m'
address m"
address conversion post packet 63
98
94
95
(d)
91
92
93
gw3 address
address m"'
address m"
address m"'
m'
packet 64
98
94
95
101
(e)
91
92
93
address β
address Γ
address α
packet 72'
96
98
94

FIG. 13

(a) migration from network A to network B

gateway	address correspon-dence	address before last migration
gw1	$m \rightarrow m'$	0
gw2	$m \rightarrow m'$	0
gw3	——	——
gw4	——	——

(b) migration from network B to network C

gateway	address correspon-dence	address before last migration
gw1	$m \rightarrow m''$	0
gw2	$m \rightarrow m''$ $m' \rightarrow m''$	0 m
gw3	$m' \rightarrow m''$	m
gw4	——	——

(c) migration from network C to network D

gateway	address correspon-dence	address before last migration
gw1	$m \rightarrow m'''$	0
gw2	$m \rightarrow m'''$ $m' \rightarrow m'''$	0 m
gw3	$m' \rightarrow m'''$ $m'' \rightarrow m'''$	m m'
gw4	$m'' \rightarrow m'''$	m'

FIG. 14

(a) migration from network A to network B

migration communication control device	content of hold unit	
	address correspondence	address before last migration
S1	m → m'	0
S2	——	——
S3	——	——
S4	——	——

(b) migration from network B to network C

migration communication control device	content of hold unit	
	address correspondence	address before last migration
S1	m → m"	0
S2	m' → m"	m
S3	——	——
S4	——	——

(c) migration from network C to network D

migration communication control device	content of hold unit	
	address correspondence	address before last migration
S1	m → m"'	0
S2	m' → m"'	m
S3	m" → m"'	m'
S4	——	——

FIG. 15

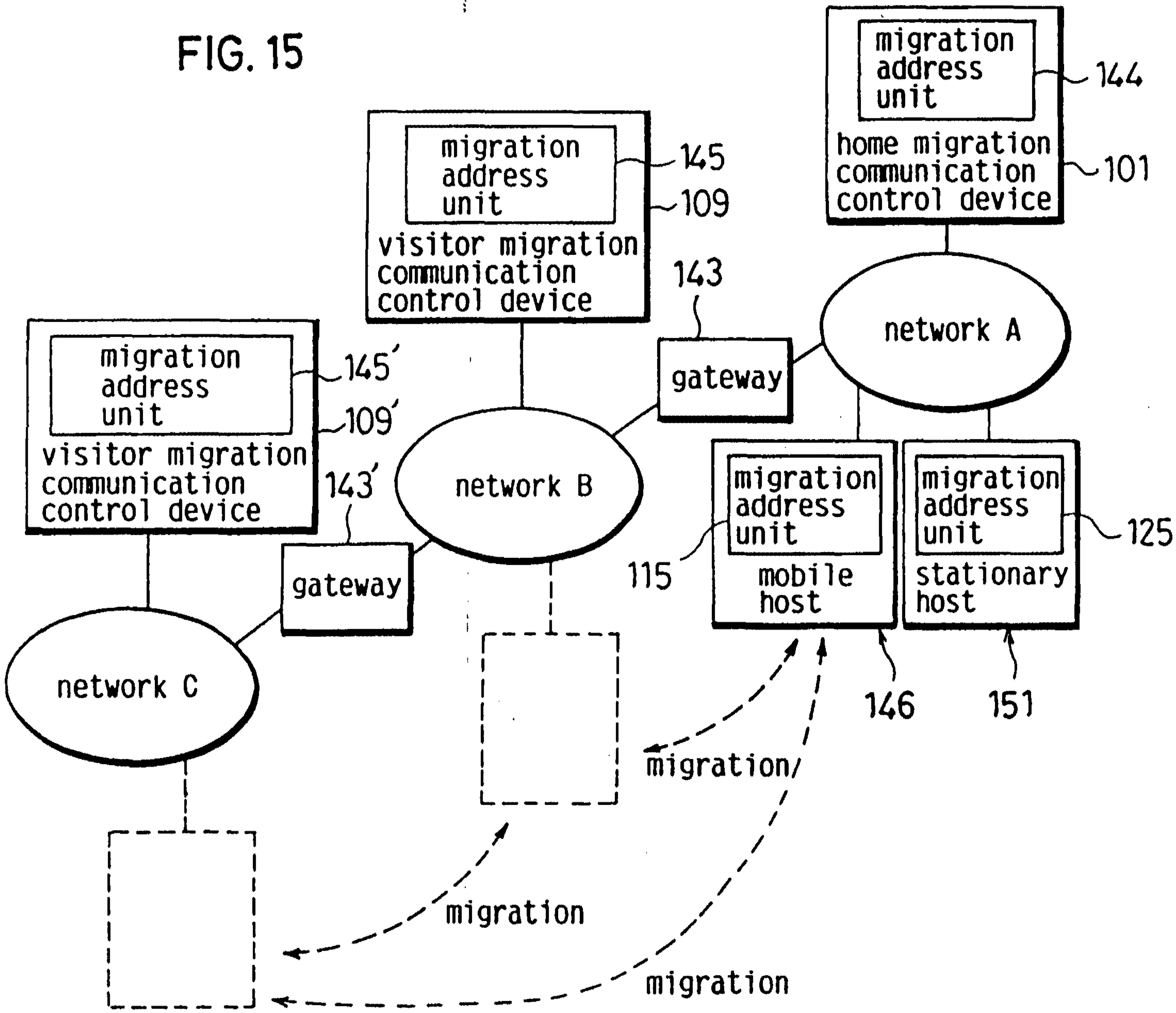

migration address unit
144
home migration communication control device
101
migration address unit
145
109
visitor migration communication control device
143
gateway
network A
migration address unit
145'
109'
visitor migration communication control device
143'
network B
gateway
network C
migration address unit
mobile host
115
migration address unit
stationary host
125
146
151
migration
migration
migration

FIG. 16

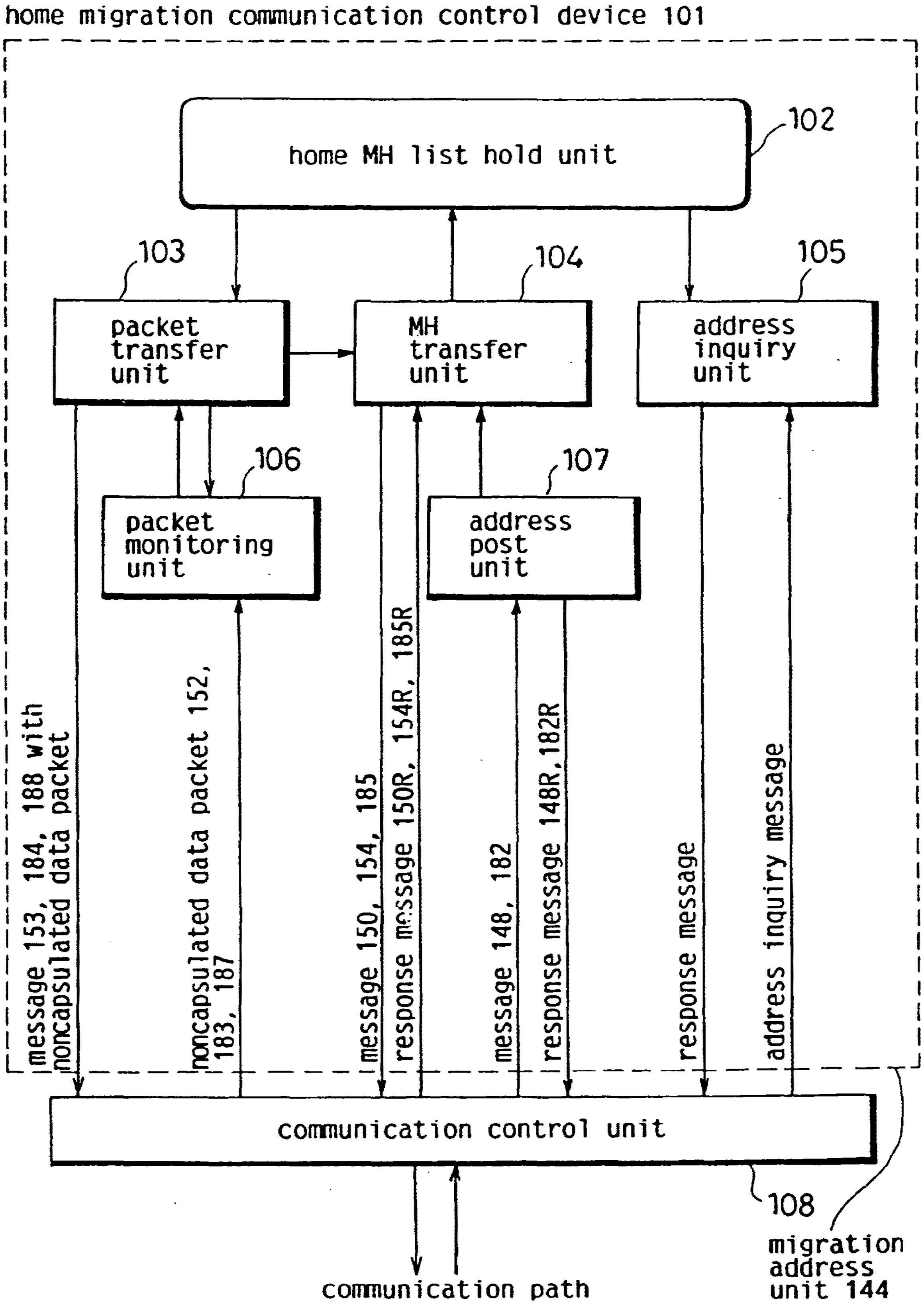
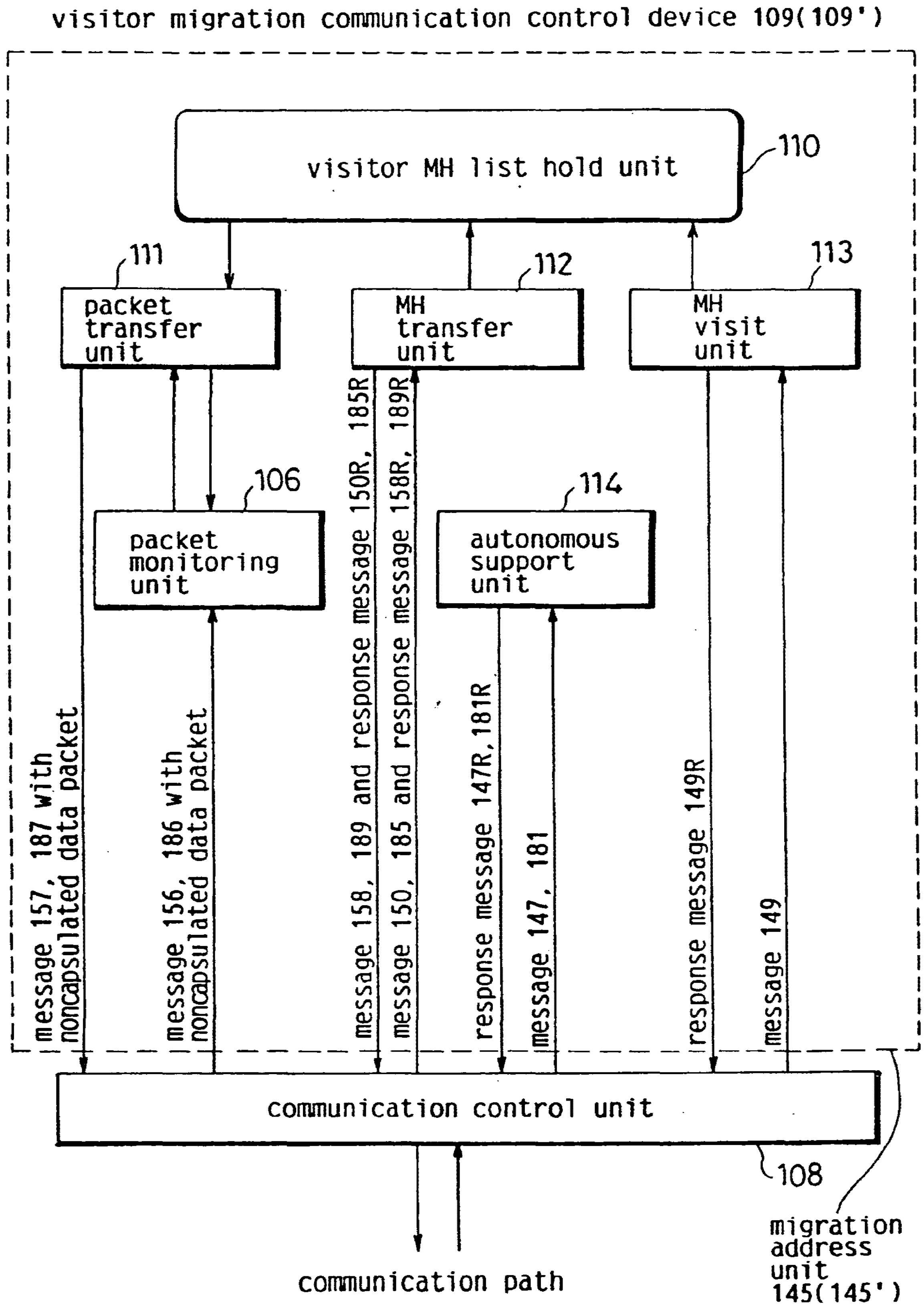

home migration communication control device 101
home MH list hold unit
102
103
packet transfer unit
104
MH transfer unit
105
address inquiry unit
106
packet monitoring unit
107
address post unit
message 153, 184, 188 with noncapsulated data packet
noncapsulated data packet 152, 183, 187
message 150, 154, 185
response message 150R, 154R, 185R
message 148, 182
response message 148R, 182R
response message
address inquiry message
communication control unit
108
migration address unit 144
communication path

FIG. 17

MH's home address	MH's current temporary address	autonomous flag F	current broadcast address
α	β or γ	1	Bba or Cba

FIG. 18



visitor migration communication control device 109(109')
visitor MH list hold unit
110
111
packet transfer unit
112
MH transfer unit
113
MH visit unit
106
packet monitoring unit
114
autonomous support unit
message 157, 187 with noncapsulated data packet
message 156, 186 with noncapsulated data packet
message 158, 189 and response message 150R, 185R
message 150, 185 and response message 158R, 189R
response message 147R, 181R
message 147, 181
response message 149R
message 149
communication control unit
108
communication path
migration address unit 145(145')

FIG. 19

MH's home address	temporary address	temporary address after migration	autonomous flag F
α	β	γ	1

FIG. 20

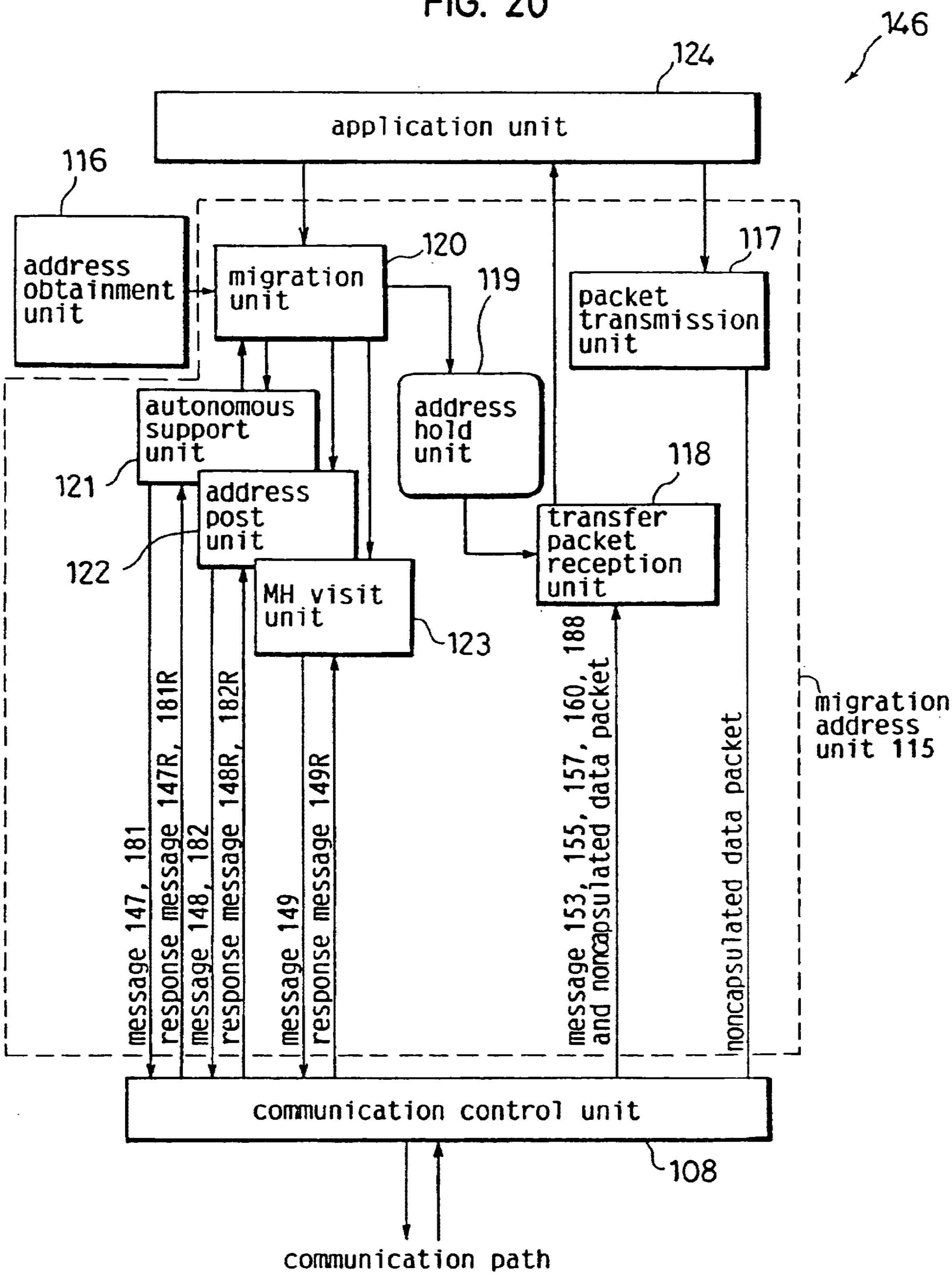

146
124
application unit
116
address obtainment unit
migration unit
120
119
117
packet transmission unit
autonomous support unit
address hold unit
121
address post unit
118
transfer packet reception unit
122
MH visit unit
123
message 147, 181
response message 147R, 181R
message 148, 182
response message 148R, 182R
message 149
response message 149R
message 153, 155, 157, 160, 188
and noncapsulated data packet
noncapsulated data packet
migration address unit 115
communication control unit
108
communication path

FIG. 21

home addres	broadcast address of home network	current temporary address	broadcast address
α	Aba	β or γ	Bba or Cba

FIG. 22

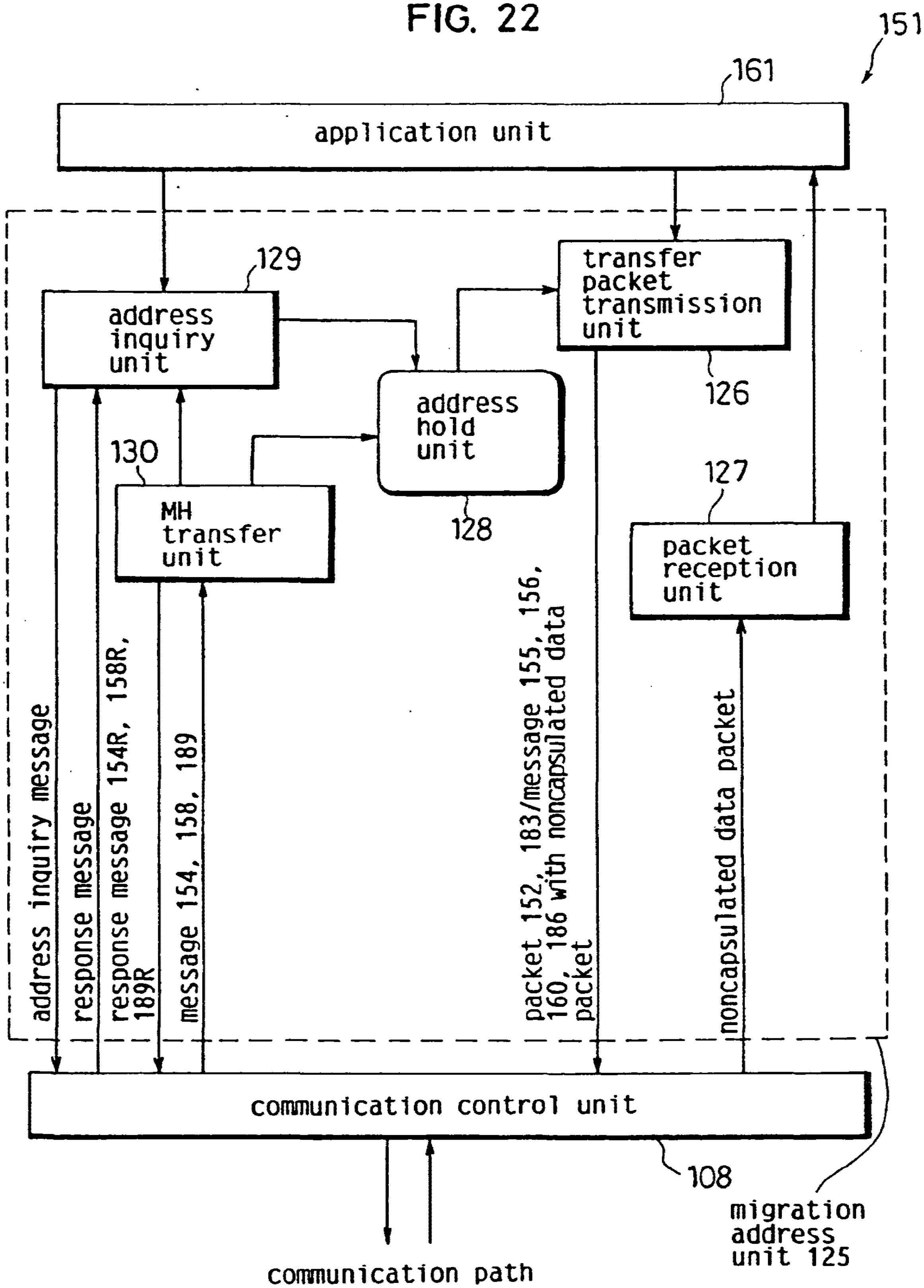

151
161
application unit
129
address inquiry unit
transfer packet transmission unit
address hold unit
126
130
127
MH transfer unit
128
packet reception unit
address inquiry message
response message
response message 154R, 158R, 189R
message 154, 158, 189
packet 152, 183/message 155, 156, 160, 186 with noncapsulated data packet
noncapsulated data packet
communication control unit
108
migration address unit 125
communication path

FIG. 23

MH's home address	MH's temporary address
α	β or γ

FIG. 24

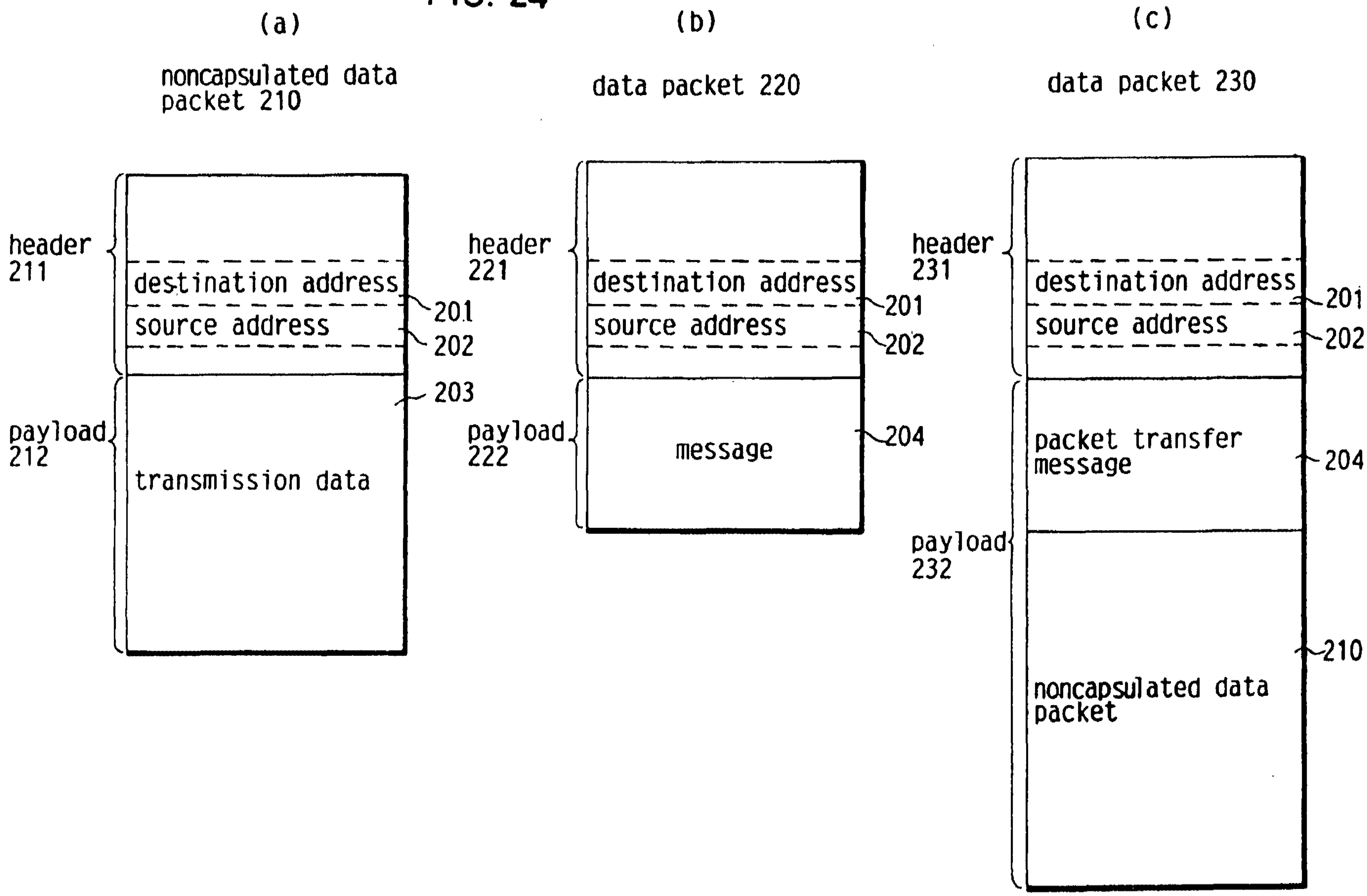

(a)
noncapsulated data packet 210
header 211
destination address
201
source address
202
203
payload 212
transmission data
(b)
data packet 220
header 221
destination address
201
source address
202
payload 222
message
204
(c)
data packet 230
header 231
destination address
201
source address
202
packet transfer message
204
payload 232
210
noncapsulated data packet

FIG. 25

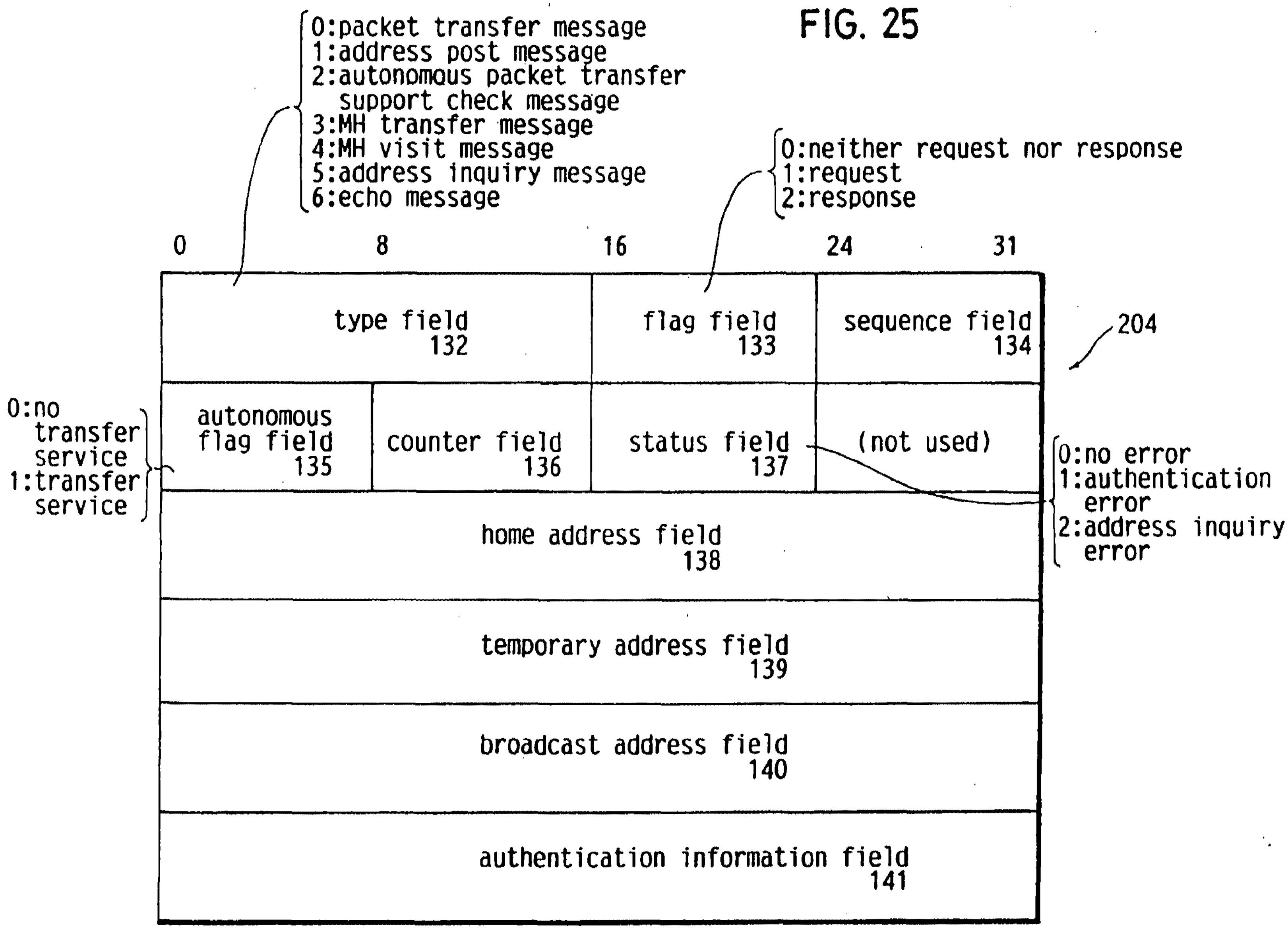

0:packet transfer message
1:address post message
2:autonomous packet transfer support check message
3:MH transfer message
4:MH visit message
5:address inquiry message
6:echo message
0:neither request nor response
1:request
2:response
0
8
16
24
31
type field 132
flag field 133
sequence field 134
204
0:no transfer service
1:transfer service
autonomous flag field 135
counter field 136
status field 137
(not used)
0:no error
1:authentication error
2:address inquiry error
home address field 138
temporary address field 139
broadcast address field 140
authentication information field 141

FIG. 26

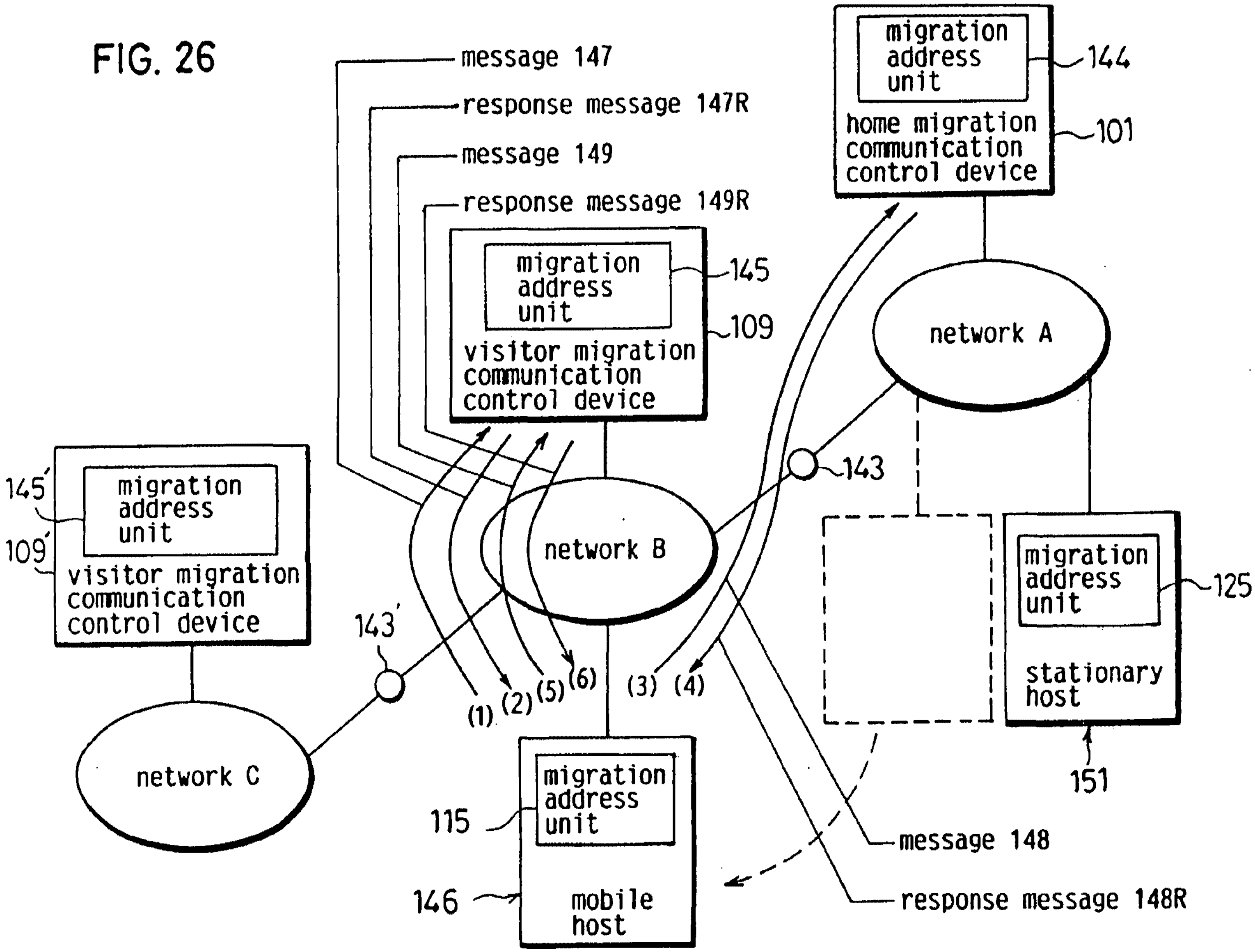

message 147
response message 147R
message 149
response message 149R
migration address unit
home migration communication control device
144
101
migration address unit
145
109
visitor migration communication control device
network A
network B
network C
143
143'
145'
109'
migration address unit
visitor migration communication control device
migration address unit
125
stationary host
151
(1) (2) (5) (6) (3) (4)
migration address unit
115
146
mobile host
message 148
response message 148R

FIG. 27 migration from network A to network B

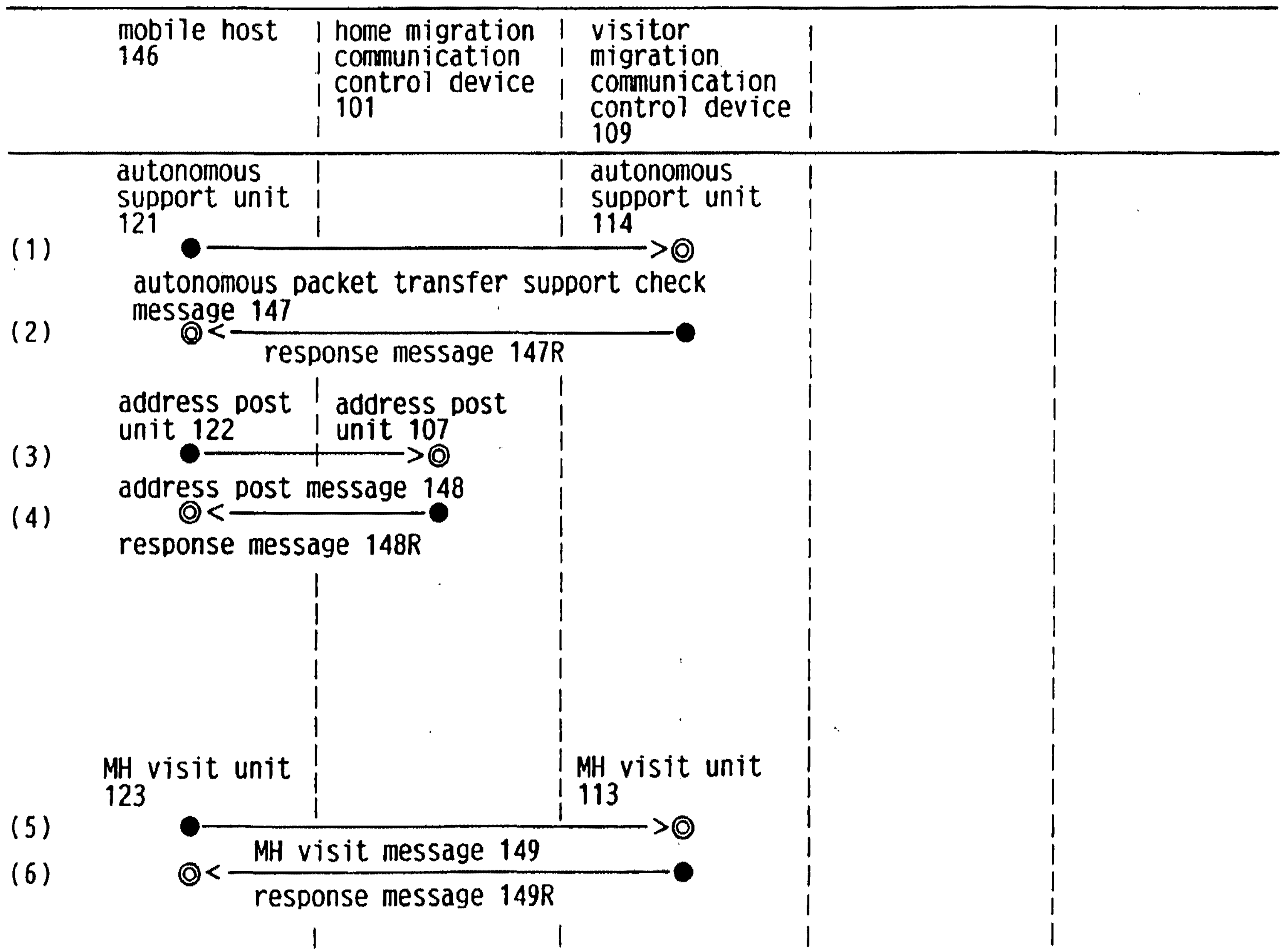
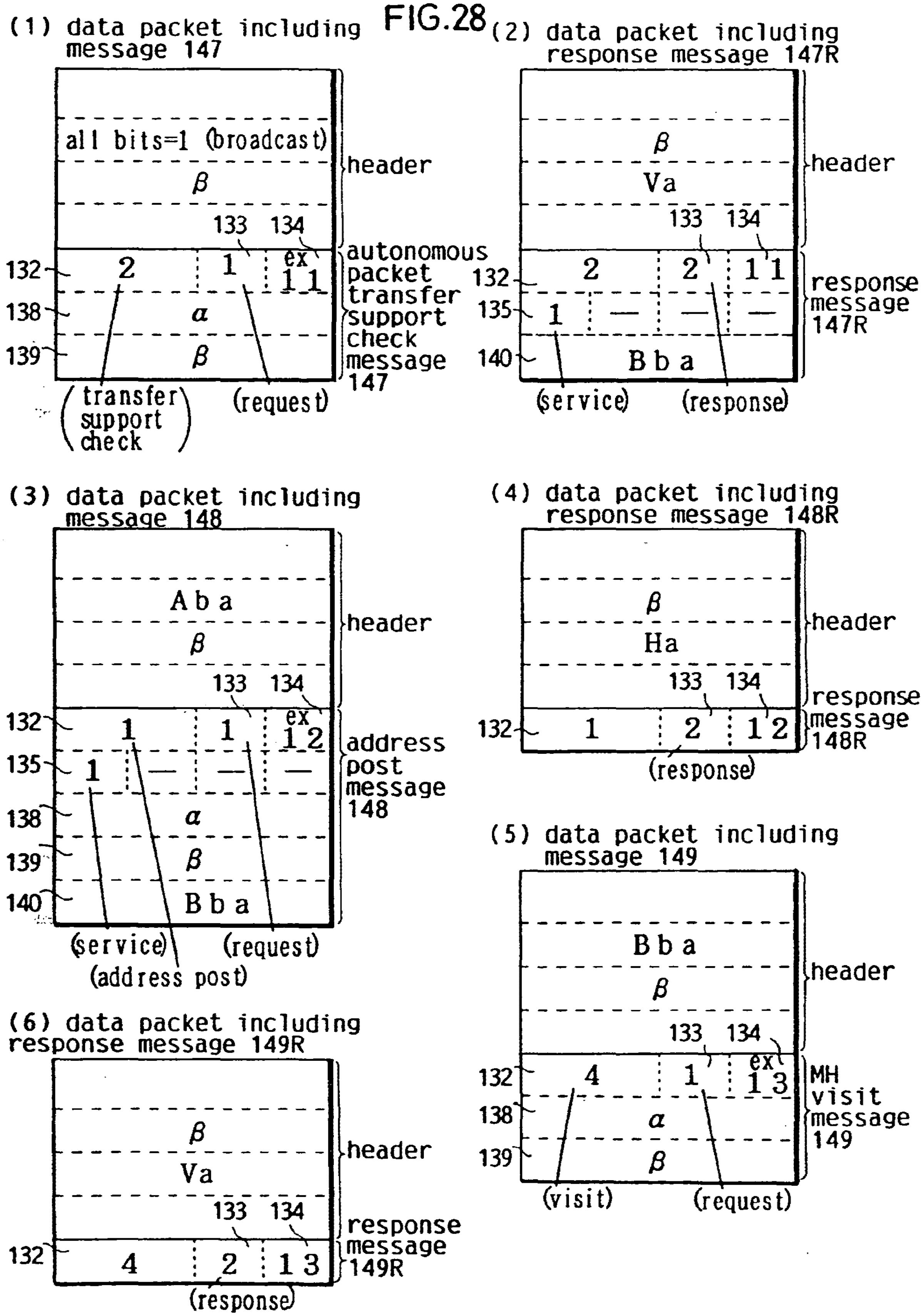


FIG.28


(1) data packet including message 147
all bits=1 (broadcast)
β
133 134
header
132
2
1
ex 1 1
138
α
139
β
autonomous packet transfer support check message 147
(transfer support check)
(request)
(2) data packet including response message 147R
β
Va
header
133 134
132
2
2
1 1
135
1
—
—
—
140
Bba
response message 147R
(service)
(response)
(3) data packet including message 148
Aba
β
header
133 134
132
1
1
ex 1 2
135
1
—
—
—
138
α
139
β
140
Bba
address post message 148
(service)
(request)
(address post)
(4) data packet including response message 148R
β
Ha
header
133 134
132
1
2
1 2
response message 148R
(response)
(5) data packet including message 149
Bba
β
header
133 134
132
4
1
ex 1 3
138
α
139
β
MH visit message 149
(visit)
(request)
(6) data packet including response message 149R
β
Va
header
133 134
132
4
2
1 3
response message 149R
(response)

		address after obtainment of β	(1)	(2)	(3)	(4)	(5)	(6)
address hold unit 119(146)	home address	α		α				
	broadcast address of home network	Aba		Aba				
	current temporary address	β		β				
	current broadcast address	–		Bba				
home MH host list hold unit 102(101)	MH's home address	α			α			
	MH's current temporary address	α			β			
	autonomous flag F	–			1			
	current broadcast address	–			Bba			
visitor MH list hold unit 110(109)	MH's home address	–					α	
	temporary address	–					β	
	temporary address after migration	–					β	
	autonomous flag F	–					–	
visitor MH list hold unit 110'(109')	MH's home address	–						
	temporary address	–						
	temporary address after migration	–						
	autonomous flag F	–						
address hold unit 128(151)	MH's home address	–						
	MH's temporary address	–						

FIG. 29

FIG. 30

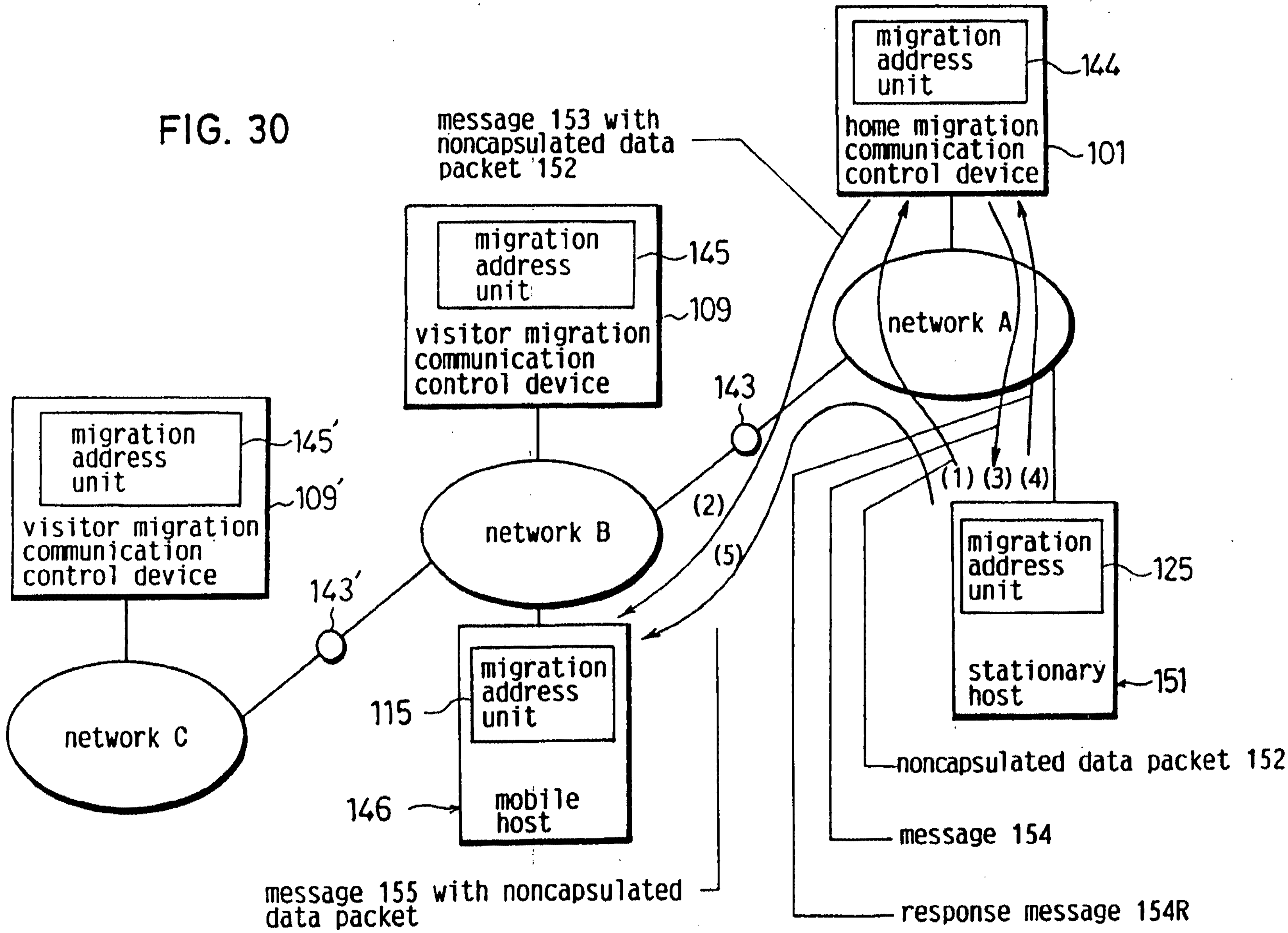

message 153 with noncapsulated data packet 152
migration address unit
144
home migration communication control device
101
migration address unit
145
109
visitor migration communication control device
network A
143
migration address unit
145'
109'
visitor migration communication control device
network B
(2)
(5)
(1) (3) (4)
migration address unit
125
stationary host
151
143'
network C
migration address unit
115
146
mobile host
noncapsulated data packet 152
message 154
response message 154R
message 155 with noncapsulated data packet

FIG. 31

data packet from SH 151 to MH 146 on network B

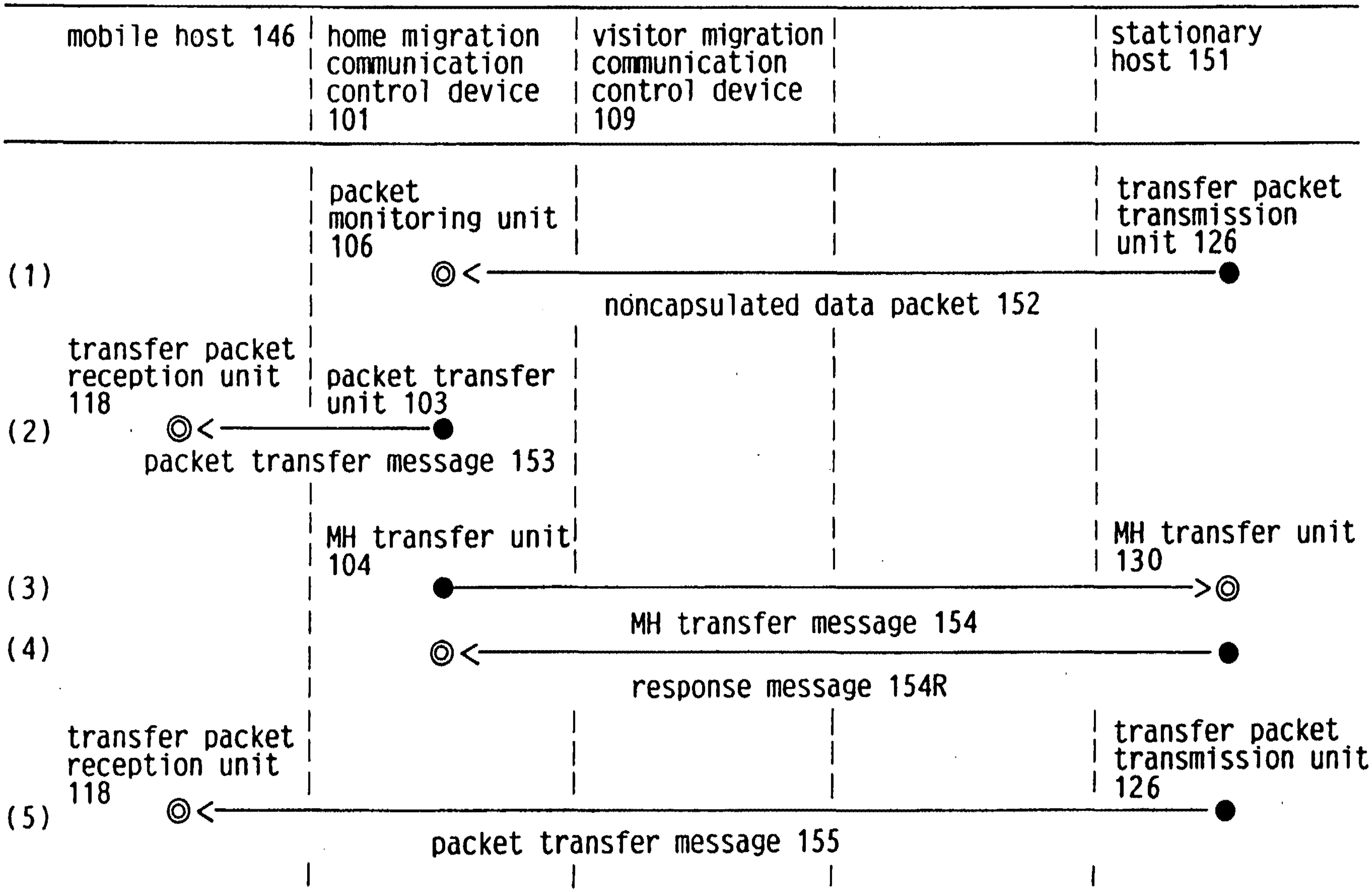


FIG. 32

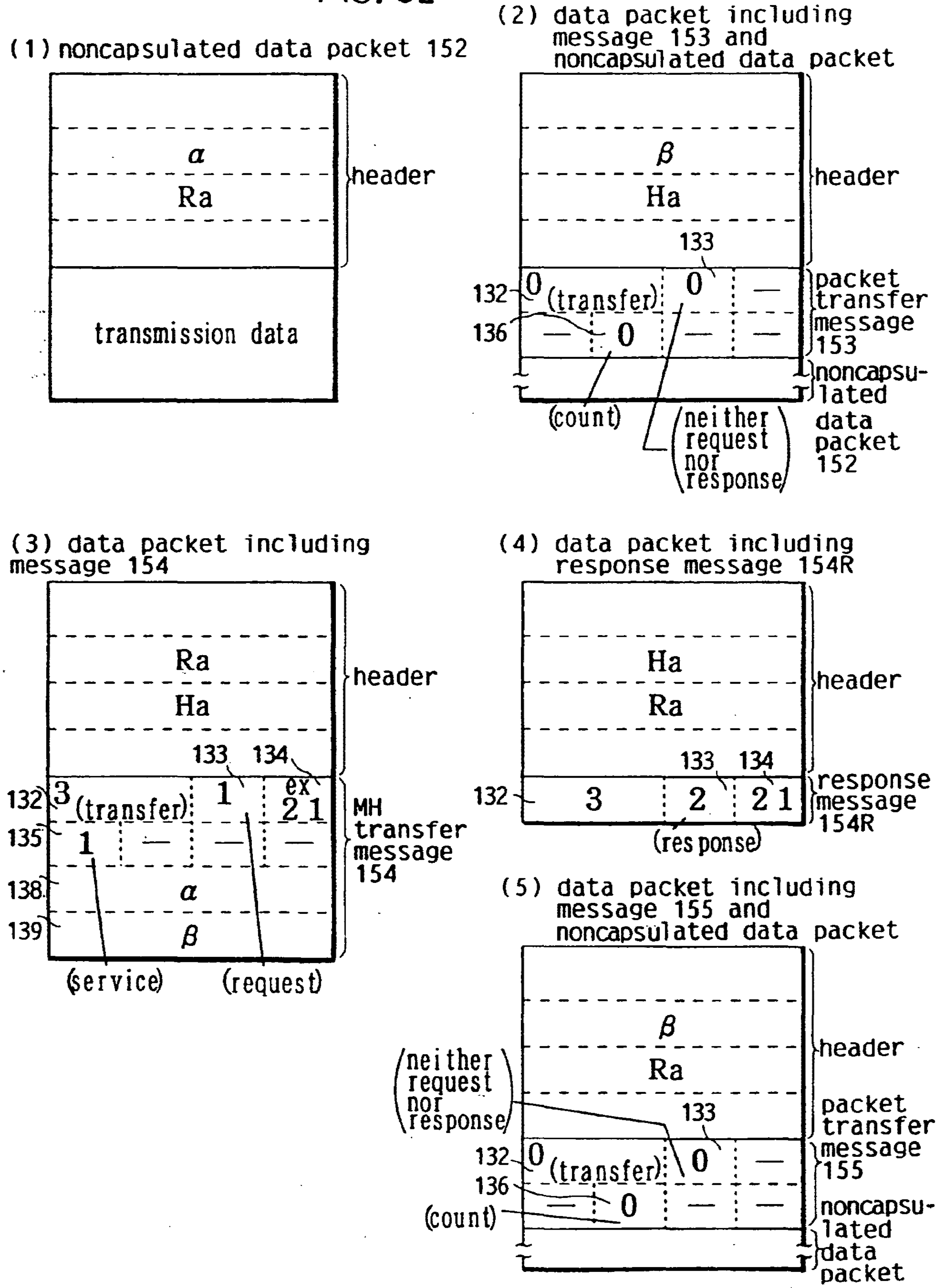

(1) noncapsulated data packet 152
α
Ra
header
transmission data
(2) data packet including message 153 and noncapsulated data packet
β
Ha
header
133
132
0
(transfer)
0
136
0
packet transfer message 153
noncapsulated data packet 152
(count)
(neither request nor response)
(3) data packet including message 154
Ra
Ha
header
133
134
132
3
(transfer)
1
ex
2 1
135
1
138
α
139
β
MH transfer message 154
(service)
(request)
(4) data packet including response message 154R
Ha
Ra
header
133
134
132
3
2
2 1
response message 154R
(response)
(5) data packet including message 155 and noncapsulated data packet
β
Ra
header
133
(neither request nor response)
132
0
(transfer)
0
136
0
(count)
packet transfer message 155
noncapsulated data packet

FIG. 33

	address hold unit 119(146)				home MH list hold unit 102(101)				visitor MH list hold unit 110(109)				visitor MH list hold unit 110'(109')				address hold unit 128(151)	
	home address	broadcast address of home network	current temporary address	current broadcast address	MH's home address	current temporary address	autonomous flag F	broadcast address	MH's home address	temporary address	temporary address after migration	autonomous flag F	MH's home address	temporary address	temporary address after migration	autonomous flag F	MH's home address	MH's temporary address
address before communica-tion	α	Aba	β	Bba	α	β	1	Bba	α	β	β	—	—	—	—	—	—	—
(1)																		
(2)																		
(3)																	α	β
(4)																		
(5)																		

FIG. 34

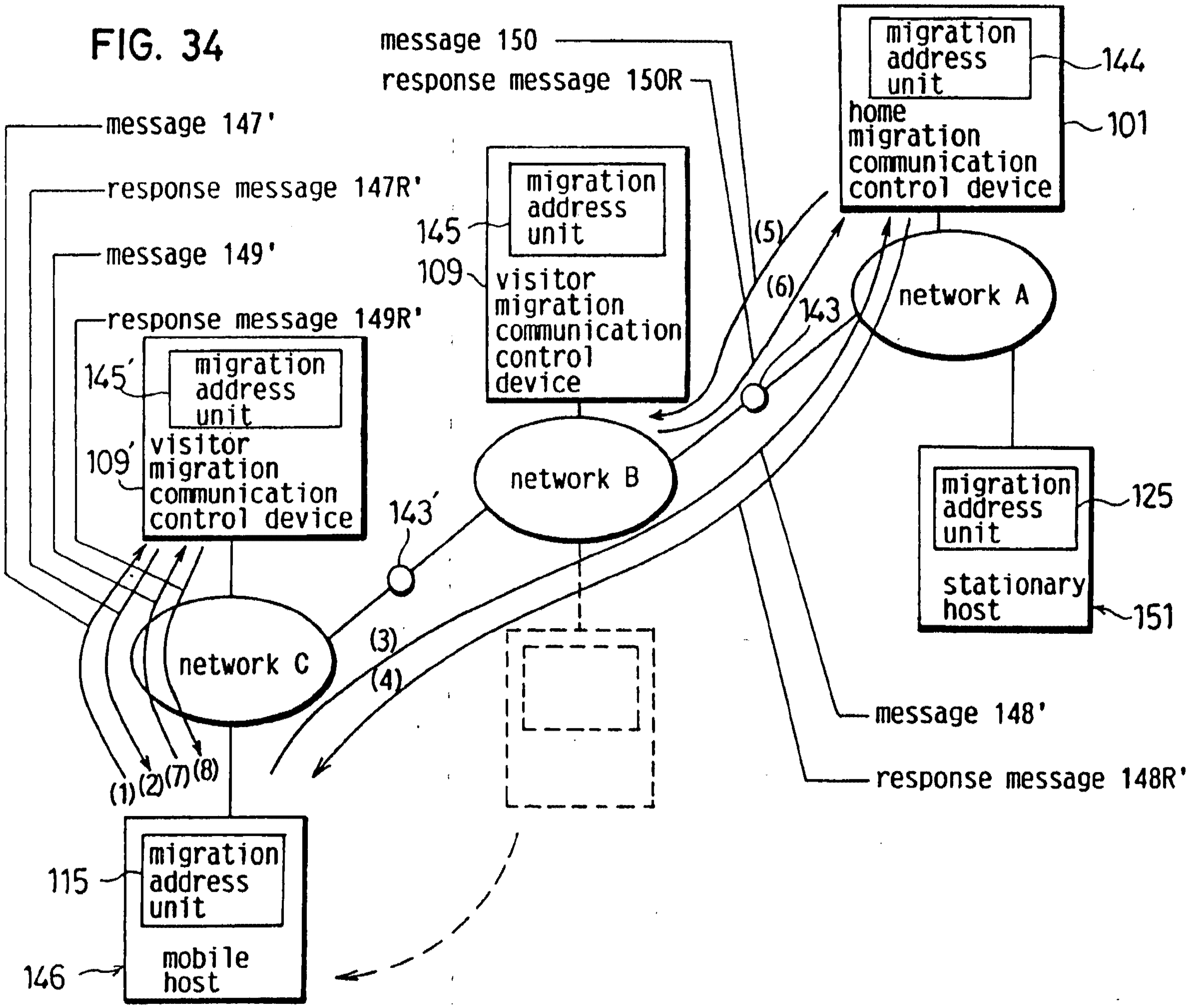

message 150
response message 150R
message 147'
response message 147R'
message 149'
response message 149R'
migration address unit
144
home migration communication control device
101
145
109
visitor migration communication control device
145'
109'
143
143'
network A
network B
network C
migration address unit
125
stationary host
151
message 148'
response message 148R'
115
146
mobile host
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)

FIG. 35 migration from network B to network C

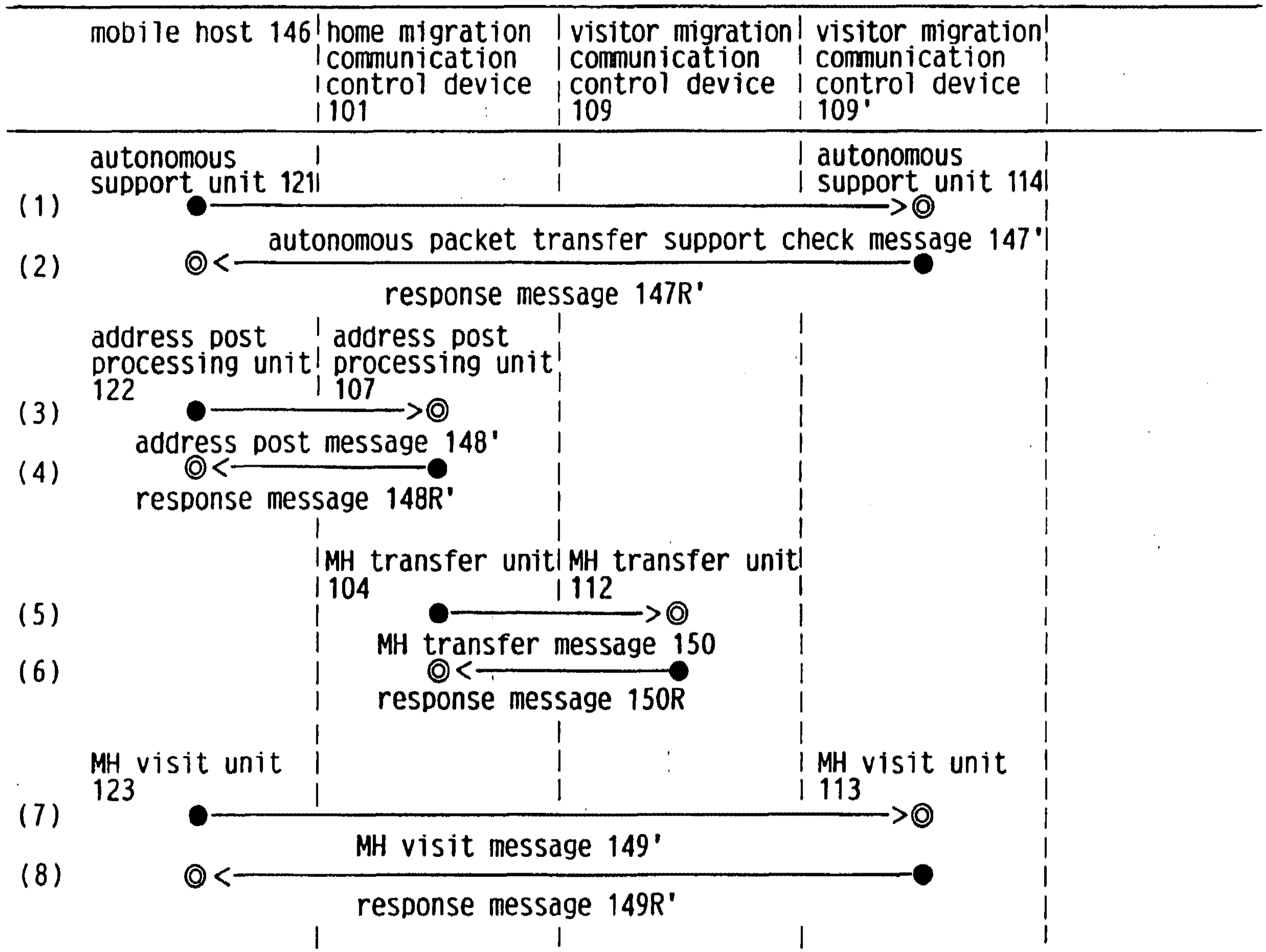


FIG.36

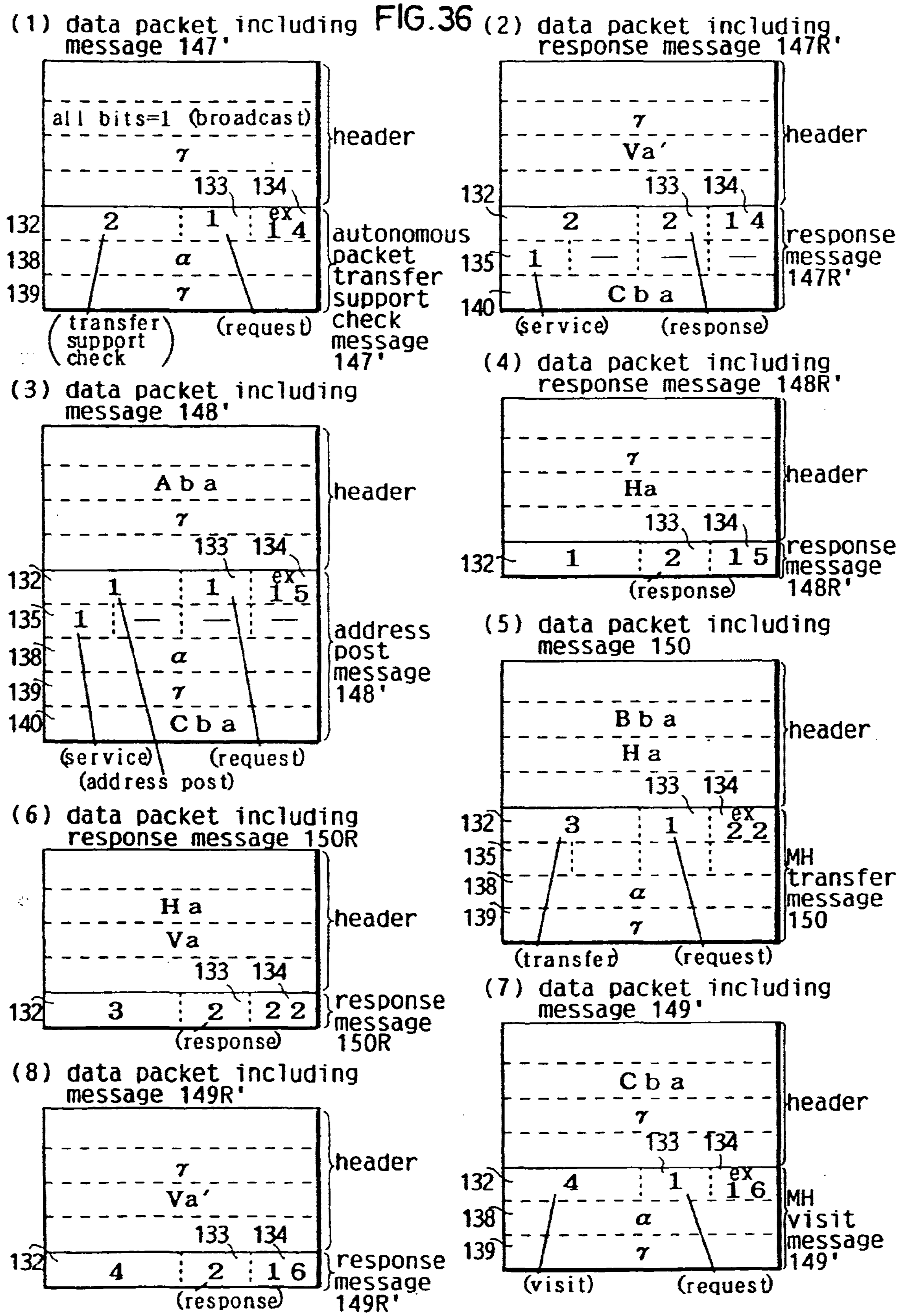

(1) data packet including message 147'
all bits=1 (broadcast)
γ
133
134
header
132
2
1
ex
1 4
138
α
139
γ
autonomous packet transfer support check message 147'
(transfer support check)
(request)
(2) data packet including response message 147R'
γ
Va'
133
134
header
132
2
2
1 4
135
1
140
C b a
response message 147R'
(service)
(response)
(3) data packet including message 148'
A b a
γ
133
134
header
132
1
1
ex
1 5
135
1
138
α
139
γ
140
C b a
address post message 148'
(service)
(request)
(address post)
(4) data packet including response message 148R'
γ
Ha
133
134
header
132
1
2
1 5
response message 148R'
(response)
(5) data packet including message 150
B b a
H a
133
134
header
132
3
1
ex
2 2
135
138
α
139
γ
MH transfer message 150
(transfer)
(request)
(6) data packet including response message 150R
H a
Va
133
134
header
132
3
2
2 2
response message 150R
(response)
(7) data packet including message 149'
C b a
γ
133
134
header
132
4
1
ex
1 6
138
α
139
γ
MH visit message 149'
(visit)
(request)
(8) data packet including message 149R'
γ
Va'
133
134
header
132
4
2
1 6
response message 149R'
(response)

FIG. 37

	address hold unit 119(146)				home MH list hold unit 102(101)				visitor MH list hold unit 110(109)				visitor MH list hold unit 110'(109')				address hold unit 128(151)	
	home address	broadcast address of home network	current temporary address	current broadcast address	MH's home address	MH's current temporary address	autonomous flag F	current broadcast address	MH's home address	temporary address	temporary address after migration	autonomous flag F	MH's home address	temporary address	temporary address after migration	autonomous flag F	MH's home address	MH's temporary address
address after obtainment of γ	α	Aba	γ	Bba	α	β	1	Bba	α	β	β	—	—	—	—	—	α	β
(1)																		
(2)	α	Aba	γ	Cba														
(3)					α	γ	1	Cba										
(4)																		
(5)									α	β	γ	1						
(6)																		
(7)													α	γ	γ	—		
(8)																		

FIG. 38

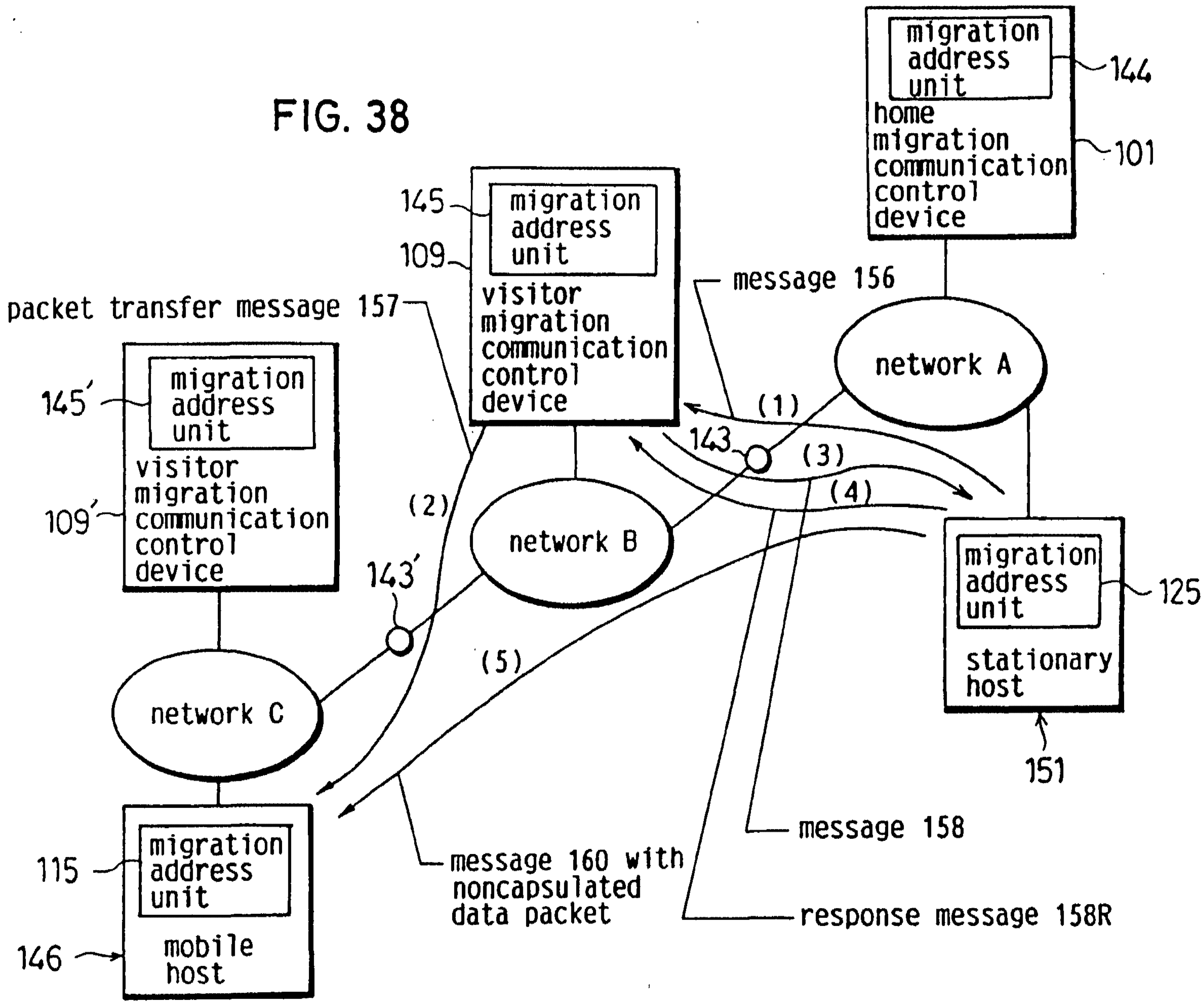

migration
address
unit
home
migration
communication
control
device
144
101
145
109
migration
address
unit
visitor
migration
communication
control
device
message 156
network A
packet transfer message 157
145′
migration
address
unit
visitor
migration
communication
control
device
109′
(1)
143
(3)
(4)
(2)
network B
migration
address
unit
stationary
host
125
143′
(5)
network C
151
migration
address
unit
mobile
host
115
146
message 158
message 160 with
noncapsulated
data packet
response message 158R

FIG. 39

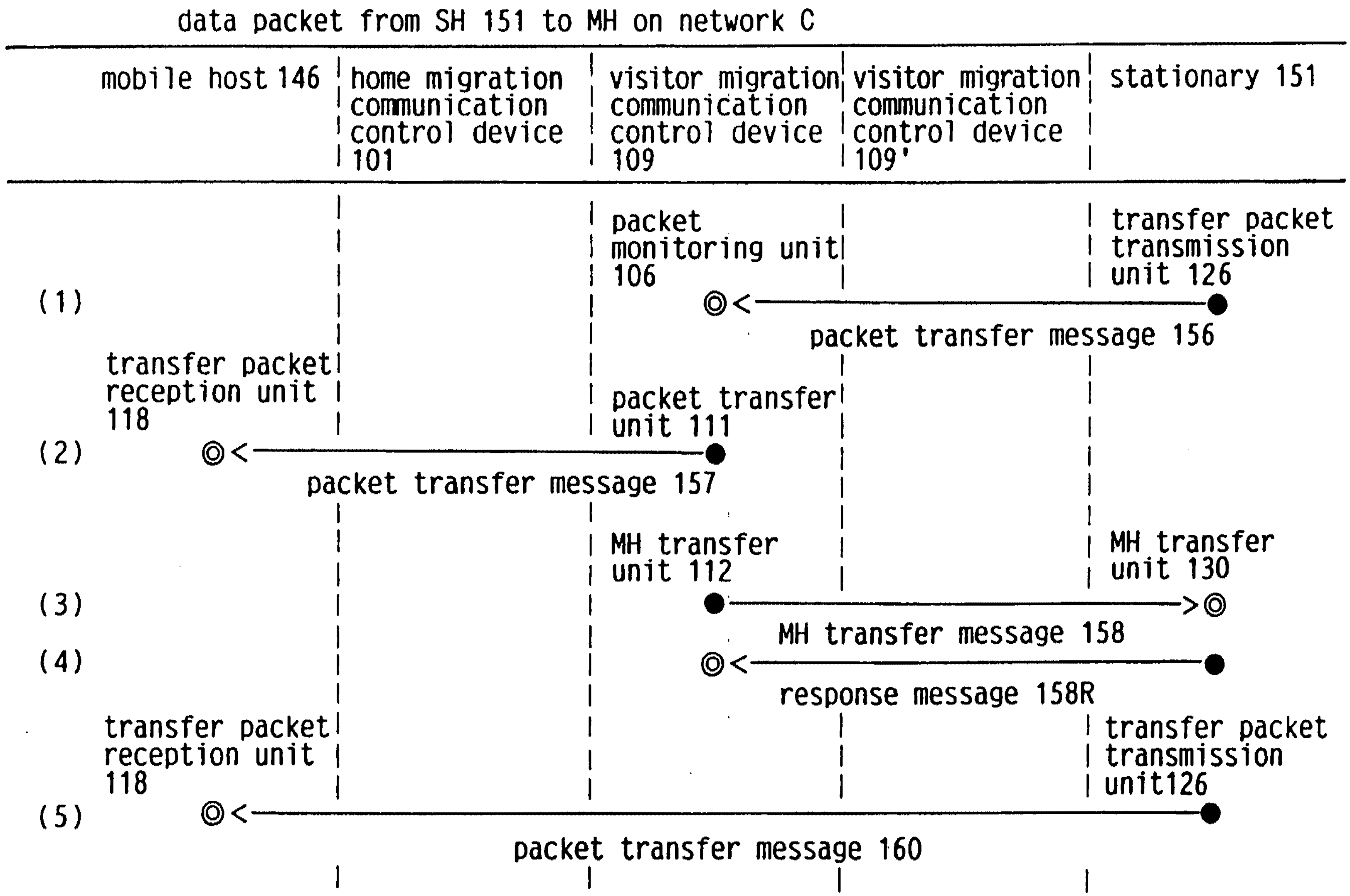

data packet from SH 151 to MH on network C
mobile host 146
home migration communication control device 101
visitor migration communication control device 109
visitor migration communication control device 109'
stationary 151
packet monitoring unit 106
transfer packet transmission unit 126
(1)
packet transfer message 156
transfer packet reception unit 118
packet transfer unit 111
(2)
packet transfer message 157
MH transfer unit 112
MH transfer unit 130
(3)
MH transfer message 158
(4)
response message 158R
transfer packet reception unit 118
transfer packet transmission unit126
(5)
packet transfer message 160

FIG. 40

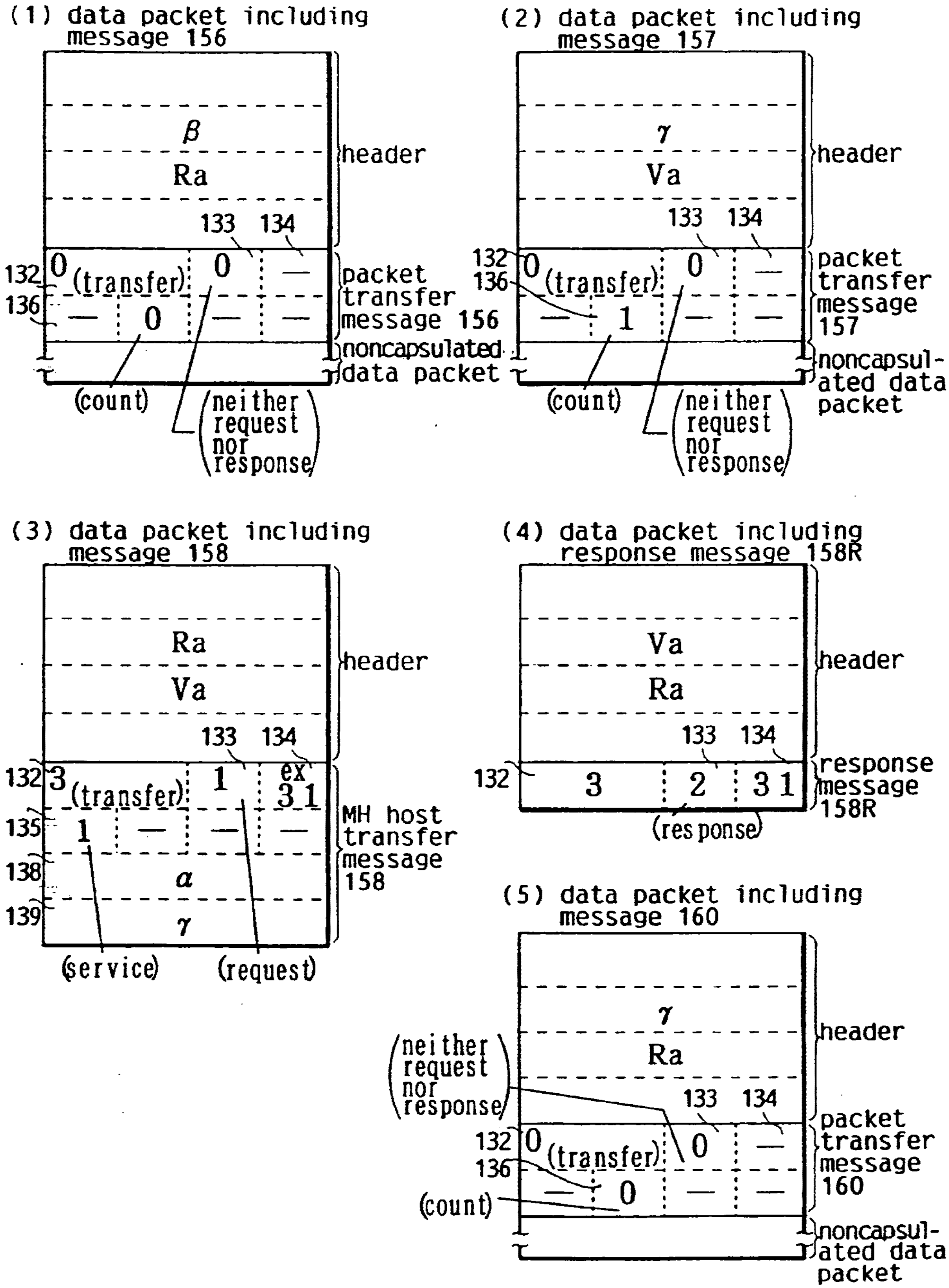

(1) data packet including message 156
β
Ra
133
134
132
136
0
(transfer)
0
header
packet transfer message 156
noncapsulated data packet
(count)
(neither request nor response)
(2) data packet including message 157
γ
Va
133
134
132
136
0
(transfer)
0
1
header
packet transfer message 157
noncapsul-ated data packet
(count)
(neither request nor response)
(3) data packet including message 158
Ra
Va
133
134
132
135
138
139
3
(transfer)
1
ex
3 1
1
α
γ
header
MH host transfer message 158
(service)
(request)
(4) data packet including response message 158R
Va
Ra
133
134
132
3
2
3 1
header
response message 158R
(response)
(5) data packet including message 160
γ
Ra
133
134
132
136
0
(transfer)
0
0
header
packet transfer message 160
noncapsul-ated data packet
(neither request nor response)
(count)

FIG. 41

	address hold unit 119				home MH list hold unit 102				visitor MH list hold unit 110				visitor MH list hold unit 109'				address hold unit 128	
	home address	broadcast address of home network	current temporary address	current broadcast address	MH's home address	MH's current temporary address	autonomous flag F	broadcast address	MH's home address	temporary address	temporary address after migration	autonomous flag F	MH's home address	temporary address	temporary address after migration	autonomous flag F	MH's home address	MH's temporary address
address before communication	α	Aba	γ	Cba	α	γ	1	Cba	α	β	γ	1	α	γ	γ	-	α	β
(1)																		
(2)																		
(3)																	α	γ
(4)																		
(5)																		

FIG. 42

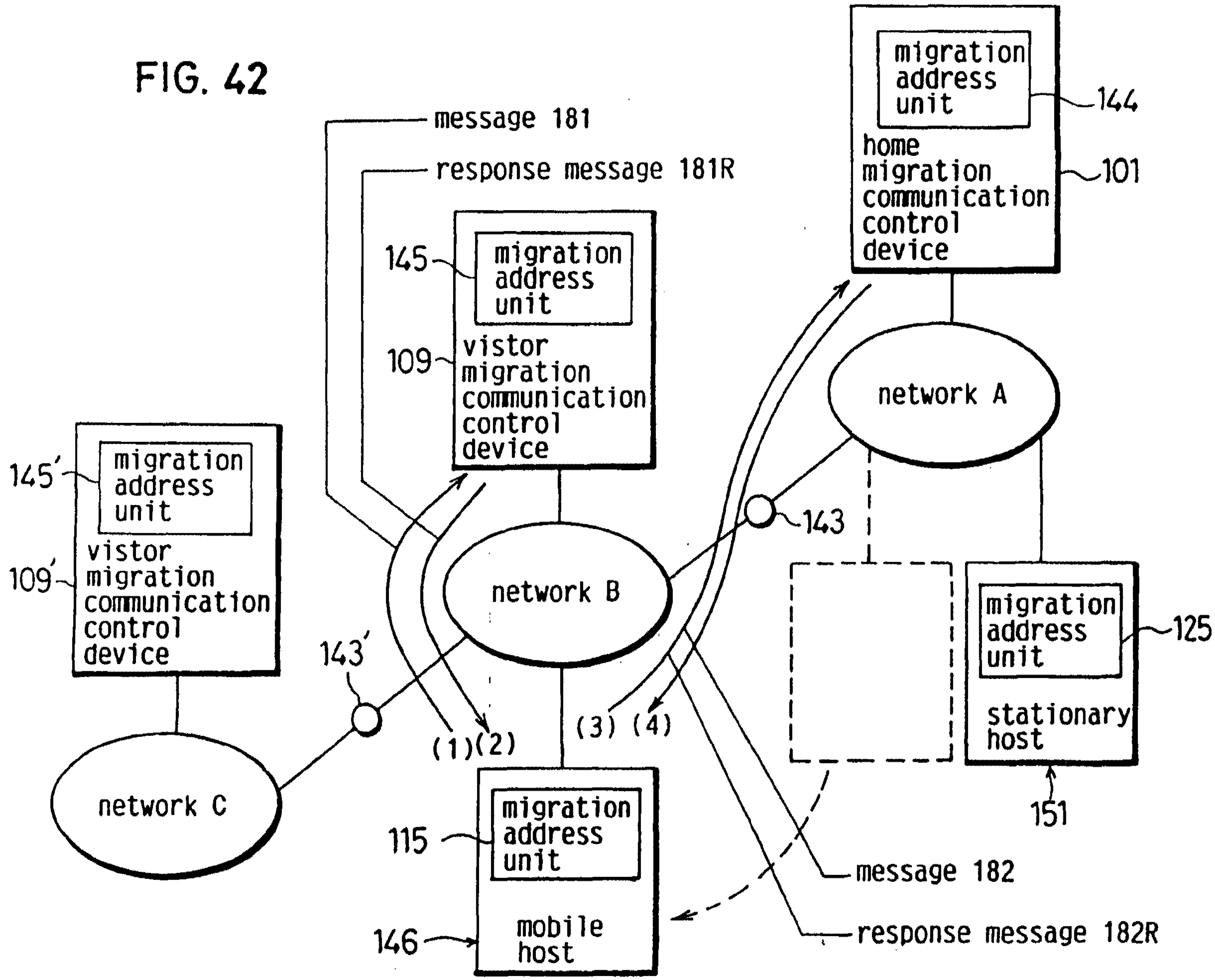

message 181
response message 181R
migration address unit
144
home migration communication control device
101
145
migration address unit
109
vistor migration communication control device
network A
143
145'
migration address unit
109'
vistor migration communication control device
network B
143'
(1)
(2)
(3)
(4)
migration address unit
125
stationary host
151
network C
115
migration address unit
146
mobile host
message 182
response message 182R

FIG. 43

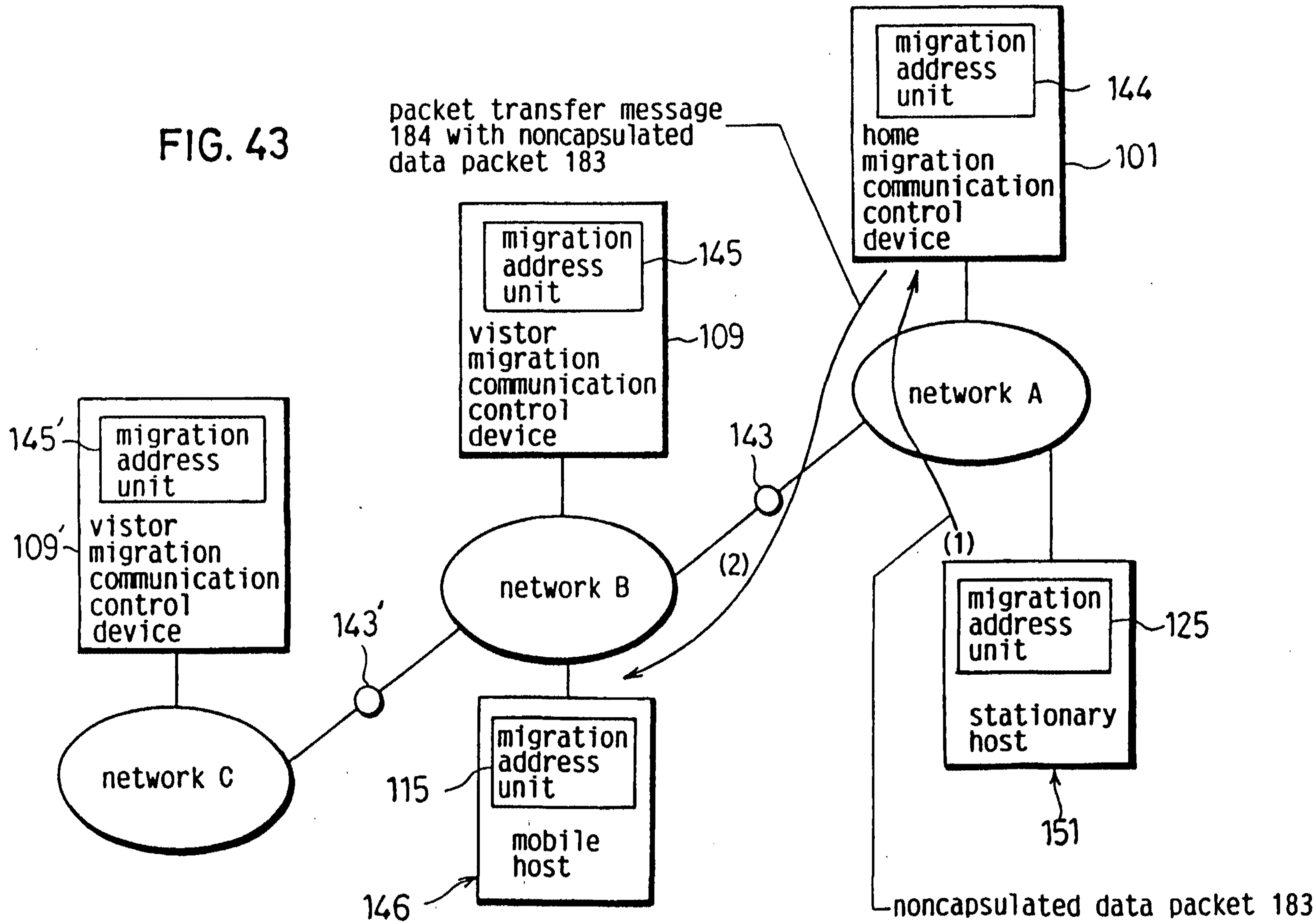

packet transfer message 184 with noncapsulated data packet 183
migration address unit
144
home migration communication control device
101
migration address unit
145
vistor migration communication control device
109
145'
migration address unit
109'
vistor migration communication control device
143
network A
network B
(2)
(1)
143'
network C
migration address unit
125
stationary host
151
migration address unit
115
mobile host
146
noncapsulated data packet 183

FIG. 44

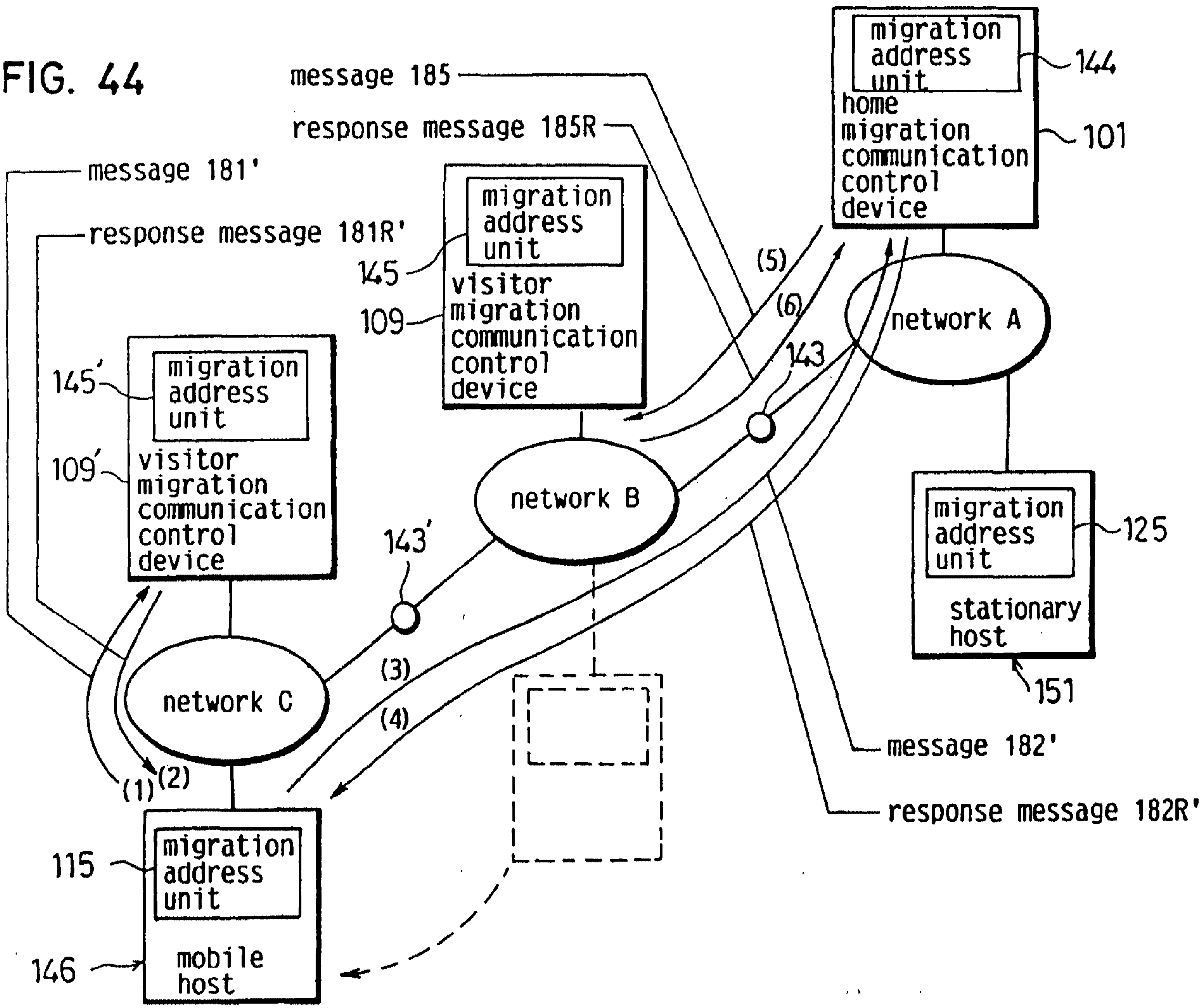
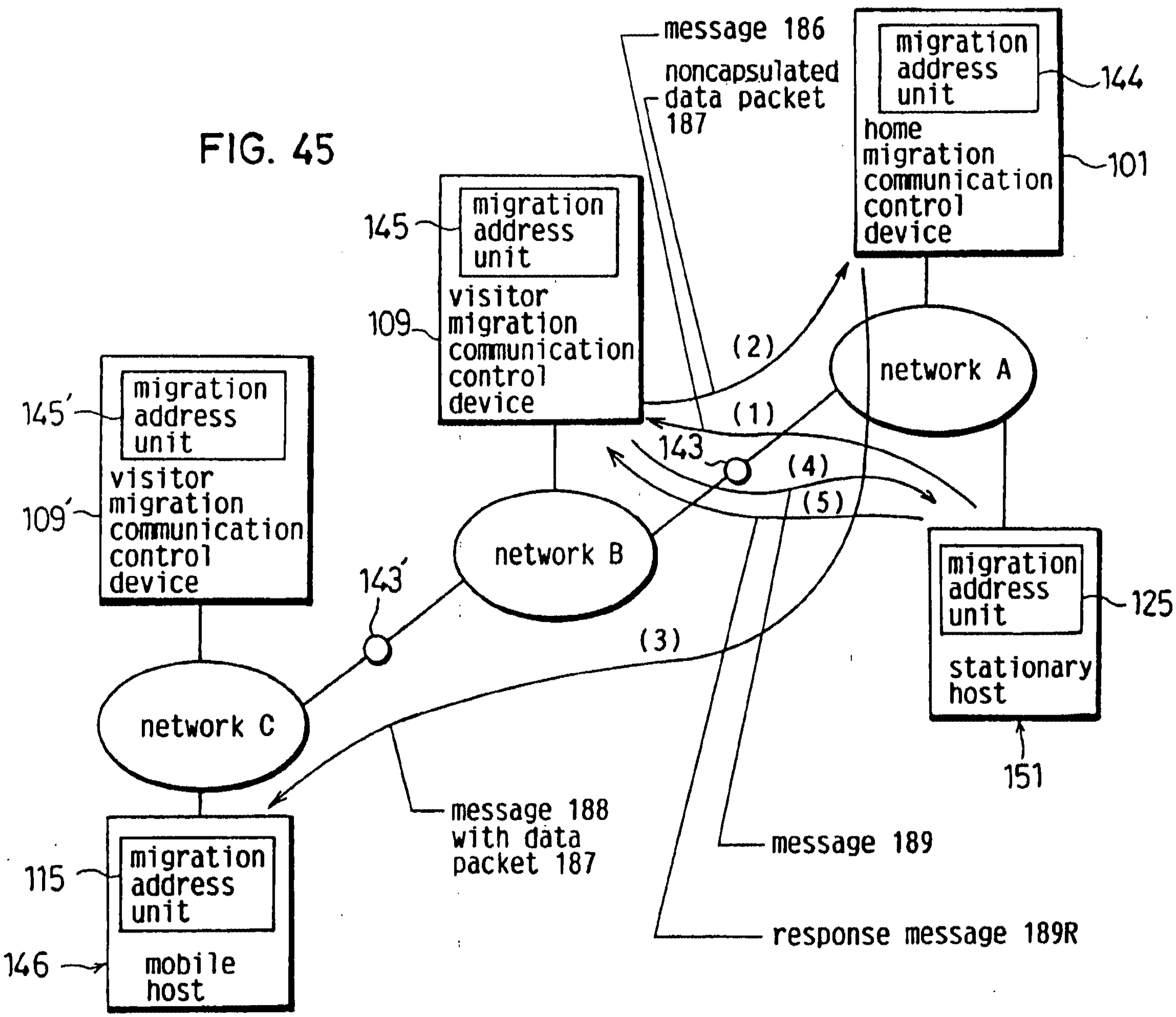

message 185
response message 185R
message 181'
response message 181R'
migration address unit
home migration communication control device
144
101
migration address unit
visitor migration communication control device
145
109
(5)
(6)
143
network A
migration address unit
visitor migration communication control device
145'
109'
network B
143'
migration address unit
stationary host
125
151
network C
(3)
(4)
(1)
(2)
message 182'
response message 182R'
migration address unit
mobile host
115
146

FIG. 45


message 186
noncapsulated data packet 187
migration address unit
144
home migration communication control device
101
145
migration address unit
visitor migration communication control device
109
(2)
network A
(1)
143
(4)
(5)
145'
migration address unit
visitor migration communication control device
109'
143'
network B
migration address unit
125
stationary host
(3)
network C
151
message 188 with data packet 187
message 189
115
migration address unit
146
mobile host
response message 189R

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 556 012 A3**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number : **93300919.3**

(22) Date of filing : **09.02.93**

(51) Int. Cl.^{5} : **H04Q 7/00,** H04L 12/56

(30) Priority : **10.02.92 JP 23506/92**
16.09.92 JP 246855/92
10.11.92 JP 299531/92

(43) Date of publication of application :
18.08.93 Bulletin 93/33

(84) Designated Contracting States :
DE FR GB

(88) Date of deferred publication of search report :
03.05.95 Bulletin 95/18

(71) Applicant : **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
1006, Kadoma
Kadoma-shi, Osaka-fu 571 (JP)

(72) Inventor : **Wada, Hiromi**
15-10, Higashigaoka, Uzumasa
Neyagawa-shi, Osaka 572 (JP)
Inventor : **Yozawa, Takashi**
5-16-19, Shinke, Aoo
Mino-shi, Osaka 562 (JP)
Inventor : **Ohnishi, Tatsuya**
281-5, Kawahara,
Aza,
Sasabe
Kawanishi-shi, Hyogo 666-01 (JP)

(74) Representative : **Cummings, Sean Patrick et al**
David Keltie Associates
Audrey House
Ely Place
London EC1N 6SN (GB)

(54) **Migration communication control device.**

(57) Disclosed is a migration communication control device constructed to control a continuous communication between a mobile node and a node unaffected the mobile node's migration. The migration communication control device comprises a first migration control unit, a second migration control unit on the mobile node, and a third migration control unit on the partner node. The first migration control unit comprises a packet transfer unit and an address post unit. The packet transfer unit receives a packet which was destined for an outdated address of the mobile node, generates a conversion packet which holds an updated address instead of the outdated address, and then transmits the conversion packet, while an address post unit transmits an address post message which indicates the updated address to the third migration control unit. The second migration control unit comprises a migration post unit and a packet resumption unit. The migration post unit transmits to the first migration control unit a migration post message which indicates the updated address when the mobile node migrates to another network while a packet resumption unit receives the conversion packet from both the first migration control unit and the third migration control unit and resumes an original packet from the conversion packet. The third migration control unit comprises a packet conversion unit which converts a destination address of a packet into the updated address, then transmits it to the mobile node.

EP 0 556 012 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 93300919.3

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	DATABASE WPIL, no. 90-311 754, DERWENT PUBLICATIONS LTD., London; & TP-A-99 004 (ANONYMOUS) * Abstract * --	1, 38-40	H 04 Q 7/00 H 04 L 12/56
A	GB - A - 2 236 393 (SHELL INTERNATIONALE RESEARCH MAATSCHAPPIJ B.V.) * Fig. 2A,2B; abstract; claim 1 * --	1, 38-40	
A	WO - A - 86/01 918 (HOLBERG) * Fig. 1,2; abstract; claim 1 * ----	1, 38-40	

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

H 04 Q 7/00
H 04 L 12/00
G 06 F 15/00
G 01 V 1/00

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
VIENNA	03-02-1995	BERGER

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : 0 455 402 A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number : 91303643.0

(51) Int. Cl.^{5} : H04L 12/24

(22) Date of filing : 23.04.91

(30) Priority : 03.05.90 US 519187

(43) Date of publication of application : 06.11.91 Bulletin 91/45

(84) Designated Contracting States : DE FR GB

(71) Applicant : Hewlett-Packard Company
Mail Stop 20 B-O, 3000 Hanover Street
Palo Alto, California 94304 (US)

(72) Inventor : Wu, Jeff C.
2630 Wapiti Road
Fort Collins, Colorado 80525 (US)

(74) Representative : Colgan, Stephen James et al
CARPMAELS & RANSFORD 43 Bloomsbury Square
London WC1A 2RA (GB)

(54) Automatic discovery of network elements.

(57) Disclosed is a computer network node discovery system that provides a general way of discovering network elements, or nodes, connected to a computer network, and a specific algorithm for discovering nodes connected to a TCP/IP network, using the SNMP protocol available within the TCP/IP network software. Some nodes on a network, called discovery agents, can convey knowledge of the existence of other nodes on the network. The network discovery system queries these agents and obtains the information they have about other nodes on the network. It then queries each of the nodes obtained to determine if that node is also a discovery agent. In this manner, most of the nodes on a network can be discovered. The process of querying discovery agents to obtain a list of nodes known to the discovery agents is repeated at timed intervals to obtain information about nodes that are not always active. In a TCP/IP network, discovery agents are nodes that respond to queries for an address translation table which translates internet protocol (IP) addresses to physical addresses. The data from each node's address translation table is used to obtain both the IP and the physical address of other nodes on the network. These nodes are then queried to obtain additional information. After all the nodes on a network are discovered, the list of nodes is written to a database where it can be displayed by the network manager or other users of the network.

EP 0 455 402 A2

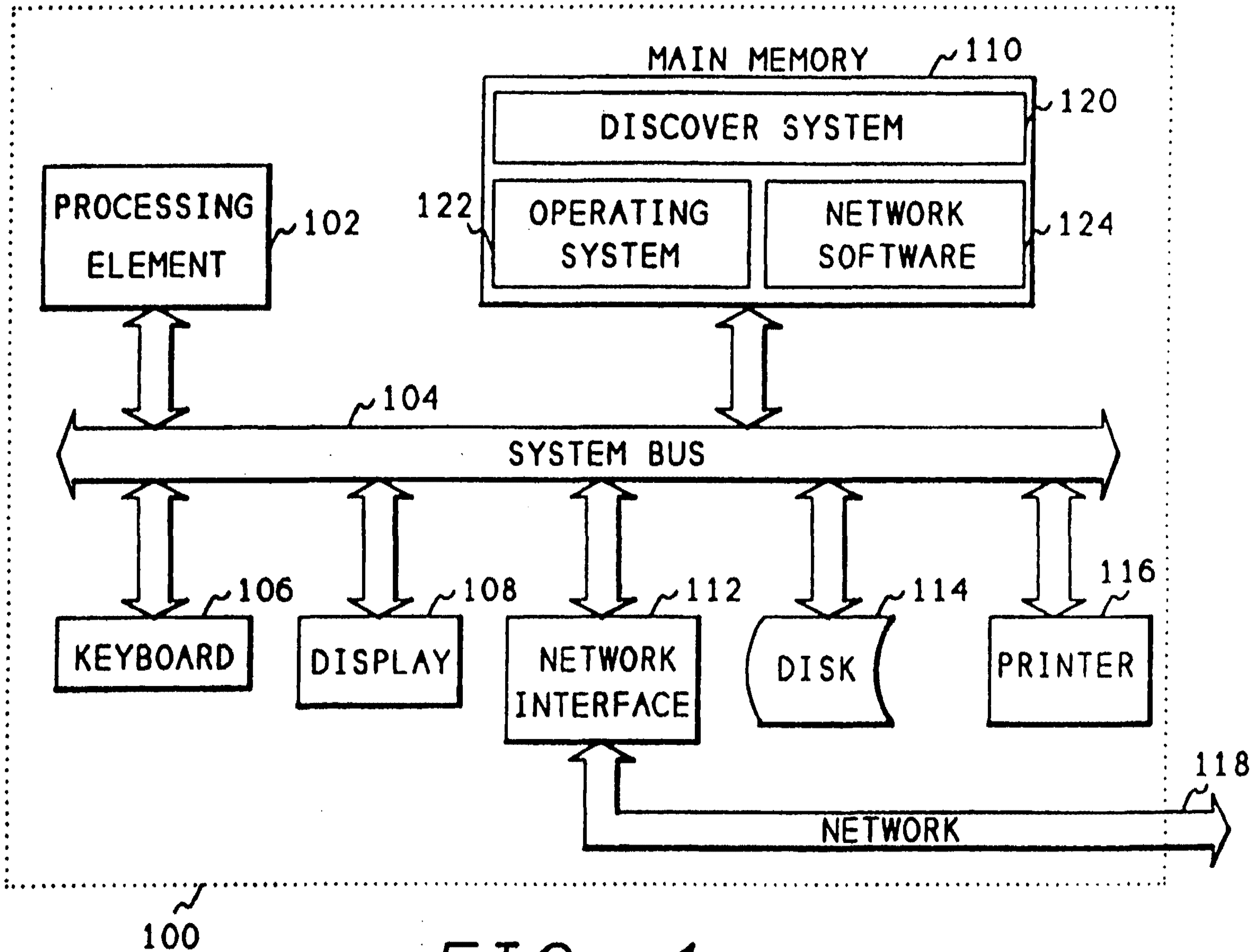

MAIN MEMORY
110
DISCOVER SYSTEM
120
PROCESSING ELEMENT
102
122
OPERATING SYSTEM
NETWORK SOFTWARE
124
104
SYSTEM BUS
106
108
112
114
116
KEYBOARD
DISPLAY
NETWORK INTERFACE
DISK
PRINTER
118
NETWORK
100

FIG. 1

FIELD OF THE INVENTION

This invention relates to computer systems and more particularly to computer networks that interconnect computers. Even more particularly, the invention relates to determining the nodes connected to a network.

BACKGROUND OF THE INVENTION

Computer networks are collections of hardware and software that connect computers and allow them to send information from one computer to another electronically. A computer network is comprised of the physical hardware connections between the various computers, for example telephone lines or a coax cable, and the software used to send and receive data and to route the data to the selected computer on the network.

A local area network (LAN) is a network connection between computers in close proximity, typically less than one mile, and usually connected by a single cable such as coax cable. A wide area network (WAN) is a network of computers located at longer distances, often connected by telephone lines or satellite links. Network software may sometimes be used with both types of networks. For example, a popular network is the Department of Defense internetworking protocol suite, known as Transmission Control Protocol/Internet Protocol (TCP/IP). This system was originally developed by the Defense Advanced Research Projects Agency (DARPA) and has now been widely distributed to Universities and industry.

When a network is fast growing, that is, network elements or nodes are being added frequently, a network administrator may not know all of the nodes connected to the network. Also, a network administrator new to his or her job may not be familiar with the nodes on the network. Determining the nodes manually is a difficult problem. The administrator may contact all the users of the network known to the administrator, however, infrequent users may be forgotten and not contacted. Also, if a node is connected to the network, but not active because the computer is not powered up or is inoperative, that node may not be included in the list. In a very short local area network, a network administrator may physically trace the cable of the network to determine which nodes are located on the network. However, since longer local area networks can extend as far as a mile, through many floors and offices within a building, physical tracing may be impossible. In a wide area network, physical tracing is almost always impossible.

For some commonly used networks, special equipment can be purchased that will determine the nodes located on the network and the distance between them. This equipment, called a probe, is often limited by the other components of the network, however. For example, in a local area network, a repeater unit may be used to extend the effective distance of the local area network to a distance greater than is capable with a single cable. A repeater unit amplifies signals, and therefore will not allow a probe to determine the location of nodes beyond the repeater.

Other units connected to the network may obscure nodes. For example a bridge unit connects two similar networks but only passes messages that are being sent from a node on one side of the bridge to a node on the other side of the bridge. It will not pass messages between nodes on the same side, in order to reduce the traffic on the other side of the bridge. A bridge will prevent a probe from determining the nodes on the other side of the bridge. A gateway is a unit that connects dissimilar networks to pass messages. Because a gateway may have to reformat a message to accommodate a different network protocol, it will prevent a probe from finding nodes beyond the gateway.

There is need in the art then for a method of determining the nodes on a local area network. There is further need in the art for determining such nodes without the use of special equipment. A still further need is for a method that will determine which nodes are located beyond the repeater units, bridges, and gateways on a network.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method of determining the elements or nodes connected to a network.

It is another object of the invention to provide a method of discovering network nodes on a TCP/IP network.

Another object of the invention is to determine which discovered nodes are discovery agents and can convey knowledge of the existence of other nodes on the network.

Another object is to query all discovery agents and ask for other nodes on the network

A further object is to query all TCP/IP nodes to retrieve the address translation table from the TCP/IP node.

The above and other objects of the invention are accomplished in a system which provides a general way of discovering network elements, or nodes, and a specific algorithm for discovering nodes within a TCP/IP network, using a standard Simple Network Management Protocol (SNMP), which is available within the TCP/IP network.

Some nodes on a network can convey knowledge of the existence of other nodes on a network, and are called discovery agents. When a network contains discovery agents, these agents can be queried to obtain the information they have about other nodes on the network. By obtaining a list of nodes from a single discovery agent, and querying each of the nodes obtained to determine if it is also a discovery agent, most of the nodes on a network can be discovered.

The process of querying discovery agents to obtain a list of nodes known to be discovery agents, must be repeated at timed intervals. At any given time on a network, one or more nodes may not be responding to the network, either because it is inoperative, or because it is not powered up. Therefore, if the discovery process is attempted during this time, these unavailable nodes will not be discovered. By repeating the discovery process over time at regular intervals, additional nodes on a network can be discovered.

In a TCP/IP network, discovery agents are nodes that respond to queries for an address translation table. Within TCP/IP network, every node will have an internet protocol (IP) address. This address is a 32 bit number and is unique to all nodes within the TCP/IP network. Although the IP address is probably unique to all nodes everywhere that use the TCP/IP protocol, the physical address of a node on a particular network will be different from the IP address. For example, some types of LANs use an 8 bit address, and can therefore use the low order 8 bits of the IP address, however, some other types of LANs use a 48 bit address and cannot use the internet address. Therefore, every node within a TCP/IP network must have an address translation table which translates the IP address to the physical address. The data from each node's address translation table can be used to obtain both the IP and the physical address of other nodes on the network. Again, as described in the above general algorithm, the queries should be repeated at timed intervals to insure that recently activated nodes are discovered. Another reason for repeating the discovery process over timed intervals in a TCP/IP network is that some of the information within a node's address translation table may be purged if the node does not use the information after a period of time. This purge is used to reduce the table size requirements within a node. By repeating the queries at timed intervals, the greatest amount of translation table information may be obtained.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features, and advantages of the invention will be better understood by reading the following more particular description of the invention, presented in conjunction with the following drawings, wherein:

Fig. 1 shows a block diagram of the hardware of the node that runs the process of the present invention;

Fig. 2 shows a diagram of a typical computer interconnection network;

Figs. 3 through 5 show a hierarchy diagram of the modules of the discovery system of the present invention;

Fig. 6 shows a flowchart of the main module of the invention;

Fig. 7 shows a flowchart of the self-seed module of the invention;

Fig. 8 shows a flowchart of the process-node module of the invention;

Fig. 9 shows a flowchart of the process-ping module of the invention;

Fig. 10 shows a flowchart of the process-IFIP module of the invention;

Fig. 11 shows a flowchart of the store-IP module of the invention;

Fig. 12 shows a flowchart of the store-IF module of the invention;

Fig. 13 shows a flowchart of the invalidnode module of the invention;

Fig. 14 shows a flowchart of the findnode module of the invention;

Fig. 15 shows a flowchart of the addnode module of the invention;

Fig. 16 shows a flowchart of the process-AT module of the invention; and

Fig. 17 shows a flowchart of the store-AT module of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The following description is of the best presently contemplated mode of carrying out the present invention. This description is not to be taken in a limiting sense but is made merely for the purpose of describing the general principles of the invention. The scope of the invention should be determined by referencing the appended claims.

Fig. 1 shows a block diagram of the computer hardware that contains the discovery system of the present invention. Referring now to Fig. 1, a computer system 100 contains a processing element 102. The processing element 102 communicates to other elements within the computer system 100 over a system bus 104. A keyboard 106 is used to input information from a user of the system, and a display 108 is used to output information to the user. A network interface 112 is used to interface the system 100 to a network 118 to allow the computer system 100 to act as a node on a network. A disk 114 is used to store the software of the discovery system of the present invention, as well as to store the data base collected by the discovery system. A printer 116 can be used to provide a hard copy output of the nodes of the network discovered by the discovery system. A main memory 110 within the system 100 contains the discovery system 120 of the present invention. The discovery system 120 communicates with in operating system 122 and network software 124 to discover the nodes on the network 118.

Fig. 2 shows a diagram of a network. Referring now to Fig. 2, a network 202 contains a node 206. Node 206 contains the processor 100 (Fig. 1) which contains the discovery system software of the present invention. Node 206 is attached to a first network segment 118. The network segment 118 is connected to a repeater 212 which is connected to a second network sequent 214. This second network system 214 has nodes 216 and 218 attached to it. A repeater, such as repeater 212, allows network sequents to be connected to allow a network to be extended over a longer distance. An important characteristic of a repeater is that there is no translation of data passing through it. That is, every message that is transmitted on one network segment, will pass unchanged through a repeater to the other network segment. Therefore, any messages broadcast, for example, by node 206 will be received by node 216 and node 218 after these messages pass through repeater 212.

Network segment 118 is also attached to a bridge 208 which connects it to a third network sequent 210. A bridge will only pass messages that are being transmitted from a node on one side of the bridge to a node on the other side of the bridge. It will block messages that are transmitted from a node on one side of the bridge to a node on that same side of the bridge. This characteristic reduces network traffic on various sequents of a network.

Segment 118 is also attached to a router/gateway 220 which connects is to a fourth network segment 222. Routers are devices that connect network segments which have similar characteristics. Gateways are devices which connect networks having different types of characteristics. For example, a gateway might connect a local area network to a wide area network.

Because bridges, routers, and gateways, must process the messages sent over the network, they also must contain information about which nodes are on the network. Therefore, bridges, routers, and gateways are authoritative sources of information for determining the nodes on the network. A protocol defines the format of messages that are sent across a network. One popular protocol is the Department of Defense Internetworking Protocol Suite, popularly known as TCP/IP. Because it was developed by the Department of Defense, this protocol is widely available and used extensively, particularly in a university environment. Also, this suite of protocols is very popular on the UNIX operating system and has seen wide distribution there. The internet protocol (IP) uses a single thirty-two bit address for all nodes that can be connected to the internet at any location. Physical addresses within a particular type of network, are normally different from an IP address. If a network address is very small, perhaps eight bits, it may be the same as the low order eight bits of the IP address. If a network address is large, for example, some LANs use forty-eight bit addresses, it is impossible for these addresses to correspond directly to IP addresses. Therefore, both an IP address and a physical address exist for each node on a network. Devices such as routers, gateways, and bridges, which can send messages from one network to another must be able to translate between IP addresses and physical addresses. Therefore, these devices have translation tables which allow them to translate between these two types of addresses. By accessing these translation tables, one of the nodes on a network can obtain information about the other nodes on the network. The existence of these translation tables allow the method of the present invention to perform its function.

A network probe 224 is also attached to the network 118. A network probe 224 is a device that assists in locating defective nodes and assists in repairing those nodes. Since it is a testing device, it may or may not be attached to a network at any given time. When a probe is attached to a network, the discovery system of the present invention can query the probe and use information obtained from the probe to assist in discovering other nodes on the network.

Figs. 3 through 5 show a hierarchy diagram of the modules of the software of the present invention. Referring now to Figs. 3 through 5, discovery module 302 is the main module of the system. Discovery calls self-seed block 304 to start the process of building a database about the network, and it calls process-node block 306 to process information about each node that it obtained from self-seed. Process-node block 306 calls process-ping block 308 to query a node on the network to determine if that node is active. Process-node block 306 also calls process-IFIP block 310 for each IP address that it obtains. Process-IFIP block 310 calls store-IP block 402 for each IP address, and store-IP block 402 calls invalidnode block 406, findnode block 408, and addnode block 410, for each IP address. For each IF entry (physical address) received, process-IFIP block 310 calls store-IF block 404. For each address translation table entry, process-node block 306 calls process-AT block 312 which in turn calls store-AT block 502. Store-AT block 502 calls invalidnode at block 504, findnode block 506, and addnode block 508.

Fig. 6 shows a flowchart of the discovery module block 302 (Fig. 3). Referring now to Fig. 6, after entry block 602 gets any options that the user wishes to enter. Block 604 then initializes the database used to permanently store the nodes, and loads node list from existing entries in the database. If a database for the network does not exist, the discovery system has the ability to create that database. If a database of the network already exists, the discovery system will use the node information which is already available in that database to query other nodes within the system.

Block 606 then initializes domains. A domain defines the limit beyond which the user of the discovery system does not wish to find nodes. That is, the domain limits the range of the discovery process. This limitation is necessary on large networks, to keep the amount of processing to reasonable level. Furthermore, a user usually is only interested in the nodes on a particular network segment, or the network segment connected by repeaters and possibly bridges.

Block 608 then calls Fig. 7 to self-seed the system. If no entries were available in the database, the discovery system can self-seed by sending a broadcast message and determine who responds to that message. After returning from self-seed, block 610 points to the first node list entry. As discussed earlier, the node list will contain a list of the nodes already known to the system. This list can be input from the database, or the list can be started from self-seed module. After pointing to the first entry, block 612 determines if there are more entries to process. If there are no more entries to process, block 612 transfers to block 614 which will wait a predetermined period of time before reprocessing the entire node list. Typically, block 614 will wait for approximately thirty seconds. By reprocessing the node list periodically, additional nodes can be discovered. This is because a node may be inactive on the system at any given time and might not be discovered by a single pass through the network. By waiting and reprocessing the node list, nodes that were inactive may now be active and additional information can be obtained.

If more entries in the node list exist, block 612 transfers to block 616 to process one of the nodes. After processing that node, block 616 transfers to block 618 which points to the next node list entry and returns to block 612 to process the next node.

Fig. 7 shows a flowchart for the self-seed block 304 (Fig. 3) which obtains initial information about nodes on the network. Referring now to Fig. 7, after entry, block 702 sends an SP broadcast request to all nodes on the network. SNMP stands for Simple Network Management Protocol, and is a part of the TCP/IP network software. After sending the broadcast request, block 702 transfers to block 704 which receives SNMP messages from the nodes. If more SNMP messages are available, block 704 transfers to block 706 which adds a node to the node list for each message received. In this manner, all nodes that are currently active on the network can be queried to obtain initial information about the node. After all SNMP messages have been received, block 704 returns to the caller.

Another way of self-seeding is to query the address translation table for the node that is executing the discovery system. This table will contain the addresses of other nodes on the network, and these addresses are then used to start the discovery process.

Fig. 8 is a flowchart of the process-node block 306 (Fig. 3). The process-node module of Fig. 8 is called from the discovery module of Fig. 6 once for each entry in the node list. Therefore, whin Fig. 8 is called, the address of a single node is passed to it. Referring now to Fig. 8, after entry, block 802 determines whether the node is within a domain. As discussed earlier, the domain defines the limits beyond which the discovery program does not wish to discover new nodes. If the node is within the domain, block 802 transfers to block 804 which calls the process-ping module of Fig. 9 to determine whether the node is active. After returning from Fig. 9, block 804 transfers to block 806 to determine whether the state of the node has changed since the last information was obtained. That is, when the process-ping module queries the node, it determines the state of the node at the present time. This state is compared, in block 806, with the state of the node as it was known previously in the database. If that state has changed, block 806 transfers to block 808 to store the new state in the database. Control then returns to block 810 which calls process-IFIP to retrieve the IF and IP tables from the node. After returning from Fig. 10, block 810 transfers to block 812 which determines whether the node responded to an SNMP request. If the node did respond to the SNMP request, block 812 transfers to block 814 which determines whether the node is currently in the database. If the node is not in the database, block 814 transfers to block 816 to add the node to the database. Control then continues at block 818 which calls Fig. 16 to retrieve the address translation table from the node. Control then returns to the caller.

Fig. 9 shows a flowchart of the process-ping module block 308 (Fig. 3). This module is called to determine whether a node is active on the network. Referring now to Fig. 9, after entry block 902 determines whether the ping interval has elapsed. The ping interval is used to prevent a node from being queried too often. If the ping interval has not elapsed, block 902 returns to the caller. If the ping interval has elapsed, block 902 transfers to block 904 which sends an ICMP-echo message to the node. The ICMP-echo protocol is defined as a part of TCP/IP and is used to cause the node to return an acknowledgement to a message. Block 904 then transfers to block 906 which determines whether a response has been received from the other node. If a response has not been received within a predetermined amount of time, typically block 906 transfers to block 910 which sets a flag to indicates that the node failed to respond. If the node does respond, block 906 transfers to block 908 which sets a flag to indicate that the node did respond and then block 912 sets a new ping interval which will prevent the node from being pinged for the period of the interval. The ping interval is typically five minutes. Block 912 then returns to the caller.

Fig. 10 shows a flowchart of the process-IFIP module block 310 (Fig. 3). The IF and IP tables are available in a node to define the translation of physical addresses to IP addresses. The information is available as two different tables, with an index contained in the IF table to cross-reference to the IP table within the node. By obtaining these two tables, the discovery system can determine what the other interfaces to which a node is connected, and therefore determine other networks to which the node is connected. Referring now to Fig. 10, after entry, block 1002 determines whether the IFIP interval has elapsed. The IFIP interval is similar to the ping interval described with respect to Fig. 9, and is used to keep a node from being queried too often. If the IFIP interval has not elapsed, block 1002 returns to the caller. If the IFIP has elapsed, block 1002 transfers to block 1004 which sends an SNMP message to request the node to send its next IP table entry to the discovery node. When an entry is received, block 1006 calls store-IP module of Fig. 11 to store the node within the node list. Block 1007 then transfers back to block 1004 if more IP entries are available. After all the entries are all stored in the node list, block 1007 transfers to block 1008 which sets a new IFIP interval of typically greater than 10 hours. Block 1010 then sends an SNMP message to request that the node send its next IF table entry to the discovery node. When an IF table entry is received, block 1012 calls the store-IF module of Fig. 12. Block 1014 then transfers back to block 101 if more entries are available. After receiving and storing all the IF table entries, block 1014 returns to the caller. Each IF table entry contains an index into the IP table. By using this index, physical addresses in the IF table can be matched with the IP address.

Fig. 11 shows a flowchart of the store-IP process block 402 (Fig. 4). Referring now to Fig. 11, after entry block 1102 calls Fig. 14 to find the node in the node list. The node will be found if the discovery system has already encountered this node in its process. Block 1304 then determines whether the node exists, and if the node does not exist, block 1104 transfers to block 1106 which calls Fig. 13 to determine whether the node is valid. Block 1108 then determines if the node is valid and if it is valid, block 1108 transfers to block 1110 to add the node to the node list. After adding the node, or if the node already existed, control goes to block 1112 which updates the state information about the node. After updating the node state information or if the node was not valid, Fig. 11 returns to the caller.

Fig. 12 is a flowchart of the store-IF process of block 404 (Fig. 4). This module is called for each table entry in the IF table received from a node. Referring now Fig. 12, after entry, block 1202 finds the IP index within the IF record. As described earlier, each IF table entry will have a corresponding IP table entry, and the IP entry is referenced by an index value contained in the IF entry. Block 1204 then determines whether a matching IP record exists. If a matching IP record does exist, block 1204 transfers to block 1206 which moves the physical address from the IP record to the node record in the node list. Block 1208 then updates any state information in the node record. After updating the state information, or if there were no matching IP record, Fig. 12 returns to its caller.

Fig. 13 shows a flowchart of the invalidnode module block 406 (Fig. 4). Referring now Fig. 13, after entry, block 1302 determines whether the address of the node is simply the loopback address of another node. Each node has a loopback address associated with it for use in testing the node. Because the loopback address refers to the same node, no additional information can be obtained from that node and the loopback address is never stored as a node address. If the IP address is not equal to the loopback address, block 1302 transfers to block 1304 to determine whether the node is within the domain. As described earlier, the domain is used to determine the limits beyond which the discovery system will not attempt to discover new nodes. If the node is within the domain, block 1304 transfers to block 1306 which returns an indication that the node is valid. If the node is not within the domain or if the IP address equals the loopback address, control transfers to block 1308 which returns an error indication indicating that node is not valid. Control then returns to the caller.

Fig. 14 is a flowchart of the findnode module block 408 (Fig. 4). The module is used to find a node within the node list. Referring now Fig. 14, after entry, block 1402 gets the node list entry. Block 1404 then determines whether the IP address matches the entry in the list. If a match does occur, block 1404 transfers to block 1408 which returns an indication that the node is in the node list. If the IP address does not match, block 1404 transfers to block 1406 which gets the next node list entry and block 1410 then determines whether the end of table has been reached. If the end of the list has not been reached, block 1410 transfers back to block 1404 to check the entry just found. If the end of the list has occurred, block 1410 transfers to block 1412 which returns an error indication indicating that the node is not in the node list.

Fig. 15 shows a flowchart of the process of adding a node to the node list. Referring now to Fig. 15, after entry, block 1502 performs a hash operation on the IP address to create a pointer into the node list. Block 1504 then allocates memory for a node record, and block 1506 stores the data available for the node into the node record at the location pointed to by the hashed IP address. Block 1506 then returns to the caller.

Fig. 16 shows a flowchart of the process-AT module of block 312 (Fig. 3). This module is called by the process-node module for each entry in the node list. Referring now to Fig. 16, after entry, block 1602 determines whether the AT interval has expired. The AT interval is used to prevent a node from being polled too frequently. If the AT interval has not expired, block

1602 simply returns to the caller. If the AT interval has expired, block 1602 transfers to block 1604 which sends an SNMP message to request that the node send its next address translation table entry to the discovery node. When an entry is received, block 1606 is called to store the table entry. Block 1607 then transfers back to block 1604 if more table entries are available. After storing all the table entries, block 1607 transfers to block 1608 which updates the node's state information in the node list. Block 1610 then sets a new AT interval, typically fifteen seconds, and returns to the caller.

Fig. 17 shows a flowchart of the store-AT module of block 502 (Fig. 5). Referring now to Fig. 17, after entry, block 1702 calls the findnode module Fig. 14 to determine whether the node is already in the node list. If the node is in the node list, block 1704 transfers to block 1712. If the node is not in the node list, block 1704 transfers to block 1706 which calls Fig. 13 to determine whether the node is a valid node. If the node is not valid, block 1708 returns to the caller. If the node is valid, block 1708 transfers to block 1710 which calls Fig. 15 to add the node to the node list. After adding the node to the node list, or if the node already existed, control to transfers block 1712 which updates the state information about the node in the node list before returning to the caller.

In addition to querying nodes on the network, the discovery system can also query any network probes that may be attached to the network. Information about other nodes on the network can be obtained from these probes, and the discovery system can use this information to assist in discovering other nodes on the network.

Having thus described a presently preferred embodiment of the present invention, it will now be appreciated that the objects of the invention have been fully achieved, and it will be understood by those skilled in the art that many changes in construction and circuitry and widely differing embodiments and applications of the invention will suggest themselves without departing from the spirit and scope of the present invention. The disclosures and the description herein are intended to be illustrative and are not in any sense limiting of the invention, more preferably defined in scope by the following claims.

Claims

1. A computer network node discovery process (120) for determining nodes (206, 216, 218) connected to a computer network (118), said process (120) comprising the steps of:

   (a) obtaining (306), from one node of a set of known nodes on said computer network (118), a list of addresses of one or more other nodes with which said one node communicates;

   (b) repeating step (a) for each of said other nodes obtained; and

   (c) storing said list of node addresses in a file (808); whereby said list of node addresses may be displayed to a user of said computer network.

2. The process of claim 1 further comprising the step of:

   (d) repeating steps (a) through (c) at regular time intervals.

3. The process of claim 2 further comprising the step of:

   (a1) obtaining from each bridge unit (208) connected to said network (118) a list of addresses of all nodes accessible by said bridge unit (208).

4. The process of claim 3 further comprising the step of:

   (a2) obtaining from each router unit (220) connected to said network (118) a list of addresses of all nodes accessible by said router unit (220).

5. The process of claim 4 further comprising the step of:

   (a3) obtaining from each gateway unit (220) connected to said network (118) a list of addresses of all nodes accessible by said gateway unit (220).

6. The process of claim 5 further comprising the step of:

   (a4) obtaining from any network probe device (224) connected to said network (118) a list of addresses of all nodes known to said network probe device (224).

7. A computer network node discovery process (120) for determining nodes connected to a TCP/IP computer network (118), said process comprising the steps of:

   (a) obtaining (306), from one node of a set of known nodes on said computer network, an address translation table containing a list of addresses of other nodes with which said one node communicates;

   (b) repeating step (a) for each of said other nodes in said address translation table;

   (c) storing said list of nodes in a file (808); and

   (d) repeating steps (a) through (c) at regular time intervals.

8. The process of claim 7 further comprising the steps of:

   (a1) obtaining from each bridge unit (208) con-

nected to said network (118) an address translation table containing a list of addresses of nodes accessible from said bridge unit (208);
(a2) obtaining from each router unit (220) connected to said network (118) an address translation table containing a list of addresses of nodes accessible from said router unit (220);
(a3) obtaining from each gateway unit (220) connected to said network (118) an address translation table containing a list of addresses of nodes accessible from said gateway unit (220);
(a4) obtaining from any network probe devices (224) attached to said network (118) a list of addresses of all nodes known to said network probe (224); and
(a5) obtaining from each node in said network (118) an interface table and an internet protocol table which defines other networks and nodes to which said node is connected.

9. A computer network node discovery process (120) for determining nodes connected to a computer network (118), said process comprising the steps of:
(a) sending a general response message (307) to all nodes on said network;
(b) creating a node list (410) containing the address of each node responding to said general response message;
(c) obtaining (306), from each node in said node list, a second list of addresses of other nodes with which said node communicates;
(d) adding each node (410) in said second list to said node list;
(e) repeating steps (c) through (d) for each of said nodes in said second list;
(f) storing said node list in a file (808); and
(g) repeating steps (a) through (f) at regular time intervals.

10. The process of claim 9 further comprising the steps of:
(c1) obtaining from each bridge unit (208) connected to said network (118) a list of addresses of all nodes accessible by said bridge unit (208);
(c2) obtaining from each router unit (220) connected to said network (118) a list of addresses of all nodes accessible by said router unit (220);
(c3) obtaining from each gateway unit (220) connected to said network (118) a list of addresses of all nodes accessible by said gateway unit (220); and
(c4) obtaining from any network probe devices (224) attached to said network (118) a list of addresses of all nodes known to the network probe (224).

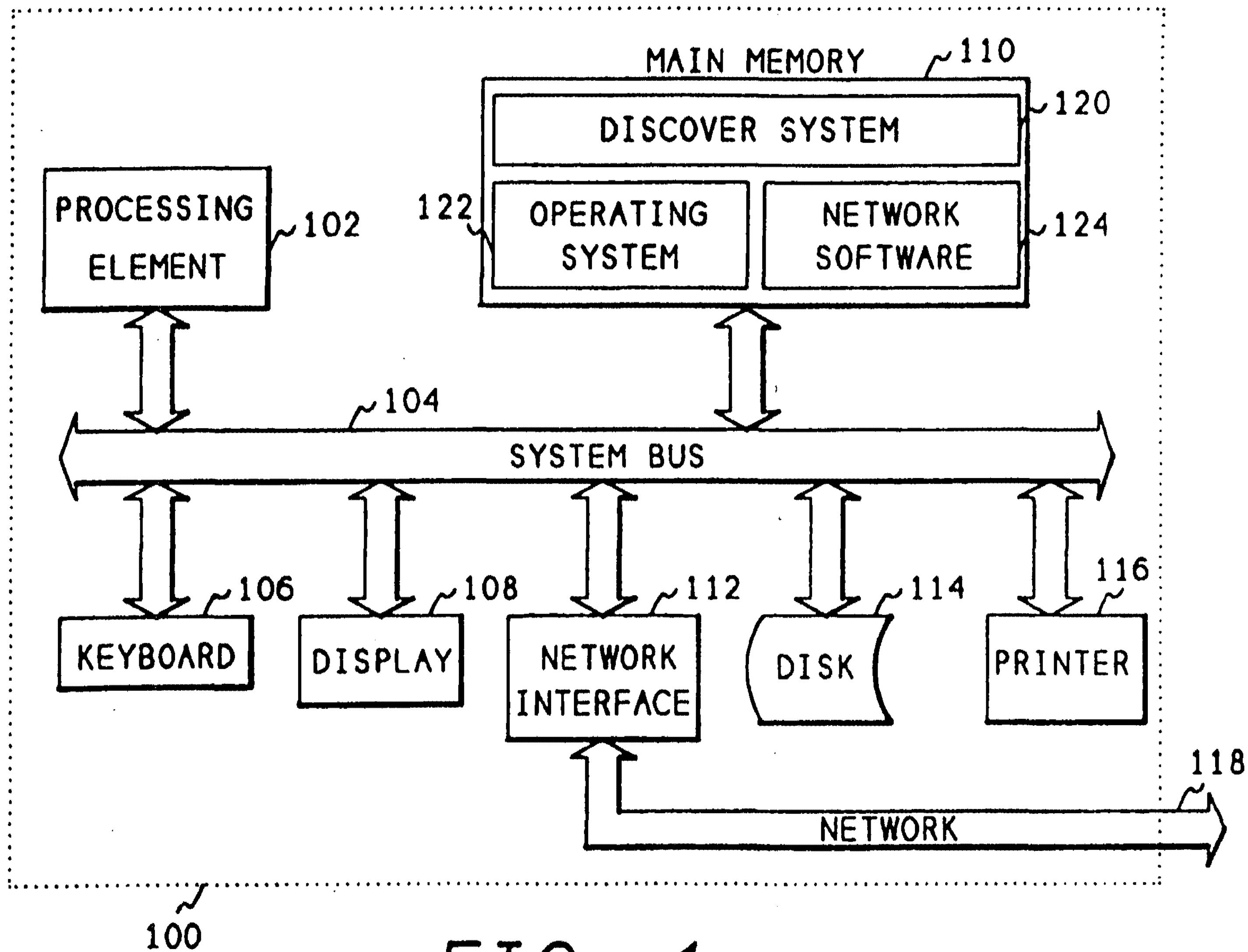

MAIN MEMORY
110
DISCOVER SYSTEM
120
PROCESSING ELEMENT
102
122
OPERATING SYSTEM
NETWORK SOFTWARE
124
104
SYSTEM BUS
106
108
112
114
116
KEYBOARD
DISPLAY
NETWORK INTERFACE
DISK
PRINTER
118
NETWORK
100

FIG. 1

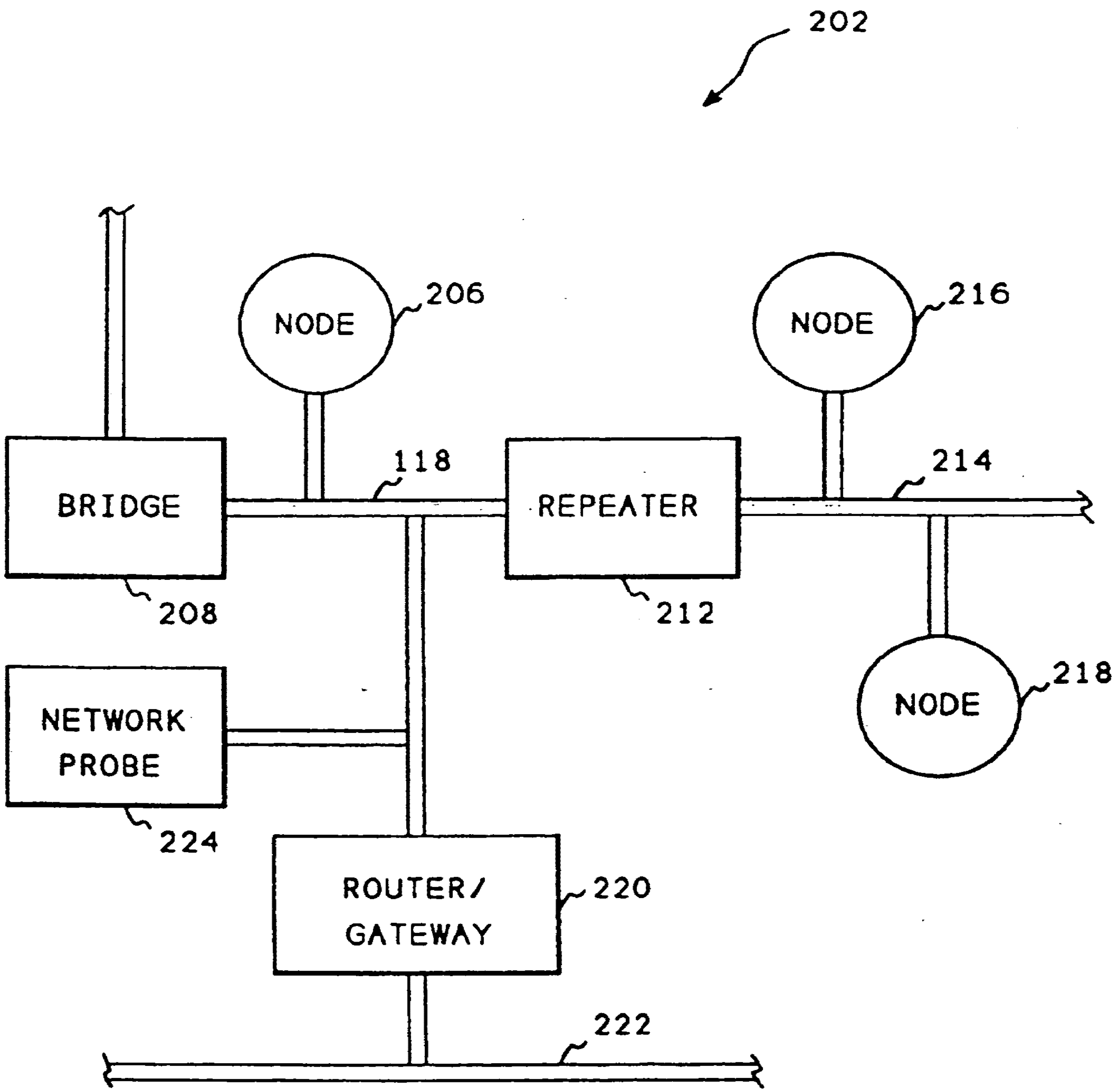

202
NODE
206
NODE
216
BRIDGE
118
REPEATER
214
208
212
NODE
218
NETWORK PROBE
224
ROUTER/ GATEWAY
220
222

FIG. 2

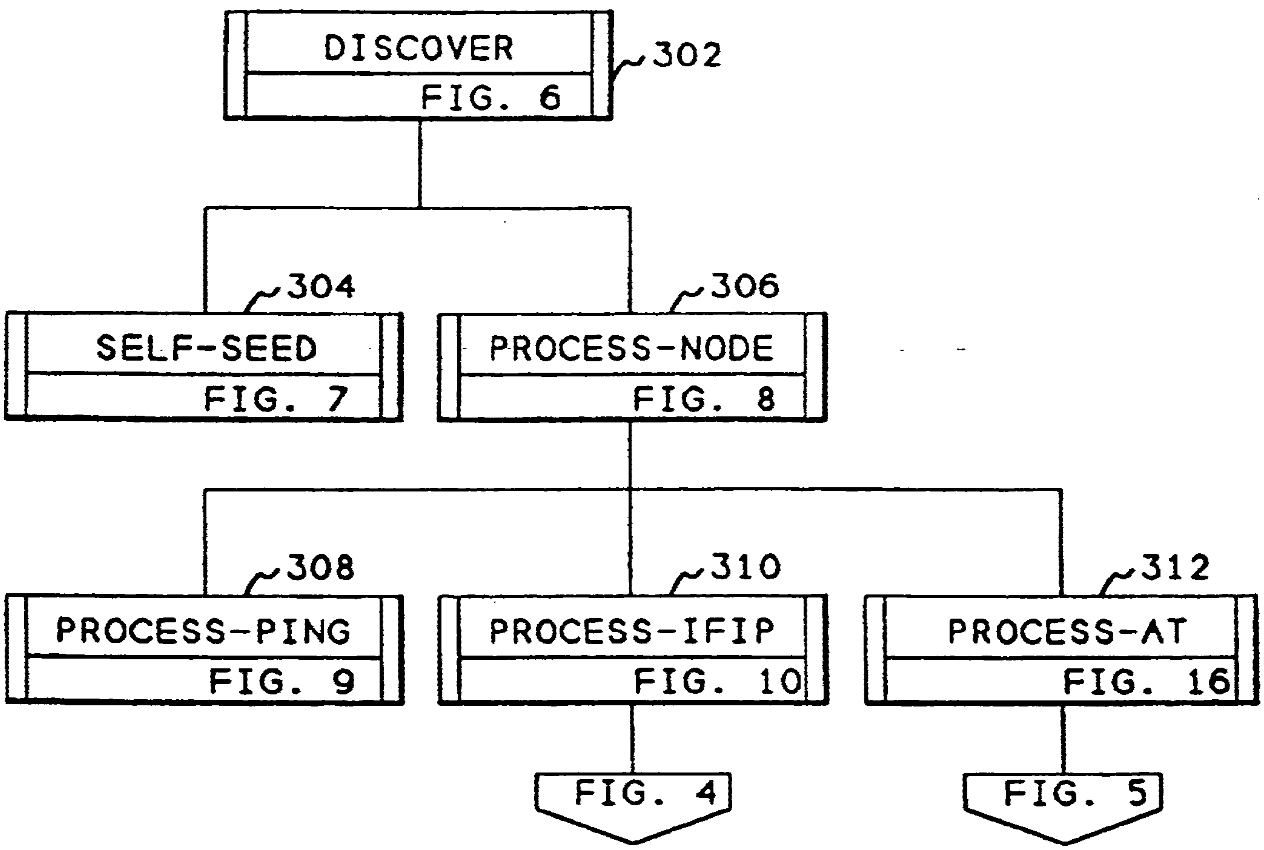

DISCOVER
FIG. 6
302
SELF-SEED
FIG. 7
304
PROCESS-NODE
FIG. 8
306
PROCESS-PING
FIG. 9
308
PROCESS-IFIP
FIG. 10
310
PROCESS-AT
FIG. 16
312
FIG. 4
FIG. 5

FIG. 3

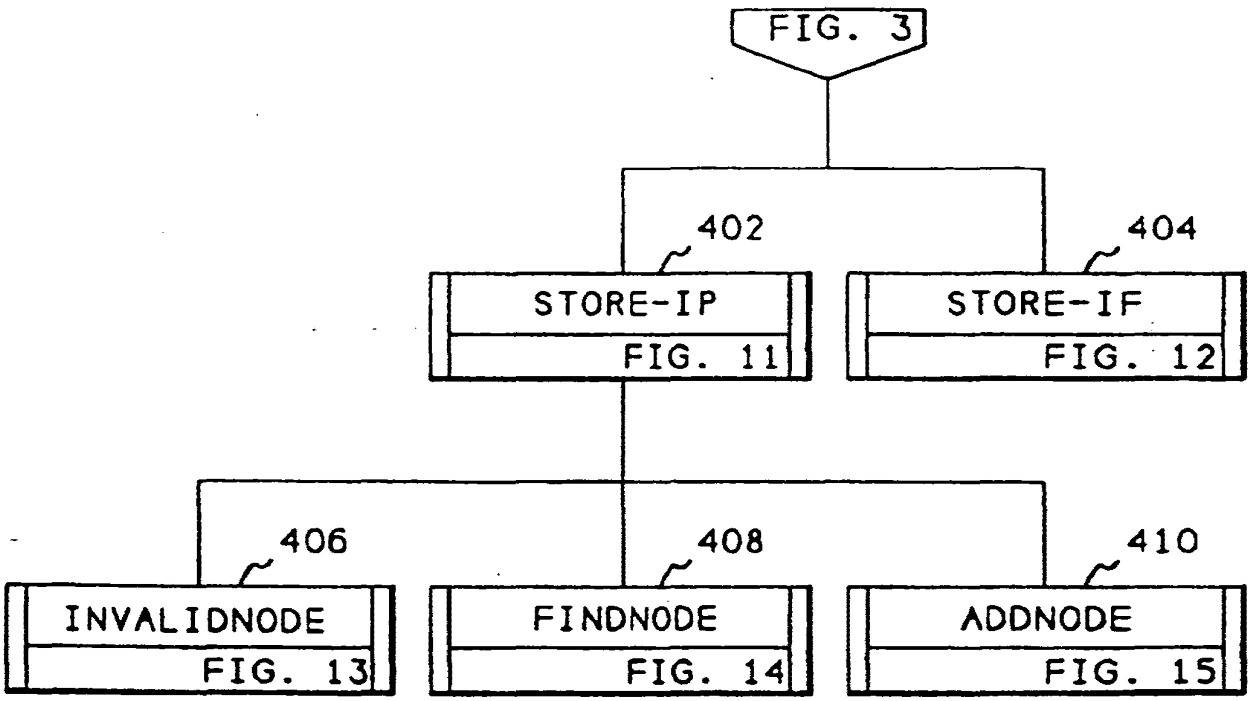


FIG. 3
402
404
STORE-IP
FIG. 11
STORE-IF
FIG. 12
406
408
410
INVALIDNODE
FIG. 13
FINDNODE
FIG. 14
ADDNODE
FIG. 15

FIG. 4

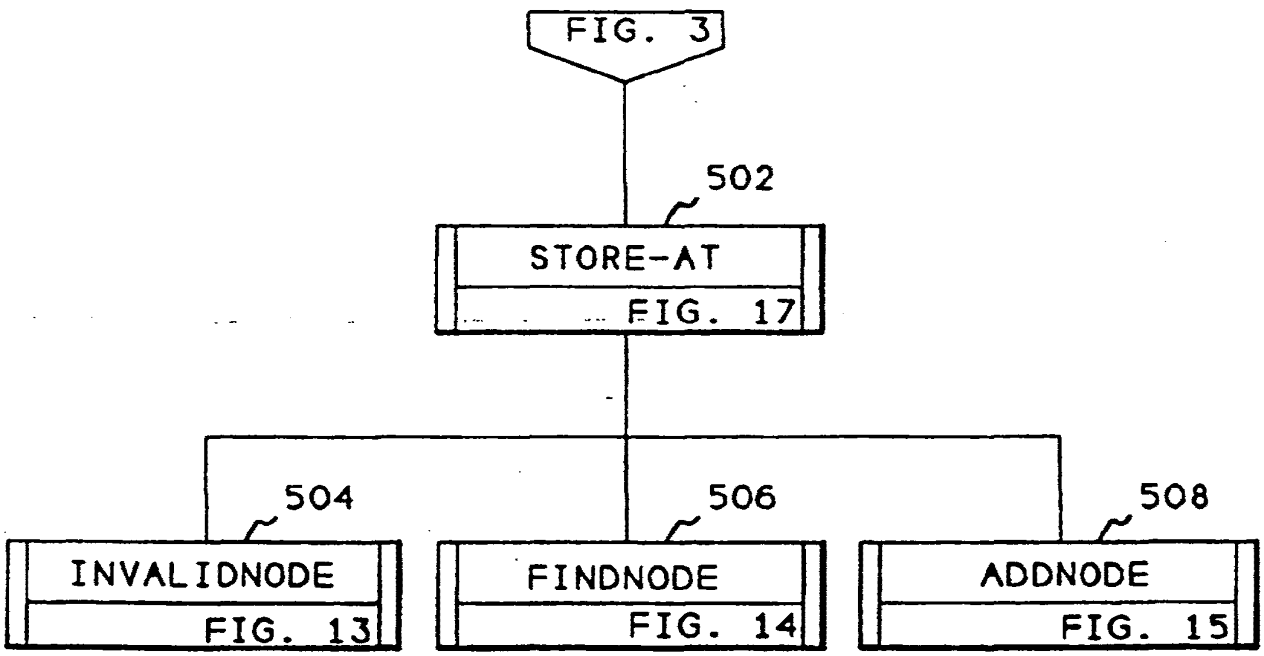


FIG. 3
502
STORE-AT
FIG. 17
504
INVALIDNODE
FIG. 13
506
FINDNODE
FIG. 14
508
ADDNODE
FIG. 15

FIG. 5

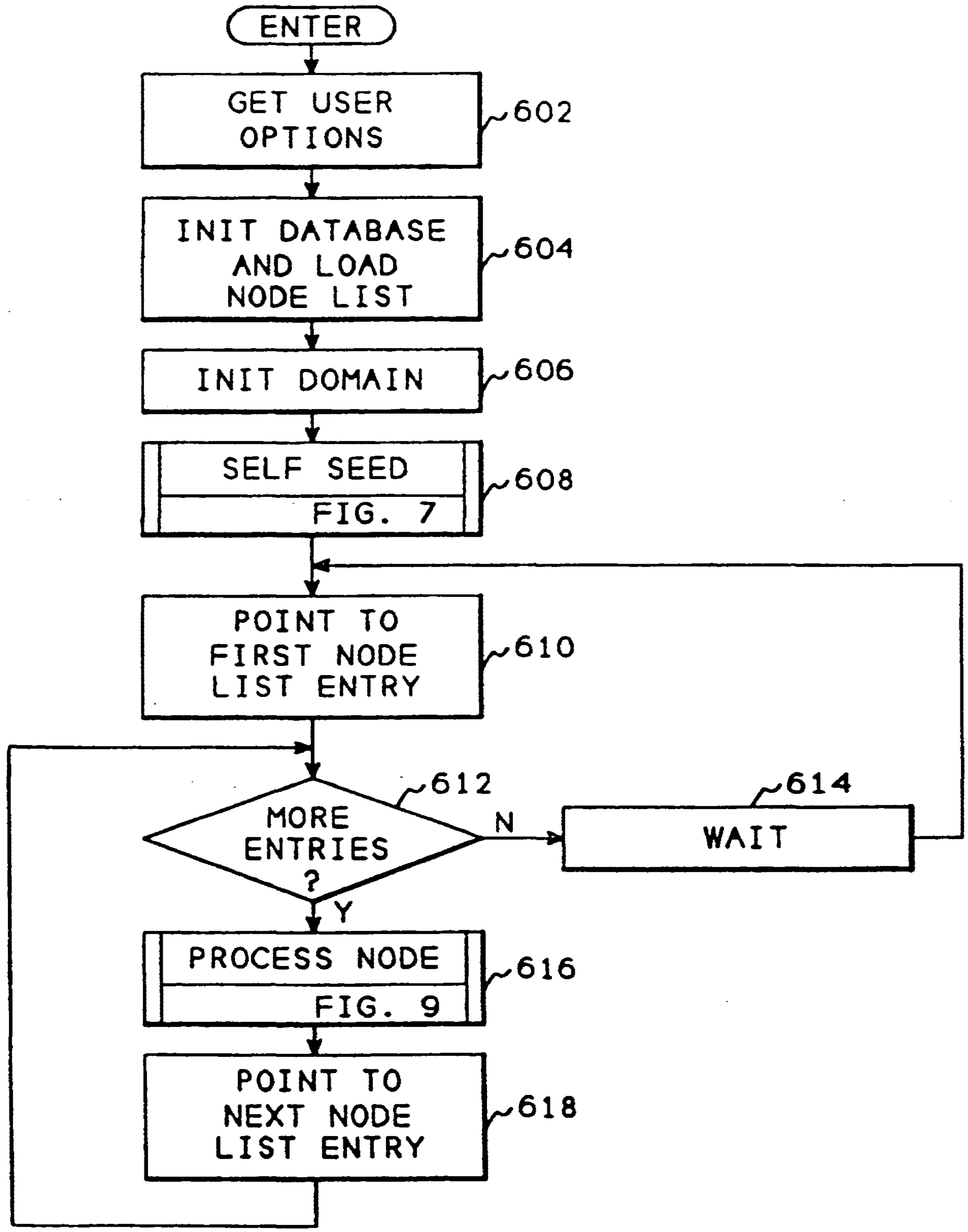
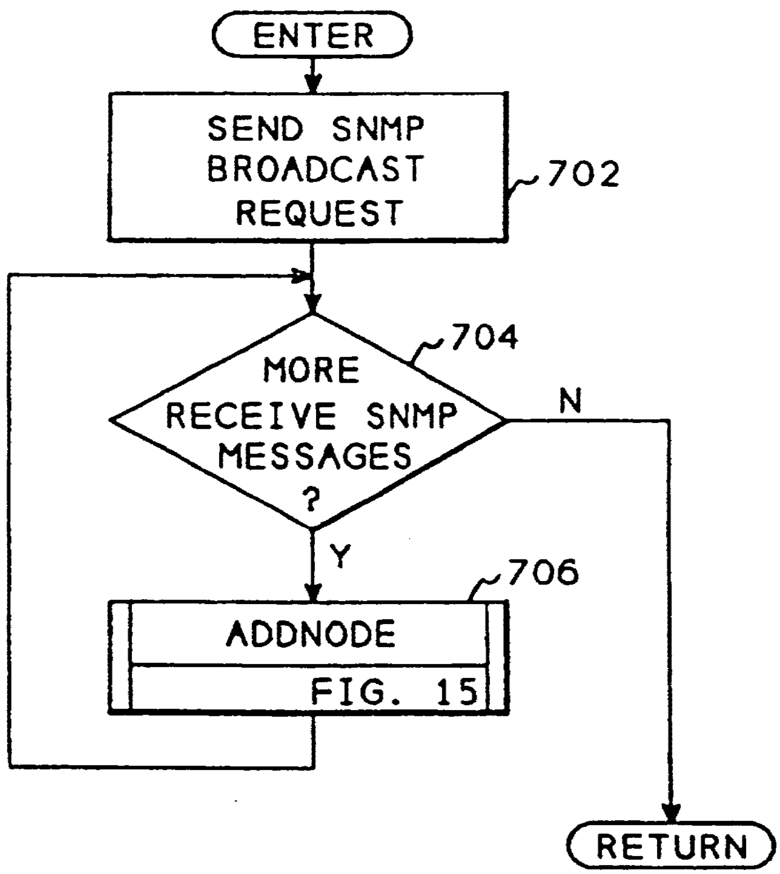

ENTER
GET USER OPTIONS
602
INIT DATABASE AND LOAD NODE LIST
604
INIT DOMAIN
606
SELF SEED
FIG. 7
608
POINT TO FIRST NODE LIST ENTRY
610
MORE ENTRIES ?
612
N
WAIT
614
Y
PROCESS NODE
FIG. 9
616
POINT TO NEXT NODE LIST ENTRY
618

FIG. 6



ENTER
SEND SNMP BROADCAST REQUEST
702
704
MORE RECEIVE SNMP MESSAGES ?
N
Y
706
ADDNODE
FIG. 15
RETURN

FIG. 7

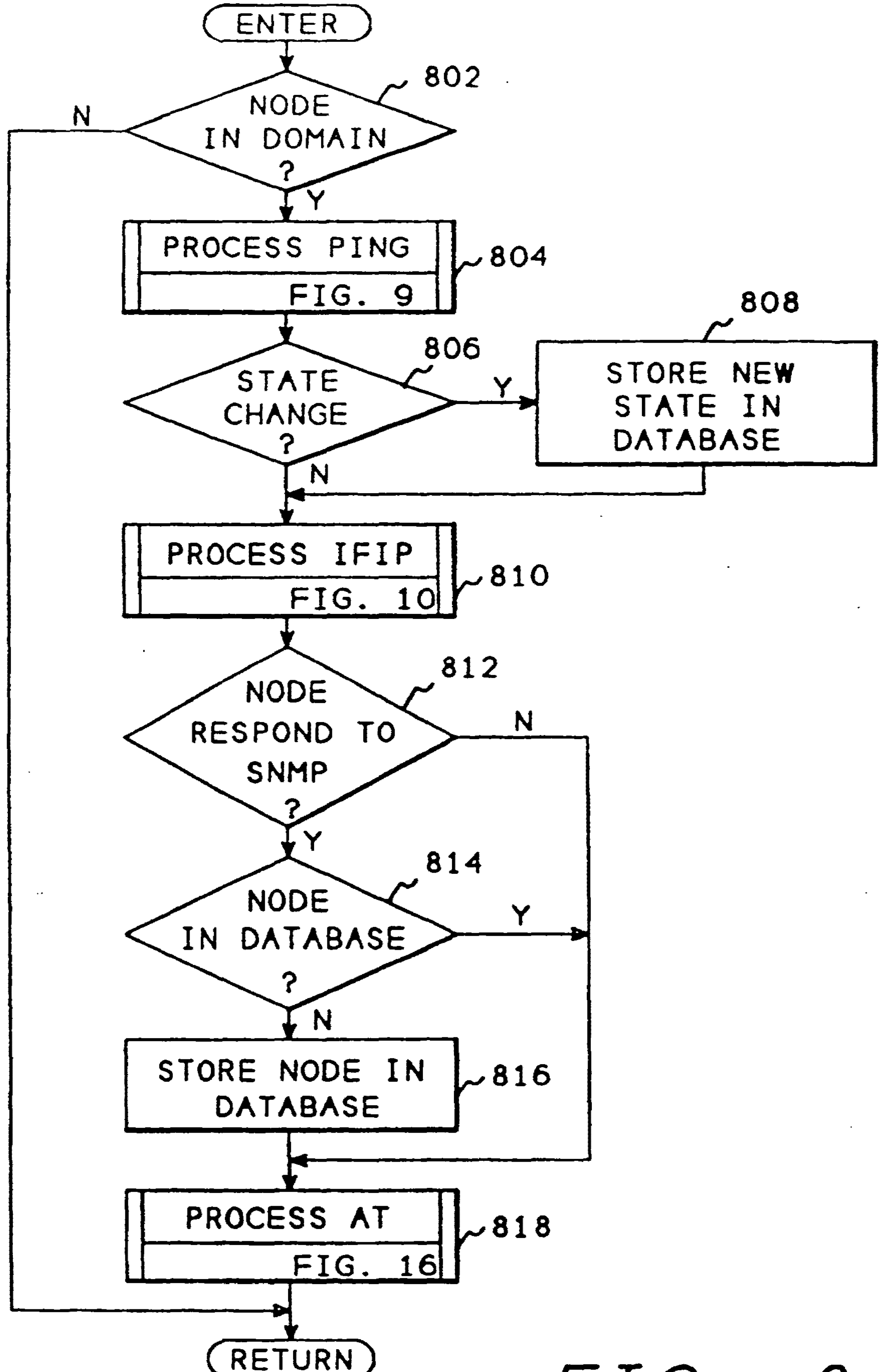

ENTER
802
NODE IN DOMAIN ?
N
Y
PROCESS PING
FIG. 9
804
806
STATE CHANGE ?
Y
808
STORE NEW STATE IN DATABASE
N
PROCESS IFIP
FIG. 10
810
812
NODE RESPOND TO SNMP ?
N
Y
814
NODE IN DATABASE ?
Y
N
STORE NODE IN DATABASE
816
PROCESS AT
FIG. 16
818
RETURN

FIG. 8

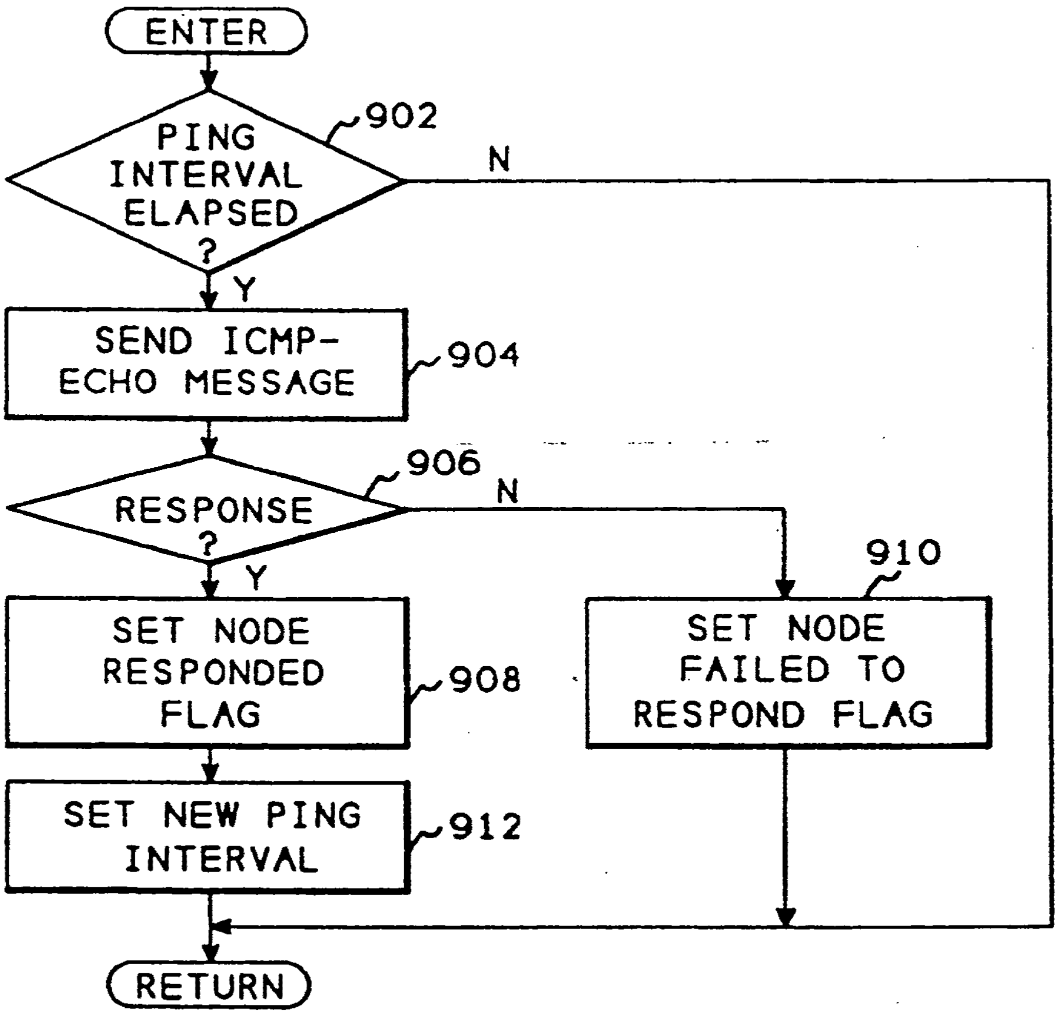

ENTER
PING INTERVAL ELAPSED ?
902
N
Y
SEND ICMP-ECHO MESSAGE
904
RESPONSE ?
906
N
Y
SET NODE RESPONDED FLAG
908
SET NODE FAILED TO RESPOND FLAG
910
SET NEW PING INTERVAL
912
RETURN

FIG. 9

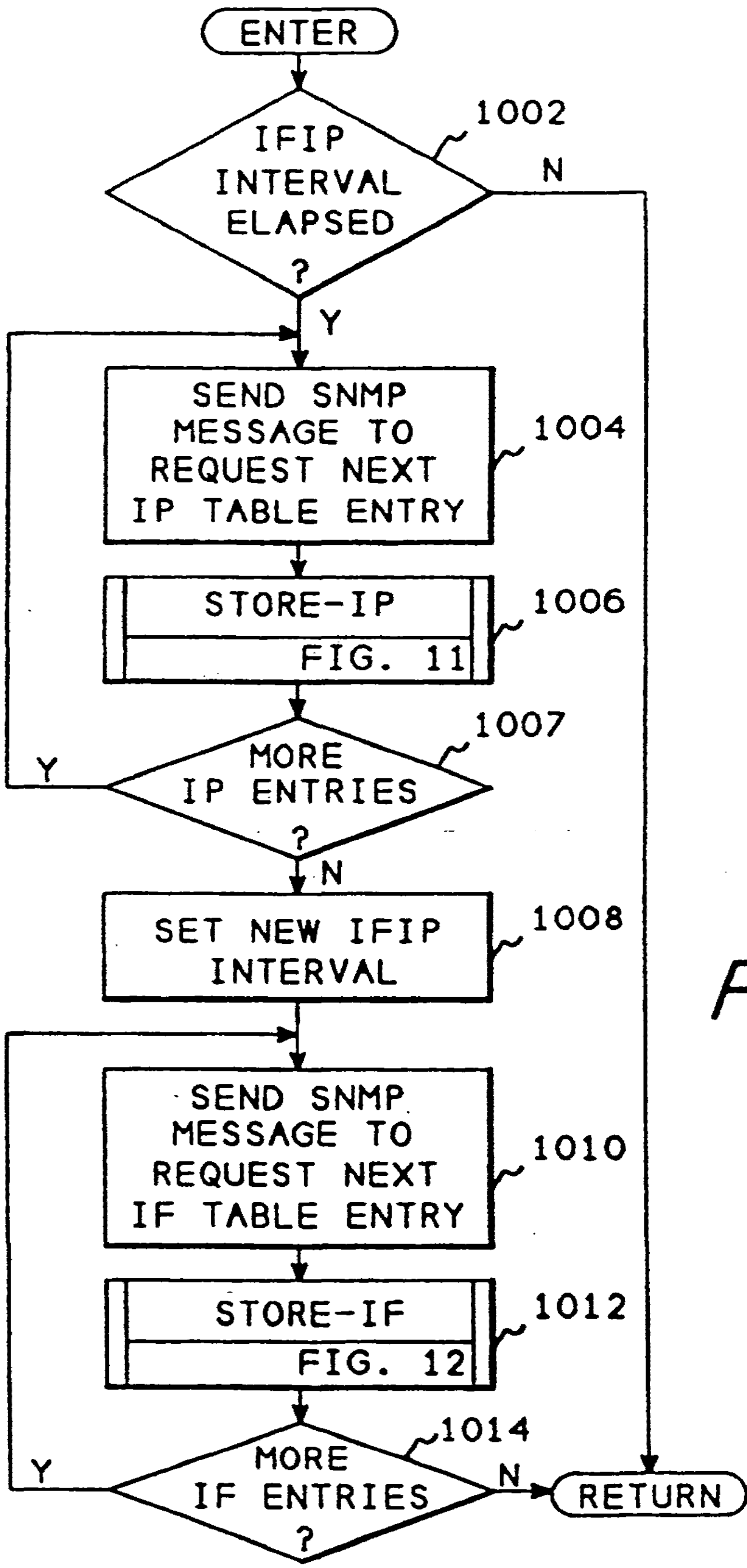

ENTER
1002
IFIP INTERVAL ELAPSED ?
N
Y
SEND SNMP MESSAGE TO REQUEST NEXT IP TABLE ENTRY
1004
STORE-IP
FIG. 11
1006
1007
MORE IP ENTRIES ?
Y
N
SET NEW IFIP INTERVAL
1008
SEND SNMP MESSAGE TO REQUEST NEXT IF TABLE ENTRY
1010
STORE-IF
FIG. 12
1012
1014
MORE IF ENTRIES ?
Y
N
RETURN

FIG. 10

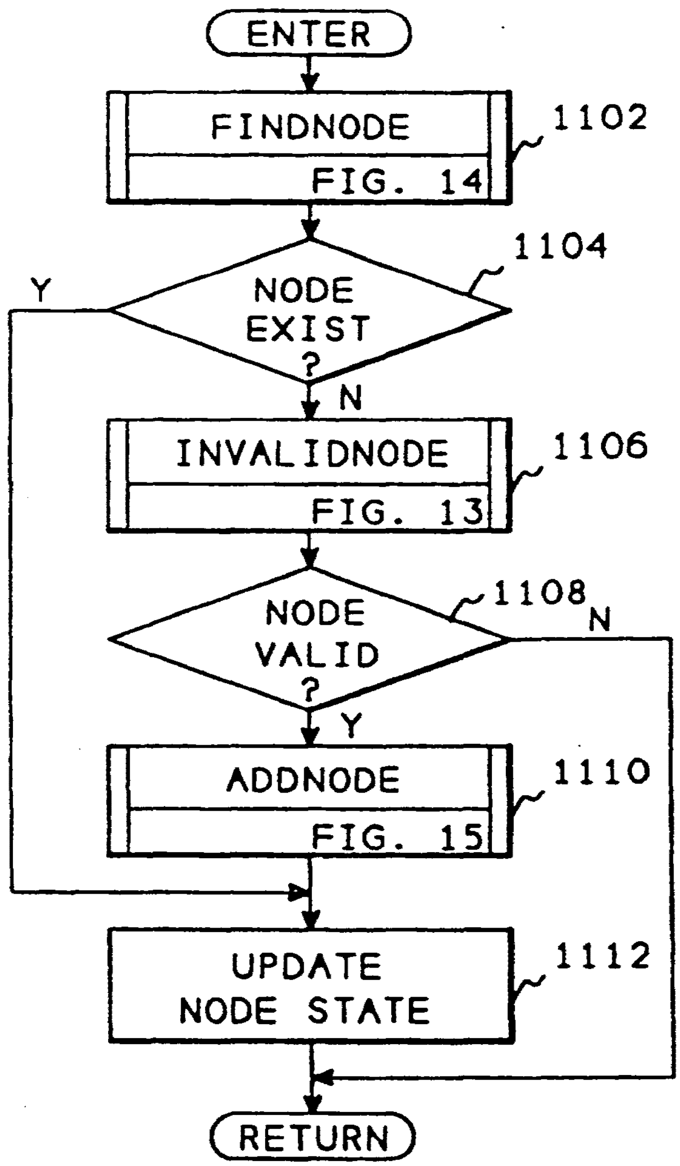

ENTER
FINDNODE
FIG. 14
1102
NODE EXIST ?
1104
Y
N
INVALIDNODE
FIG. 13
1106
NODE VALID ?
1108
N
Y
ADDNODE
FIG. 15
1110
UPDATE NODE STATE
1112
RETURN

FIG. 11

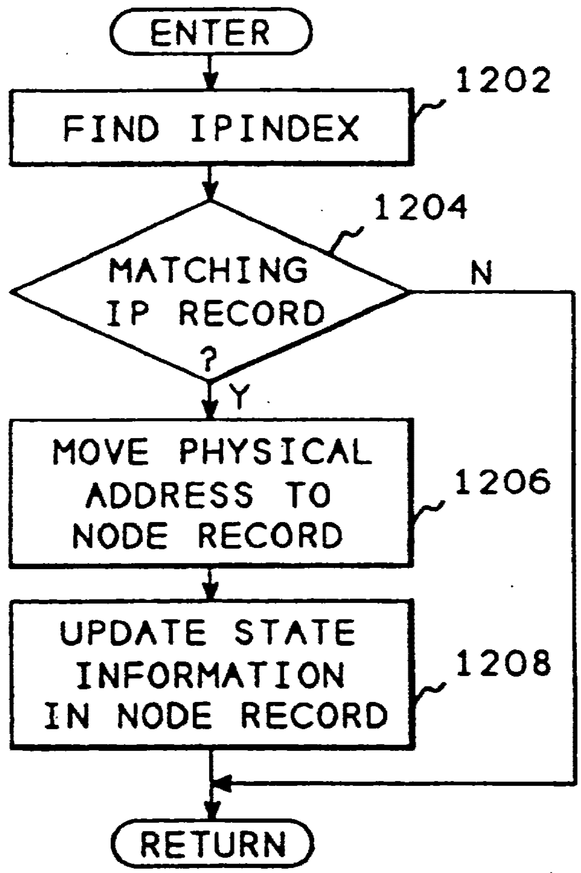

ENTER
FIND IPINDEX
1202
MATCHING IP RECORD ?
1204
N
Y
MOVE PHYSICAL ADDRESS TO NODE RECORD
1206
UPDATE STATE INFORMATION IN NODE RECORD
1208
RETURN

FIG. 12

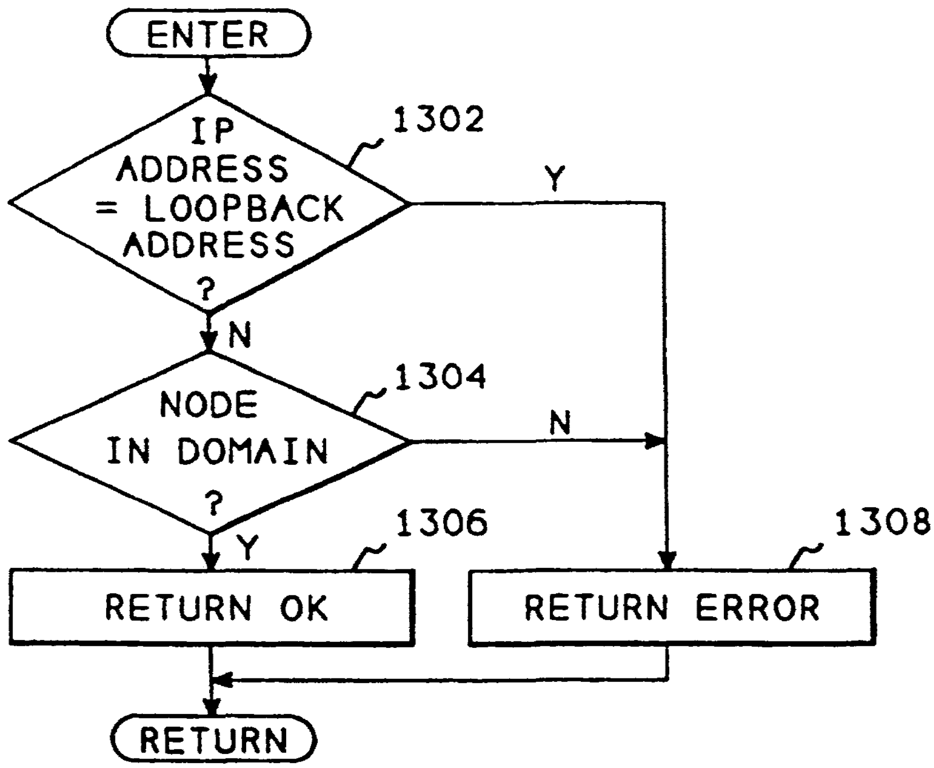
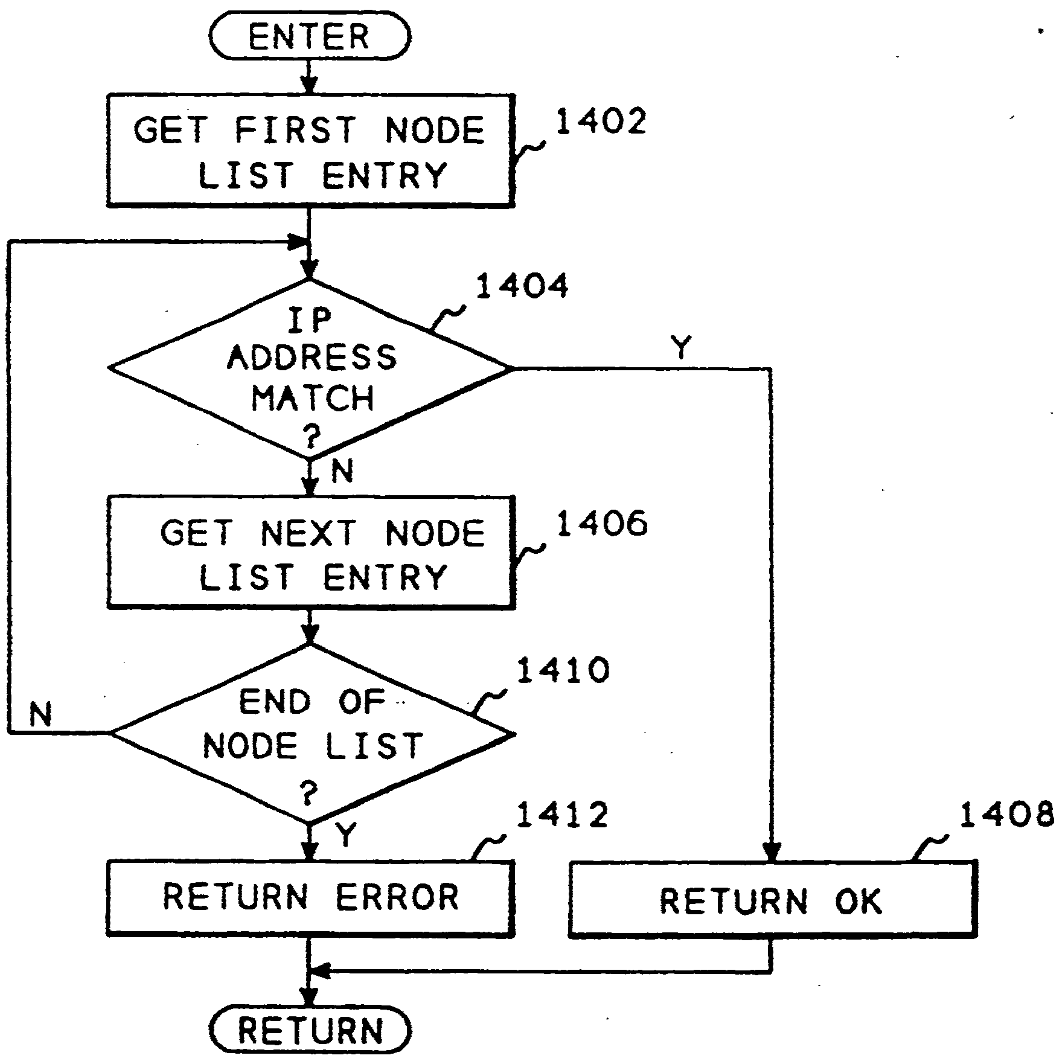

ENTER
IP ADDRESS = LOOPBACK ADDRESS ?
1302
Y
N
NODE IN DOMAIN ?
1304
N
Y
1306
1308
RETURN OK
RETURN ERROR
RETURN

FIG. 13



ENTER
GET FIRST NODE LIST ENTRY
1402
IP ADDRESS MATCH ?
1404
Y
N
GET NEXT NODE LIST ENTRY
1406
END OF NODE LIST ?
1410
N
Y
1412
1408
RETURN ERROR
RETURN OK
RETURN

FIG. 14

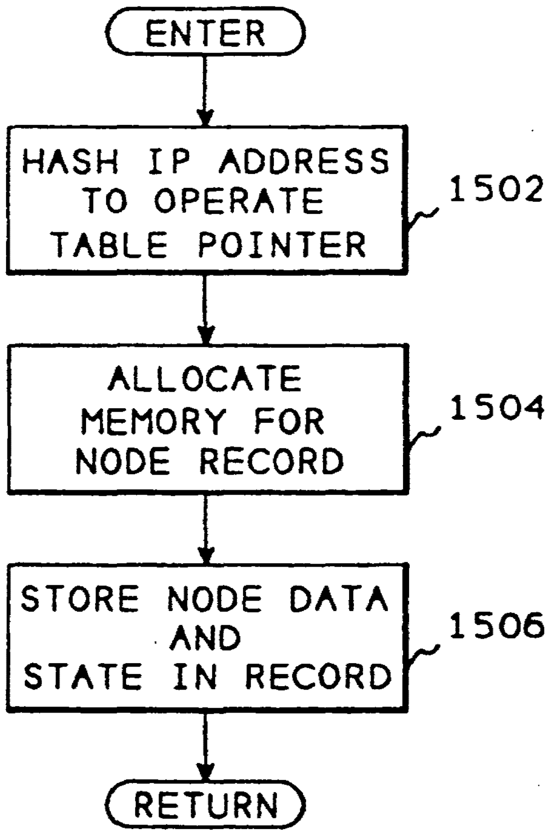

ENTER
HASH IP ADDRESS TO OPERATE TABLE POINTER
1502
ALLOCATE MEMORY FOR NODE RECORD
1504
STORE NODE DATA AND STATE IN RECORD
1506
RETURN

FIG. 15

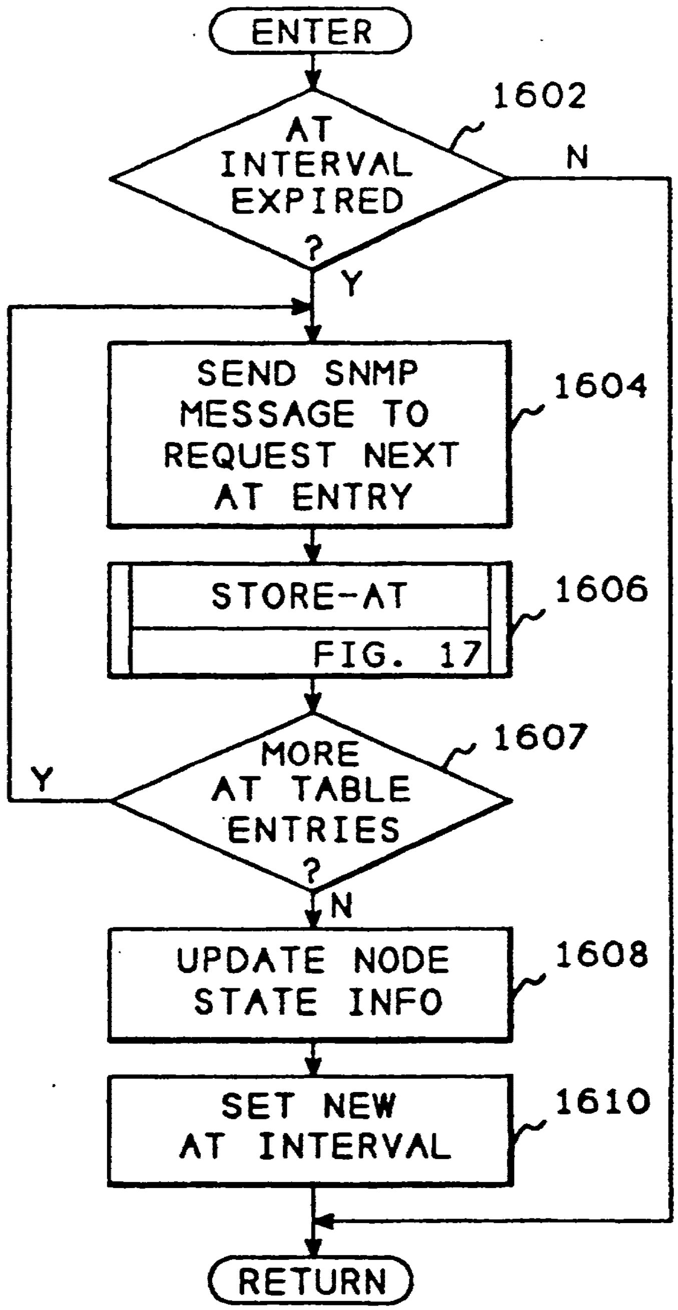

ENTER
1602
AT INTERVAL EXPIRED ?
N
Y
SEND SNMP MESSAGE TO REQUEST NEXT AT ENTRY
1604
STORE-AT
FIG. 17
1606
MORE AT TABLE ENTRIES ?
1607
Y
N
UPDATE NODE STATE INFO
1608
SET NEW AT INTERVAL
1610
RETURN

FIG. 16

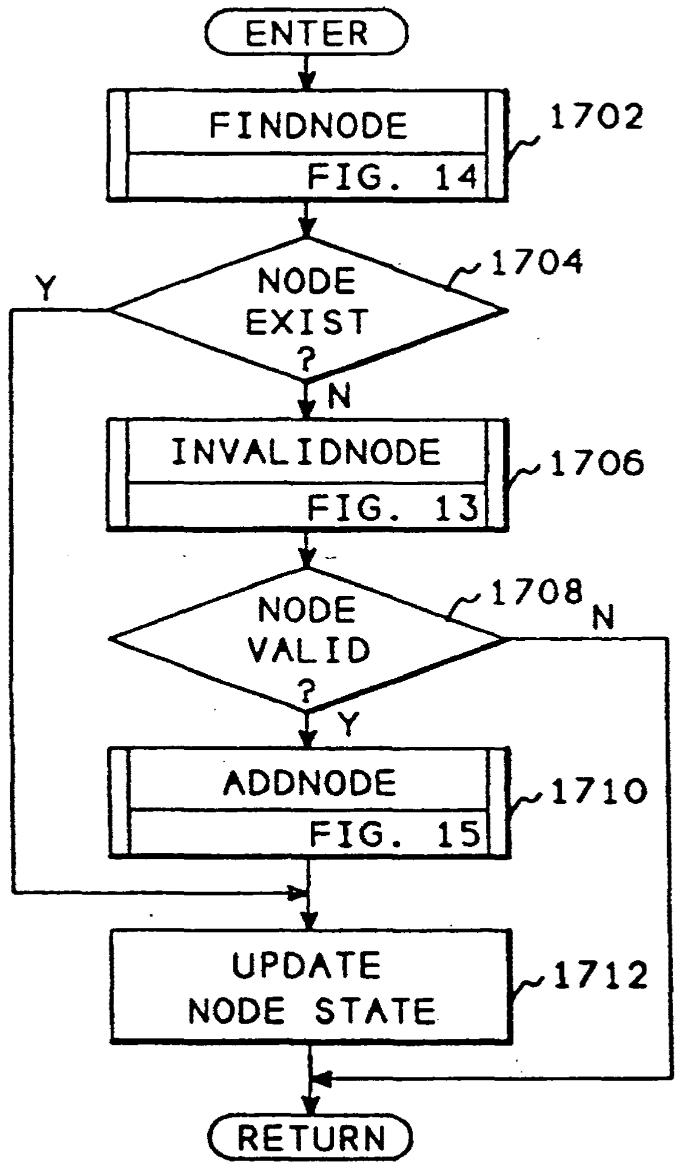

ENTER
FINDNODE
FIG. 14
1702
NODE EXIST ?
1704
Y
N
INVALIDNODE
FIG. 13
1706
NODE VALID ?
1708
N
Y
ADDNODE
FIG. 15
1710
UPDATE NODE STATE
1712
RETURN

FIG. 17

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 455 402 A3**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number : **91303643.0**

(22) Date of filing : **23.04.91**

(51) Int. Cl.^{5} : **H04L 12/24**

(30) Priority : **03.05.90 US 519187**

(43) Date of publication of application :
06.11.91 Bulletin 91/45

(84) Designated Contracting States :
DE FR GB

(88) Date of deferred publication of search report :
11.01.95 Bulletin 95/02

(71) Applicant : **Hewlett-Packard Company**
Mail Stop 20 B-O,
3000 Hanover Street
Palo Alto, California 94304 (US)

(72) Inventor : **Wu, Jeff C.**
2630 Wapiti Road
Fort Collins, Colorado 80525 (US)

(74) Representative : **Colgan, Stephen James et al**
CARPMAELS & RANSFORD
43 Bloomsbury Square
London WC1A 2RA (GB)

(54) **Automatic discovery of network elements.**

(57) Disclosed is a computer network node discovery system (120) that provides a general way of discovering network elements, or nodes (100), connected to a computer network (118), and a specific algorithm for discovering nodes connected to a TCP/IP network, using the SNMP protocol available within the TCP/IP network software. Some nodes on a network, called discovery agents, can convey knowledge of the existence of other nodes on the network. The network discovery system queries these agents and obtains the information they have about other nodes on the network. It then queries each of the nodes obtained to determine if that node is also a discovery agent. In this manner, most of the nodes on a network can be discovered. The process of querying discovery agents to obtain a list of nodes known to the discovery agents is repeated at timed intervals to obtain information about nodes that are not always active. In a TCP/IP network, discovery agents are nodes that respond to queries for an address translation table which translates internet protocol (IP) addresses to physical addresses. The data from each node's address translation table is used to obtain both the IP and the physical address of other nodes on the network. These nodes are then queried to obtain additional information. After all the nodes on a network are discovered, the list of nodes is written to a database where it can be displayed by the network manager or other users of the network.

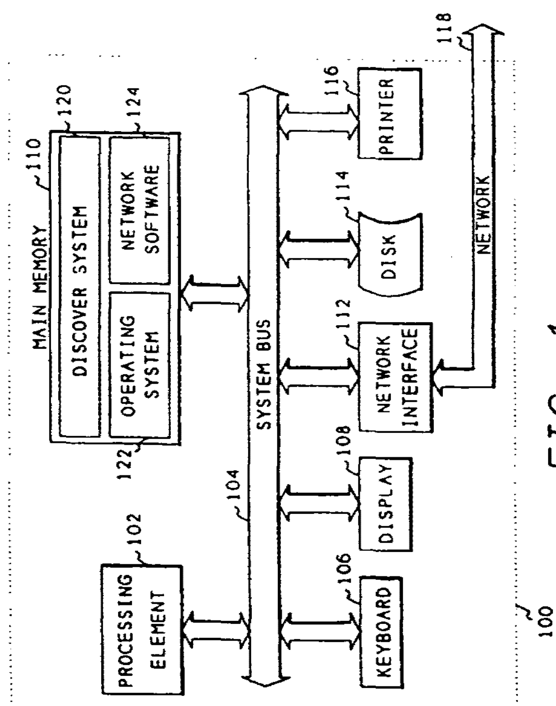


FIG. 1

EP 0 455 402 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 91 30 3643

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
Y	GB-A-2 217 488 (RACAL DATA COMMUNICATIONS INC.) * page 10, line 14 - page 14, line 2 * * page 15, line 18 - page 22, line 13 * * abstract * ---	1,7,9	H04L12/24
Y	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION., vol.7, no.7, September 1989, NEW YORK US pages 1104 - 1114, XP54539 L.N.CASSEL ET AL 'NETWORK MANAGEMENT ARCHITECTURES AND PROTOCOLS: PROBLEMS AND APPROACHES' * paragraph V * -----	1,7,9	
			TECHNICAL FIELDS SEARCHED (Int.Cl.5)
			H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	31 October 1994	Canosa Areste, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04J 3/14, 3/24, H04L 12/56	A1	(11) International Publication Number: WO 92/19054 (43) International Publication Date: 29 October 1992 (29.10.92)

(21) International Application Number: PCT/US92/02995

(22) International Filing Date: 10 April 1992 (10.04.92)

(30) Priority data:
684,695 12 April 1991 (12.04.91) US

(71) Applicant: CONCORD COMMUNICATIONS, INC. [US/US]; 753 Forest Street, Marlboro, MA 01752 (US).

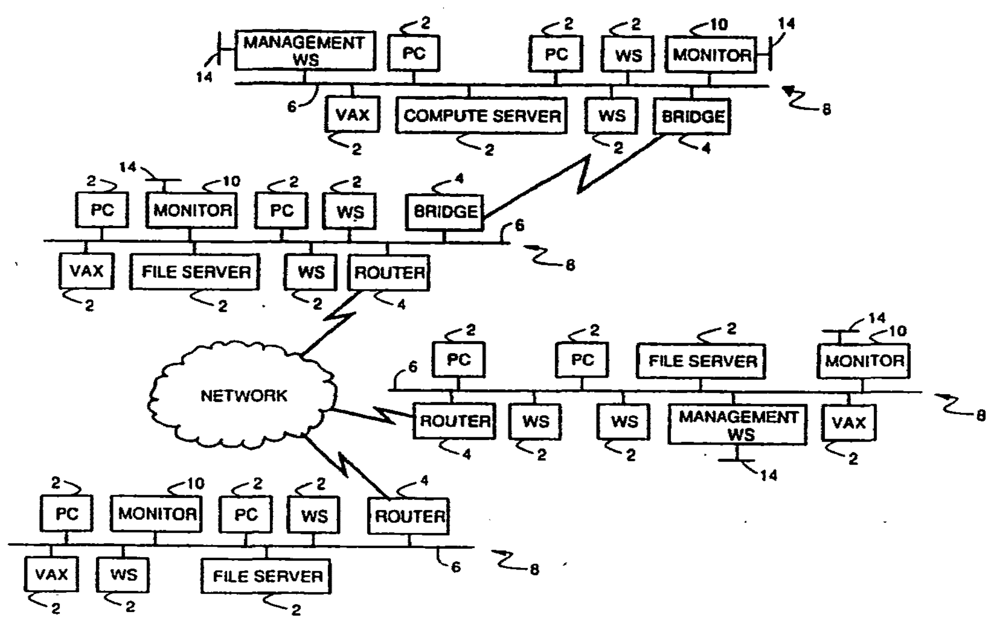
(72) Inventors: FERDINAND, Engel ; 21 Joseph Road, Northborough, MA 01532 (US). JONES, Kendall, S. ; 90 Boulder Road, Newton Center, MA 02159 (US). ROBERTSON, Kary ; 398 North Road, Bedford, MA 01739 (US). THOMPSON, David, M. ; 5127 243rd Road, Redmond, WA 98053 (US). WHITE, Gerard ; 133 Massapoag Road, Tyngsborough, MA 01879 (US).

(74) Agent: PRAHL, Eric, L.; Fish & Richardson, 225 Franklin Street, Boston, MA 02110-2804 (US).

(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), MC (European patent), NL (European patent), SE (European patent).

Published
With international search report.

(54) Title: NETWORK MONITORING



(57) Abstract

Monitoring is done of communications which occur in a network of nodes (2), each communication being effected by a transmission of one or more packets among two or more communicating nodes (2), each communication complying with a predefined communication protocol selected from among protocols available in the network. The contents of packets are detected passively and in real time, communication information (130, 152, 178) associated with multiple protocols is derived from the packet contents.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CS	Czechoslovakia
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GN	Guinea
GR	Greece
HU	Hungary
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
PL	Poland
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

NETWORK MONITORING

Background of the Invention

The invention relates to monitoring and managing communication networks for computers.

Todays computer networks are large complex systems with many components from a large variety of vendors. These networks often span large geographic areas ranging from a campus-like setting to world wide networks. While the network itself can be used by many different types of organizations, the purpose of these networks is to move information between computers. Typical applications are electronic mail, transaction processing, remote database, query, and simple file transfer. Usually, the organization that has installed and is running the network needs the network to be running properly in order to operate its business. Since these networks are complex systems, there are various controls provided by the different equipment to control and manage the network. Network management is the task of planning, engineering, securing and operating a network.

To manage the network properly, the Network Manager has some obvious needs. First, the Network Manager must trouble shoot problems. As the errors develop in a running network, the Network Manager must have some tools that notify him of the errors and allow him to diagnose and repair these errors. Second, the Network Manager needs to configure the network in such a manner that the network loading characteristics provide the best service possible for the network users. To do this the Network Manager must have tools that allow him visibility into access patterns, bottlenecks and general loading. With such data, the Network Manager can reconfigure the network components for better service.

There are many different components that need to be managed in the network. These elements can be, but are not limited to: routers, bridges, PC's, workstations, minicomputers, supercomputers, printers, file servers, switches and pbx's. Each component provides a protocol for reading and writing the management variables in the machine. These variables are usually defined by the component vendor and are usually referred to as a Management Information Base (MIB). There are some standard MIB's, such as the IETF (Internet Engineering Task Force) MIB I and MIB II standard definitions. Through the reading and writing of MIB variables, software in other computers can manage or control the component. The software in the component that provides remote access to the MIB variables is usually called an agent. Thus, an individual charged with the responsibility of managing a large network often will use various tools to manipulate the MIB's of various agents on the network.

Unfortunately, the standards for accessing MIBs are not yet uniformly provided nor are the MIB definitions complete enough to manage an entire network. The Network Manager must therefore use several different types of computers to access the agents in the network. This poses a problem, since the errors occurring on the network will tend to show up in different computers and the Network Manager must therefore monitor several different screens to determine if the network is running properly. Even when the Network Manager is able to accomplish this task, the tools available are not sufficient for the Network Manager to function properly.

Furthermore, there are many errors and loadings on the network that are not reported by agents. Flow control problems, retransmissions, on-off segment loading, network capacities and utilizations are some of the types of data that are not provided by the agents.

Simple needs like charging each user for actual network usage are impossible.

Summary of the Invention

In general, in one aspect, the invention features monitoring communications which occur in a network of nodes, each communication being effected by a transmission of one or more packets among two or more communicating nodes, each communication complying with a predefined communication protocol selected from among protocols available in the network. The contents of packets are detected passively and in real time, communication information associated with multiple protocols is derived from the packet contents.

Preferred embodiments of the invention include the following features. The communication information derived from the packet contents is associated with multiple layers of at least one of the protocols.

In general, in another aspect, the invention features monitoring communication dialogs which occur in a network of nodes, each dialog being effected by a transmission of one or more packets among two or more communicating nodes, each dialog complying with a predefined communication protocol selected from among protocols available in the network. Information about the states of dialogs occurring in the network and which comply with different selected protocols available in the network is derived from the packet contents.

Preferred embodiments of the invention include the following features. A current state is maintained for each dialog, and the current state is updated in response to the detected contents of transmitted packets. For each dialog, a history of events is maintained based on information derived from the contents of packets, and the history of events is analyzed to derive information about the dialog. The analysis of the history includes counting events and gathering statistics about events. The history is monitored for dialogs which are inactive, and dialogs which have been inactive for a predetermined period of time are purged. For example, the current state is updated to data state in response to observing the transmission of at least two data related packets from each node. Sequence numbers of data related packets stored in the history of events are analyzed and retransmissions are detected based on the sequence numbers. The the current state is updated based on each new packet associated with the dialog; if an updated current state cannot be determined, information about prior packets associated with the dialog is consulted as an aid in updating the state. The history of events may be searched to identify the initiator of a dialog.

The full set of packets associated with a dialog up to a point in time completely define a true state of the dialog at that point in time, and the step of updating the current state in response to the detected contents of transmitted packets includes generating a current state (e.g., "unknown") which may not conform to the true state. The current state may be updated to the true state based on information about prior packets transmitted in the dialog.

Each communication may involve multiple dialogs corresponding to a specific protocol. Each protocol layer of the communication may be parsed and analyzed to isolate each dialog and statistics may be kept for each dialog. The protocols may include a connectionless-type protocol in which the state of a dialog is implicit in transmitted packets, and the step of deriving information about the states of dialogs includes inferring the states of the dialogs from the packets. Keeping statistics for protocol layers may be temporarily suspended when parsing and statistics gathering is not rapid enough to match the rate of packets to be parsed.

In general, in another aspect, the invention features monitoring the operation of the network with respect to specific items of performance during normal operation, generating a model of the network based on the monitoring, and setting acceptable threshold levels for the specific items of performance based on the model. In preferred embodiments, the operation of the network is monitored with respect to the specific items of performance during periods which may include abnormal operation.

In general, in another aspect, the invention features the combination of a monitor connected to the network medium for passively, and in real time, monitoring transmitted packets and storing information about dialogs associated with the packets, and a workstation for receiving the information about dialogs from the monitor and providing an interface to a user. In preferred embodiments, the workstation includes means for enabling a user to observe events of active dialogs.

In general, in another aspect, the invention features apparatus for monitoring packet communications in a network of nodes in which communications may be in accordance with multiple protocols. The apparatus includes a monitor connected to a communication medium of the network for passively, and in real time, monitoring transmitted packets of different protocols and storing information about communications associated with the packets, the communications being in accordance with different protocols, and a workstation for receiving the information about the communciations from the monitor and providing an interface to a user. The monitor and the workstation include means for relaying the information about multiple protocols with respect to communication in the different protocols from the monitor to the workstation in accordance with a single common network management protocol.

In general, in another aspect, the invention features diagnosing communication problems between two nodes in a network of nodes interconnected by links. The operation of the network is monitored with respect to specific items of performance during normal operation. A model of normal operation of the network is generated based on the monitoring. Acceptable threshold levels are set for the specific items of performance based on the model. The operation of the network is monitored with respect to the specific items of performance during periods which may include abnormal operation. When abnormal operation of the network with respect to communication between the two nodes is detected, the problem is diagnosed by separately analyzing the performance of each of the nodes and each of the links connecting the two nodes to isolate the abnormal operation.

In general, in another aspect, the invention features a method of timing the duration of a transaction of interest occurring in the course of communication between nodes of a network, the beginning of the transaction being defined by the sending of a first packet of a particular kind from one node to the other, and the end of the transaction being defined by the sending of another packet of a particular kind between the nodes. In the method, packets transmitted in the network are monitored passively and in real time. The beginning time of the transaction is determined based on the appearance of the first packet. A determination is made of when the other packet has been transmitted. The timing of the duration of the transaction is ended upon the appearance of the other packet.

In general, in another aspect, the invention features, tracking node address to node name mappings in a network of nodes of the kind in which each node has a possibly nonunique node name and a unique node address within the network and in which node addresses can be assigned and reassigned to node names dynamically using a name binding protocol message incorporated within a packet. In the method, packets transmitted in the network are monitored, and a table linking node names to node addresses is updated based on information contained in the name binding protocol messages in the packets.

One advantage of the invention is that it enables a network manager to passively monitor multi-protocol networks at multiple layers of the communications. In addition, it organizes and presents network performance statistics in terms of dialogs which are occurring at any desired level of the communication. This technique of organizing and displaying network performance statistics provides an effective and useful view of network performance and facilitates a quick diagnosis of network problems.

Other advantages and features will become apparent from the following description of the preferred embodiment and from the claims.

Description of the Preferred Embodiments

Fig. 1 is a block diagram of a network;

Fig. 2 shows the layered structure of a network communication and a protocol tree within that layered environment;

Fig. 3 illustrates the structure of an ethernet/IP/TCP packet;

Fig. 4 illustrates the different layers of a communication between two nodes;

Fig. 5 shows the software modules within the Monitor;

Fig. 6 shows the structure of the Monitor software in terms of tasks and intertask communication mechanisms;

Figs. 7a-c show the STATS data structures which store performance statistics relating to the the data link layer;

Fig. 8 is a event/state table describing the operation of the state machine for a TCP connection;

Fig. 9a is a history data structure that is identified by a pointer found in the appropriate dialog statistics data within STATS;

Fig. 9b is a record from the history table;

Fig. 10 is a flow diagram of the Look_for_Data_State routine;

Fig. 11 is a flow diagram of the Look_for_Initiator routine that is called by the Look_for_Data_State routine;

Fig. 12 is a flow diagram of the Look_for_Retransmission routine which is called by the Look_at_History routine;

Fig. 13 is a diagram of the major steps in processing a frame through the Real Time Parser (RTP);

Fig. 14 is a diagram of the major steps in the processing a statistics threshold event;

Fig. 15 is a diagram of the major steps in the processing of a database update;

Fig. 16 is a diagram of the major steps in the processing of a monitor control request;

Fig. 17 is a logical map of the network as displayed by the Management Workstation;

Fig. 18 is a basic summary tool display screen;

Fig. 19 is a protocol selection menu that may be invoked through the summary tool display screen;

Figs. 20a-g are examples of the statistical variables which are displayed for different protocols;

Fig. 21 is an example of information that is displayed in the dialogs panel of the summary tool display screen;

Fig. 22 is a basic data screen presenting a rate values panel, a count values panel and a protocols seen panel;

Fig. 23 is a traffic matrix screen;

Fig. 24 is a flow diagram of the algorithm for adaptively establishing network thresholds based upon actual network performance;

Fig. 25 is a simple multi-segment network;

Fig. 26 is a flow diagram of the operation of the diagnostic analyzer algorithm;

Fig. 27 is a flow diagram of the source node analyzer algorithm;

Fig. 28 is a flow diagram of the sink node analyzer algorithm;

Fig. 29 is a flow diagram of the link analysis logic;

Fig. 30 is a flow diagram of the DLL problem checking routine;

Fig. 31 is a flow diagram of the IP problem checking routine;

Fig. 32 is a flow diagram of the IP link component problem checking routine;

Fig. 33 is a flow diagram of the DLL link component problem checking routine;

Fig. 34 shows the structure of the event timing database;

Fig. 35 is a flow diagram of the operation of the event timing module (ETM) in the Network Monitor;

Fig. 36 is a network which includes an Appletalk® segment;

Fig. 37 is a Name Table that is maintained by the Address Tracking Module (ATM);

Fig. 38 is a flow diagram of the operation of the ATM; and

Fig. 39 is a flow diagram of the operation of the ATM.

Also attached hereto before the claims are the following appendices:

Appendix I identifies the SNMP MIB subset that is supported by the Monitor and the Management Workstation (2 pages);

Appendix II defines the extension to the standard MIB that are supported by the Monitor and the Management Workstation (25 pages);

Appendix III is a summary of the protocol variables for which the Monitor gathers statistics and a brief description of the variables, where appropriate (17 pages);

Appendix IV is a list of the Summary Tool Values Display Fields with brief descriptions (2 pages); and

Appendix V is a description of the actual screens for the Values Tool (34 pages).

Structure and Operation

The Network:

A typical network, such as the one shown in Fig. 1, includes at least three major components, namely, network nodes 2, network elements 4 and communication lines 6. Network nodes 2 are the individual computers on the network. They are the very reason the network exists. They include but are not limited to workstations (WS), personal computers (PC), file servers (FS), compute servers (CS) and host computers (e.g., a VAX), to name but a few. The term server is often used as though it was different from a node, but it is, in fact, just a node providing special services.

In general, network elements 4 are anything that participate in the service of providing data movement in a network, i.e., providing the basic communications. They include, but are not limited to, LAN's, routers, bridges, gateways, multiplexors, switches and connectors. Bridges serve as connections between different network segments. They keep track of the nodes which are connected to each of the segments to which they are connected. When they see a packet on one segment that is addressed to a node on another of their segments, they grab the packet from the one segment and transfer it to the proper segment. Gateways generally provide connections between different network segments that are operating under different protocols and serve to convert communications from one protocol to the other. Nodes send packets to routers so that they may be directed over the appropriate segments to the intended destination node.

Finally, network or communication lines 6 are the components of the network which connect nodes 2 and elements 4 together so that communicatons between nodes 2 may take place. They can be private lines, satellite lines or Public Carrier lines. They are expensive resources and are usually managed as separate entities. Often networks are organized into segments 8 that are connected by network elements 4. A segment 8 is a section of a LAN connected at a physical level (this may include repeaters). Within a segment, no protocols at layers above the physical layer are needed to enable signals from two stations on the same segment to reach each other (i.e., there are no routers, bridges, gateways...).

<u>The Network Monitor and the Management Workstation</u>:

In the described embodiment, there are two basic elements to the monitoring system which is to be described, namely, a Network Monitor 10 and a Management

Workstation 12. Both elements interact with each other over the local area network (LAN).

Network Monitor 10 (referred to hereinafter simply as Monitor 10) is the data collection module which is attached to the LAN. It is a high performance real time front end processor which collects packets on the network and performs some degree of analysis to search for actual or potential problems and to maintain statistical information for use in later analysis. In general, it performs the following functions. It operates in a promiscuous mode to capture and analyze all packets on the segment and it extracts all items of interest from the frames. It generates alarms to notify the Management Workstation of the occurence of significant events. It receives commands from the Management Workstation, processes them appropriately and returns responses.

Management Workstation 12 is the operator interface. It collects and presents troubleshooting and performance information to the user. It is based on the SunNet Manager (SNM) product and provides a graphical network-map-based interface and sophisticated data presentation and analysis tools. It receives information from Monitor 10, stores it and displays the information in various ways. It also instructs Monitor 10 to perform certain actions. Monitor 10, in turn, sends responses and alarms to Management Workstation 12 over either the primary LAN or a backup serial link 14 using SNMP with the MIB extensions defined later.

These devices can be connected to each other over various types of networks and are not limited to connections over a local area network. As indicated in Fig. 1, there can be multiple Workstations 12 as well as multiple Monitors 10.

Before describing these components in greater detail, background information will first be reviewed regarding communication protocols which specify how communications are conducted over the network and regarding the structure of the packets.

The Protocol Tree:

As shown in Fig. 2, communication over the network is organized as a series of layers or levels, each one built upon the next lower one, and each one specified by one or more protocols (represented by the boxes). Each layer is responsible for handling a different phase of the communication between nodes on the network. The protocols for each layer are defined so that the services offered by any layer are relatively independent of the services offered by the neighbors above and below. Although the identities and number of layers may differ depending on the network (i.e., the protocol set defining communication over the network), in general, most of them share a similar structure and have features in common.

For purposes of the present description, the Open Systems Interconnection (OSI) model will be presented as representative of structured protocol architectures. The OSI model, developed by the International Organization for Standardization, includes seven layers. As indicated in Fig. 2, there is a physical layer, a data link layer (DLL), a network layer, a transport layer, a session layer, a presentation layer and an application layer, in that order. As background for what is to follow, the function of each of these layers will be briefly described.

The physical layer provides the physical medium for the data transmission. It specifies the electrical and mechanical interfaces of the network and deals with bit level detail. The data link layer is responsible for ensuring an error-free physical link between the communicating nodes. It is responsible for creating and recognizing frame boundaries (i.e., the boundaries of the packets of data that are sent over the network.) The network layer determines how packets are routed within the network. The transport layer accepts data from the layer above it (i.e., the session layer), breaks the packets up into smaller units, if required, and passes these to the network layer for transmission over the network. It may insure that the smaller pieces all arrive properly at the other end. The session layer is the user's interface into the network. The user must interface with the session layer in order to negotiate a connection with a process in another machine. The presentation layer provides code conversion and data reformatting for the user's application. Finally, the application layer selects the overall network service for the user's application.

Fig. 2 also shows the protocol tree which is implemented by the described embodiment. A protocol tree shows the protocols that apply to each layer and it identifies by the tree structure which protocols at each layer can run "on top of" the protocols of the next lower layer. Though standard abbreviations are used to identify the protocols, for the convenience of the reader, the meaning of the abbreviations are as follows:

ARP	Address Resolution Protocol
ETHERNET	Ethernet Data Link Control
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LLC	802.2 Logical Link Control
MAC	802.3 CSMA/CD Media Access Control
NFS	Network File System
NSP	Name Server Protocol
RARP	Reverse Address Resolution Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol

Two terms are commonly used to describe the protocol tree, namely, a protocol stack and a protocol family (or suite). A protocol stack generally refers to the underlying protocols that are used when sending a message over a network. For example, FTP/TCP/IP/LLC is a protocol stack. A protocol family is a loose association of protocols which tend to be used on the same network (or derive from a common source). Thus, for example, the TCP/IP family includes IP, TCP, UDP, ARP, TELNET and FTP. The Decnet family includes the protocols from Digital Equipment Corporation. And the SNA family includes the protocols from IBM.

The Packet:

The relevant protocol stack defines the structure of each packet that is sent over the network. Fig. 3, which shows an TCP/IP packet, illustrates the typical structure of a packet. In general, each level of the protocol stack takes the data from the next higher level and adds header information to form a protocol data unit (PDU) which it passes to the next lower level. That is, as the data from the application is passed down through the protocol layers in preparation for transmission over the network, each layer adds its own information to the data passed down from above until the complete packet is assembled. Thus, the structure of a packet ressembles that of an onion, with each PDU of a given layer wrapped within the PDU of the adjacent lower level.

At the ethernet level, the PDU includes a destination address (DEST MAC ADDR), a source address (SRC MAC ADDR), a type (TYPE) identifying the protocol which is running on top of this layer, and a DATA field for the PDU from the IP layer.

Like the ethernet packet, the PDU for the IP layer includes an IP header plus a DATA field. The IP header includes a type field (TYPE) for indicating the type of service, a length field (LGTH) for specifying the total length of the PDU, an identification field (ID), a protocol field (PROT) for identifying the protocol which is running on top of the IP layer (in this case, TCP), a source address field (SRC ADDR) for specifying the IP address of the sender, a destination address field (DEST ADDR) for specifying the IP address of the destination node, and a DATA field.

The PDU built by the TCP protocol also consists of a header and the data passed down from the next higher layer. In this case the header includes a source port field (SRC PORT) for specifying the port number of the sender, a destination port field (DEST PORT) for specifying the port number of the destination, a sequence number field (SEQ NO.) for specifying the sequence number of the data that is being sent in this packet, and an acknowledgment number field (ACK NO.) for specifying the number of the acknowledgment being returned. It also includes bits which identify the packet type, namely, an acknowledgment bit (ACK), a reset connection bit (RST), a synchronize bit (SYN), and a no more data from sender bit (FIN). There is also a window size field (WINDOW) for specifying the size of the window being used.

<u>The Concept of a Dialog</u>:

The concept of a dialog is used throughout the following description. As will become apparent, it is a concept which provides a useful way of conceptualizing, organizing and displaying information about the performance of a network - for any protocol and for any layer of the multi-level protocol stack.

As noted above, the basic unit of information in communication is a packet. A packet conveys meaning between the sender and the receiver and is part of a larger framework of packet exchanges. The larger exchange is called a dialog within the context of this document. That is, a dialog is a communication between a sender and a receiver, which is composed of one or more packets being transmitted between the two. There can be multiple senders and receivers which can change roles. In fact, most dialogs involve exchanges in both directions.

Stated another way, a dialog is the exchange of messages and the associated meaning and state that is inherent in any particular exchange at any layer. It refers to the exchange between the peer entities (hardware or software) in any communication. In those situations where there is a layering of protocols, any particular message exchange could be viewed as belonging to multiple dialogs. For example, in Fig. 4 Nodes A and B are exchanging packets and are engaged in multiple dialogs. Layer 1 in Node A has a dialog with Layer 1 in Node B. For this example, one could state that this is the data link layer and the nature of the dialog deals with the message length, number of messages, errors and perhaps the guarantee of the delivery. Simultaneously, Layer n of Node A is having a dialog with Layer n of node B. For the sake of the example, one could state that this is an application layer dialog which deals with virtual terminal connections and response rates. One can also assume that all of the other layers (2 through n-1) are also having simultaneous dialogs.

In some protocols there are explicit primitives that deal with the dialog and they are generally referred to as connections or virtual circuits. However, dialogs exist even in stateless and connectionless protocols. Two more examples will be described to help clarify the concept further, one dealing with a connection oriented protocol and the other dealing with a connectionless protocol.

In a typical connection oriented protocol, Node A sends a connection request (CR) message to Node B. The CR is an explicit request to form a connection. This is the start of a particular dialog, which is no different from the start of the connection. Nodes A and B could have other dialogs active simultaneously with this particular dialog. Each dialog is seen as unique. A connection is a particular type of dialog.

In a typical connectionless protocol, Node A sends Node B a message that is a datagram which has no connection paradigm, in fact, neither do the protocol(s) at higher layers. The application protocol designates this as a request to initiate some action. For example, a file server protocol such as Sun Microsystems' Network File System (NFS) could make a mount request. A dialog comes into existence once the communication between Nodes A and B has begun. It is possible to determine that communication has occurred and to determine the actions being requested. If in fact there exists more than one communication thread between Nodes A and B, then these would represent separate, different dialogs.

Inside the Network Monitor:

Monitor 10 includes a MIPS R3000 general purpose microprocessor (from MIPS Computer Systems, Inc.) running at 25 MHz. It is capable of providing 20 mips processing power. Monitor 10 also includes a 64Kbyte instruction cache and a 64Kbyte data cache, implemented by SRAM.

The major software modules of Monitor 10 are implemented as a mixture of tasks and subroutine libraries as shown in Fig. 5. It is organized this way so as to minimise the context switching overhead incurred during critical processing sequences. There is NO PREEMPTION of any module in the monitor subsystem. Each module is cognizant of the fact that it should return control to the kernel in order to let other tasks run. Since the monitor subsystem is a closed environment, the software is aware of real time constraints.

Among the major modules which make up Monitor 10 is a real time kernel 20, a boot/load module 22, a driver 24, a test module 26, an SNMP Agent 28, a Timer module 30, a real time parser (RTP) 32, a Message Transport Module (MTM) 34, a statistics database (STATS) 36, an Event Manager (EM) 38, an Event Timing Module (ETM) 40 and a control module 42. Each of these will now be described in greater detail.

Real Time Kernel 20 takes care of the general housekeeping activities in Monitor 10. It is responsible for scheduling, handling intertask communications via queues, managing a potentially large number of timers, manipulating linked lists, and handling simple memory management.

Boot/Load Module 22, which is FProm based, enables Monitor 10 to start itself when the power is turned on in the box. It initializes functions such as diagnostics, and environmental initialization and it initiates down loading of the Network Monitor Software including program and configuration files from the Management Workstation. Boot/load module 22 is also responsible for reloading program and/or configuration data following internal error detection or on command from the Management Workstation. To accomplish down loading, boot/load module 22 uses the Trivial File Transfer Protocol (TFTP). The protocol stack used for loading is TFTP/UDP/IP/ethernet over the LAN and TFTP/UDP/IP/SLIP over the serial line.

Device Driver 24 manages the network controller hardware so that Monitor 10 is able to read and write packets from the network and it manages the serial interface. It does so both for the purposes of monitoring traffic (promiscuous mode) and for the purposes of communicating with the Management Workstation and other devices on the network. The communication occurs through the network controller hardware of the physical network (e.g. Ethernet). The drivers for the LAN controller and serial line interface are used by the boot load module and the MTM. They provide access to the chips and isolate higher layers from the hardware specifics.

Test module 26 performs and reports results of physical layer tests (TDR, connectivity,...) under control of the Management Workstation. It provides traffic load information in response to user requests identifying the particular traffic data of interest. The load information is reported either as a percent of available bandwidth or as frame size(s) plus rate.

SNMP Agent 28 translates requests and information into the network management protocol being used to communicate with the Management Workstation, e.g., the Simple Network Management Protocol (SNMP).

Control Module 42 coordinates access to monitor control variables and performs actions necessary when these are altered. Among the monitor control variables which it handles are the following:

set reset monitor - transfer control to reset logic;

set time of day - modify monitor hardware clock and generate response to Management Workstation;

get time of day - read monitor hardware clock and generate response to Workstation;

set trap permit - send trap control ITM to EM and generate response to Workstation;

get trap permit - generate response to Workstation;

Control module 42 also updates parse control records within STATS when invoked by the RTP (to be described) or during overload conditions so that higher layers of parsing are dropped until the overload situation is resolved. When overload is over it restores full parsing.

Timer 30 is invoked periodically to perform general housekeeping functions. It pulses the watchdog timer at appropriate intervals. It also takes care of internal time stamping and kicking off routines like the EM routine which periodically recalculates certain numbers within the statistical database (i.e., STATS).

Real Time Parser (RTP) 32 sees all frames on the network and it determines which protocols are being used and interprets the frames. The RTP includes a protocol parser and a state machine. The protocol parser parses a received frame in the "classical" manner, layer-by-layer, lowest layer first. The parsing is performed such that the statistical objects in STATS (i.e., the network parameters for which performance data is kept) are maintained. Which layers are to have statistics stored for them is determined by a parse control record that is stored in STATS (to be described later). As each layer is parsed, the RTP invokes the appropriate functions in the statistics module (STATS) to update those statistical objects which must be changed.

The state machine within RTP 32 is responsible for tracking state as appropriate to protocols and connections. It is responsible for maintaining and updating the connection oriented statistical elements in

STATS. In order to track connection states and events, the RTP invokes a routine within the state machine. This routine determines the state of a connection based on past observed frames and keeps track of sequence numbers. It is the routine that determines if a connection is in data transfer state and if a retransmission has occurred. The objectives of the state machine are to keep a brief history of events, state transitions, and sequence numbers per connection; to detect data transfer state so that sequence tracking can begin; and to count inconsistencies but still maintain tracking while falling into an appropriate state (e.g. unknown).

RTP 32 also performs overload control by determining the number of frames awaiting processing and invoking control module 42 to update the parse control records so as to reduce the parsing depth when the number becomes too large.

Statistics Module (STATS) 36 is where Monitor 10 keeps information about the statistical objects it is charged with monitoring. A statistical object represents a network parameter for which performance information is gathered. This information is contained in an extended MIB (Management Information Base), which is updated by RTP 32 and EM 38.

STATS updates statistical objects in response to RTP invocation. There are at least four statistical object classes, namely, counters, timers, percentages (%), and meters. Each statistical object is implemented as appropriate to the object class to which it belongs. That is, each statistical object behaves such that when invoked by RTP 32 it updates and then generates an alarm if its value meets a preset threshold. (Meets means that for a high threshold the value is equal to or greater than the threshold and for a low threshold the value is equal to or less than the threshold. Note that a single object may have both high and low thresholds.)

STATS 36 is responsible for the maintenance and initial analysis of the database. This includes coordinating access to the database variables, ensuring appropriate interlocks are applied and generating alarms when thresholds are crossed. Only STATS 36 is aware of the internal structure of the database, the rest of the system is not.

STATS 36 is also responsible for tracking events of interest in the form of various statistical reductions. Examples are counters, rate meters, and rate of change of rate meters. It initiates events based on particular statistics reaching configured limits, i.e., thresholds. The events are passed to the EM which sends a trap (i.e., an alarm) to the Management Workstation. The statistics within STATS 36 are readable from the Management Workstation on request.

STATS performs lookup on all addressing fields. It assigns new data structures to address field values not currently present. It performs any hashing for fast access to the database. More details will be presented later in this document.

Event Manager (EM) 38 extracts statistics from STATS and formats it in ways that allow the Workstation to understand it. It also examines the various statistics to see if their behavior warrants a notification to the Management Workstation. If so, it uses the SNMP Agent software to initiate such notifications.

If the Workstation asks for data, EM 38 gets the data from STATS and sends it to the Workstation. It also performs some level of analysis for statistical, accounting and alarm filtering and decides on further action (e.g. delivery to the Management Workstation).

EM 38 is also responsible for controlling the delivery of events to the Management Workstation, e.g., it performs event filtering. The action to be taken on receipt of an event (e.g. threshold exceeded in STATS) is specified by the event action associated with the threshold. The event is used as an index to select the defined action (e.g. report to Workstation, run local routine xxxx, ignore). The action can be modified by commands from the Management Workstation (e.g., turn off an alarm) or by the control module in an overload situation. An update to the event action, however, does not affect events previously processed even if they are still waiting for transmission to the Management Workstation. Discarded events are counted as such by EM 38.

EM 38 also implements a throttle mechanism to limit the rate of delivery of alarms to the console based on configured limits. This prevents the rapid generation of multiple alarms. In essence, Monitor 10 is given a maximum frequency at which alarms may be sent to the Workstation. Although alarms in excess of the maximum frequency are discarded, a count is kept of the number of alarms that were discarded.

EM 38 invokes routines from the statistics module (STATS) to perform periodic updates such as rate calculations and threshold checks. It calculates time averages, e.g., average traffic by source stations, destination stations. EM 38 requests for access to monitor control variables are passed to the control module.

EM 38 checks whether asynchronous traps (i.e., alarms) to the Workstation are permitted before generating any.

EM 38 receives database update requests from the Management Workstation and invokes the statistics module (STATS) to process these.

Message Transport Module (MTM) 34, which is DRAM based, has two distinct but closely related functions. First, it is responsible for the conversion of Workstation commands and responses from the internal format used within Monitor 10 to the format used to communicate over the network. It isolates the rest of the system from the protocol used to communicate within Management Workstation. It translates between the internal representation of data and ASN.1 used for SNMP. It performs initial decoding of Workstation requests and directs the requests to appropriate modules for processing. It implements SNMP/UDP/IP/LLC or ETHERNET protocols for LAN and SNMP/UDP/IP/SLIP protocols for serial line. It receives network management commands from the Management Workstation and delivers these to the appropriate module for action. Alarms and responses destined for the Workstation are also directed via this module.

Second, MTM 34 is responsible for the delivery and reception of data to and from the Management Workstation using the protocol appropriate to the network. Primary and backup communication paths are provided transparently to the rest of the monitor modules (e.g. LAN and dial up link). It is capable of full duplex delivery of messages between the console and monitoring module. The messages carry event, configuration, test and statistics data.

Event Timing Module (ETM) 40 keeps track of the start time and end times of user specified transactions over the network. In essence, this module monitors the responsiveness of the network at any protocol or layer specified by the user.

Address Tracking Module 42 keeps track of the node name to node address bindings on networks which implement dynamic node addressing protocols.

Memory management for Monitor 10 is handled in accordance with following guidelines. The available memory is divided into four blocks during system initialization. One block includes receive frame buffers. They are used for receiving LAN traffic and for receiving secondary link traffic. These are organized as linked lists of fixed sized buffers. A second block includes system control message blocks. They are used for intertask messages within Monitor 10 and are organized as a linked list of free blocks and multiple linked lists of in process intertask messages. A third block includes transmit buffers. They are used for creation and transmission of workstation alarms and responses and are organized as a linked list of fixed sized buffers. A fourth block is the statistics. This is allocated as a fixed size area at system initialization and managed by the statistics module during system operation.

Task Structure of Monitor;

The structure of the Monitor in terms of tasks and intertask messages is shown in Fig. 6. The rectangular blocks represent interrupt service routines, the ovals represent tasks and the circles represent input queues.

Each task in the system has a single input queue which it uses to receive all input. All inter-process communications take place via messages placed onto the input queue of the destination task. Each task waits on a (well known) input queue and processes events or inter-task messages (i.e., ITM's) as they are received. Each task returns to the kernel within an appropriate time period defined for each task (e.g. after processing a fixed number of events).

Interrupt service routines (ISR's) run on receipt of hardware generated interrupts. They invoke task level processing by sending an ITM to the input queue of the appropriate task.

The kernel scheduler acts as the base loop of the system and calls any runnable tasks as subroutines. The determination of whether a task is runnable is made from the input queue, i.e., if this has an entry the task has work to perform. The scheduler scans the input queues for each task in a round robin fashion and invokes a task with input pending. Each task processes items from its input queue and returns to the scheduler within a defined period. The scheduler then continues the scan cycle of the input queues. This avoids any task locking out others by processing a continuously busy input queue. A task may be given an effectively higher priority by providing it with multiple entries in the scan table.

Database accesses are generally performed using access routines. This hides the internal structure of the database from other modules and also ensures that appropriate interlocks are applied to shared data.

The EM processes a single event from the input queue and then returns to the scheduler.

The MTM Xmit task processes a single event from its input queue and then returns control to the scheduler. The MTM Recv task processes events from the input queue until it is empty or a defined number (e.g. 10) events have been processed and then returns control to the scheduler.

The timer task processes a single event from the input queue and then returns control to the scheduler.

RTP continues to process frames until the input queue is empty or it has processed a defined number (e.g. 10) frames. It then returns to the scheduler.

The following sections contain a more detailed description of some of the above-identified software modules.

<u>The Statistics Module (STATS)</u>:

The functions of the statistics module are:

* to define statistics records;
* to allocate and initialize statistics records;
* to provide routines to lookup statistics records, e.g. lookup_id_addr;
* to provide routines to manipulate the statistics within the records, e.g. stats_age, stats_incr and stats_rate;
* to provide routines to free statistics records, e.g. stats_allocate and stats_deallocate

It provides these services to the Real Time Parser (RTP) module and to the Event Manager (EM) module.

STATS defines the database and it contains subroutines for updating the statistics which it keeps.

STATS contains the type definitions for all statistics records (e.g. DLL, IP, TCP statistics). It provides an initialization routine whose major function is to allocate statistics records at startup from cacheable memory. It provides lookup routines in order to get at the statistics. Each type of statistics record has its own lookup routine (e.g. lookup_ip_address) which returns a pointer to a statistics record of the appropriate type or NULL.

As a received frame is being parsed, statistics within statistics records need to be manipulated (e.g. incremented) to record relevant information about the frame. STATS provides the routines to manipulate those statistics. For example, there is a routine to update counters. After the counter is incremented/decremented and if there is a non-zero threshold associated with the counter, the internal routine compares its value to the threshold. If the threshold has been exceeded, the Event Manager is signaled in order to send a trap to the Workstation. Besides manipulating statistics, these routines, if necessary, signal the Event Manager via an Intertask Message (ITM) to send a trap to the Management Workstation.

The following is an example of some of the statistics records that are kept in STATS.

o monitor statistics
o mac statistics for segment
o llc statisics for segment
o statistics per ethernet/lsap type for segment
o ip statistics for segment
o icmp statistics for segment
o tcp statistics for segment
o udp statistics for segment
o nfs statistics for segment
o ftp control statistics for segment
o ftp data statistics for segment
o telnet statistics for segment
o smtp statistics for segment
o arp statistics for segment

o statistics per mac address
o statistics per ethernet type/lasp per mac address
o statistics per ip address (includes icmp)
o statistics per tcp socket
o statistics per udp socket
o statistics per nfs socket
o statistics per ftp control socket
o statistics per ftp data socket
o statistics per telnet socket
o statistics per smtp socket
o arp statistics per ip address

o statistics per mac address pair
o statistics per ip pair (includes icmp)

o statistics per tcp connection
o statistics per udp pair
o statistics per nfs pair
o statistics per ftp control connection
o statistics per ftp data connection
o statistics per telnet connection
o statistics per smtp connection

o connection histories per udp and tcp socket

All statistics are organized similarly across protocol types. The details of the data structures for the DLL level are presented later.

As noted earlier, there are four statistical object classes (i.e., variables), namely, counts, rates, percentages (%), and meters. They are defined and implemented as follows.

A count is a continuously incrementing variable which rolls around to 0 on overflow. It may be reset on command from the user (or from software). A threshold may be applied to the count and will cause an alarm when the threshold count is reached. The threshold count fires each time the counter increments past the threshold value. For example, if the threshold is set to 5, alarms are generated when the count is 5, 10, 15,...

A rate is essentially a first derivative of a count variable. The rate is calculated at a period appropriate to the variable. For each rate variable, a minimum, maximum and average value is maintained. Thresholds may be set on high values of the rate. The maximums and minimums may be reset on command. The threshold event is triggered each time the rate calculated is in the threshold region.

As commonly used, the % is calculated at a period appropriate to the variable. For each % variable a minimum, maximum and average value is maintained. A threshold may be set on high values of the %. The threshold event is triggered each time the % calculated is in the threshold region.

Finally, a meter is a variable which may take any discrete value within a defined range. The current value has no correlation to past or future values. A threshold may be set on a maximum and/or minimum value for a meter.

The rate and % fields of network event variables are updated differently than counter or meter fields in that they are calculated at fixed intervals rather than on receipt of data from the network.

Structures for statistics kept on a per address or per address pair basis are allocated at initialization time. There are several sizes for these structures. Structures of the same size are linked together in a free pool. As a new structure is needed, it is obtained from a free queue, initialized, and linked into an active list. Active lists are kept on a per statistics type basis.

As an address or address pair (e.g. mac, ip, tcp...) is seen, RTP code calls an appropriate lookup routine. The lookup routine scans active statistics structures to see if a structure has already been allocated for the statistics. Hashing algorithms are used in order to provide for efficient lookup. If no structure has been allocated, the lookup routine examines the appropriate parse control records to determine whether statistics should be kept, and, if so, it allocates a structure of the appropriate size, initializes it and links it into an active list.

Either the address of a structure or a NULL is returned by these routines. If NULL is returned, the RTP does not stop parsing, but it will not be allowed to store the statistics for which the structure was requested.

The RTP updates statistics within the data base as it runs. This is done via macros defined for the RTP. The macros call on internal routines which know how to manipulate the relevant statistic. If the pointer to the statistics structure is NULL, the internal routine will not be invoked.

The EM causes rates to be calculated. The STATS module supplies routines (e.g. stats_rate) which must be called by the EM in order to perform the rate calculations. It also calls subroutines to reformat the data in the database in order to present it to the Workstation (i.e., in response to a get from the Workstation).

The calculation algorithms for the rate and % fields of network event variables are as follows.

The following rates are calculated in units per second, at the indicated (approximate) intervals:

1. 10 second intervals:
   e.g. DLL frame, byte, ethernet, 802.3, broadcast, multicast rates
2. 60 second intervals
   e.g., all DLL error, ethertype/dsap rates
   all IP rates.
   TCP packets, bytes, errors, retransmitted packets, retransmitted bytes, acks, rsts
   UDP packet, error, byte rates
   FTP file transfer, byte transfer, error rates

For these rates, the new average replaces the previous value directly. Maximum and minimum values are retained until reset by the user.

The following rates are calculated in units per hour at the indicated time intervals:

1. 15 minute interval.

e.g., TCP - connection rate
Telnet connection rate
FTP session rate

The hourly rate is calculated from a sum of the last twelve 5 minute readings, as obtained from the buckets for the pertinent parameter. Each new reading replaces the oldest of the twelve values maintained. Maximum and minimum values are retained until reset by the user.

There are a number of other internal routines in STATS. For example, all statistical data collected by the Monitor is subject to age out. Thus, if no activity is seen for an address (or address pair) in the time period defined for age out, then the data is discarded and the space reclaimed so that it may be recycled. In this manner, the Monitor is able to use the memory for active elements rather than stale data. The user can select the age out times for the different components. The EM periodically kicks off the aging mechanism to perform this recycling of resources. STATS provides the routines which the EM calls, e.g. stats_age.

There are also routines in STATS to allocate and de-allocate Statistics, e.g., stats_allocate and stats_de-allocate. The allocate routine is called when stations and dialogs are picked up by the Network Monitor. The de-allocate routine is called by the aging routines when a structure is to be recycled.

<u>The Data Structures in STATS</u>

The general structure of the database within STATS is illustrated by Figs. 7a-c, which shows information that is maintained for the Data Link Layer (DLL) and its organization. A set of data structures is kept for each address associated with the layer. In this case there are three relevant addresses, namely a segment address, indicating which segment the node is on, a MAC address for the node on the segment, and an address which identifies the dialog occurring over that layer. The dialog address is the combination of the MAC addresses for the two nodes which make up the dialog. Thus, the overall data structure has three identifiable components: a segment address data structure (see Fig. 7a), a MAC address data structure (see Fig. 7b) and a dialog data structure (see Fig. 7c).

The segment address structure includes a doubly linked list 102 of segment address records 104, each one for a different segment address. Each segment address record 104 contains a forward and backward link (field 106) for forward and backward pointers to neighboring records and a hash link (field 108). In other words, the segment address records are accessed by either walking down the doubly linked list or by using a hashing mechanism to generate a pointer into the doubly linked list to the first record of a smaller hash linked list. Each record also contains the address of the segment (field 110) and a set of fields for other information. Among these are a flags field 112, a type field 114, a parse_control field 116, and an EM_control field 118. Flags field 112 contains a bit which indicates whether the identified address corresponds to the address of another Network Monitor. This field only has meaning in the MAC address record and not in the segment or dialog address record. Type field 114 identifies the MIB group which applies to this address. Parse control field 116 is a bit mask which indicates what subgroups of statistics from the identified MIB group are maintained, if any. Flags field 112, type field 114 and parse control field 116 make up what is referred to as the parse control record for this MAC address. The Network Monitor uses a default value for parse control field 116 upon initialization or whenever a new node is detected.

The default value turns off all statistics gathering. The statistics gathering for any particular address may subsequently be turned on by the Workstation through a Network Monitor control command that sets the appropriate bits of the parse control field to one.

EM_control field 118 identifies the subgroups of statistics within the MIB group that have changed since the EM last serviced the database to update rates and other variables. This field is used by the EM to identify those parts of STATS which must be updated or for which recalculations must be performed when the EM next services STAT.

Each segment address record 104 also contains three fields for time related information. There is a start_time field 120 for the time that is used to perform some of the rate calculations for the underlying statistics; a first_seen field 122 for the time at which the Network Monitor first saw the communication; and a last_seen field 124 for the time at which the last communication was seen. The last_seen time is used to age out the data structure if no activity is seen on the segment after a preselected period of time elapses. The first_seen time is a statistic which may be of interest to the network manager and is thus retrievable by the Management Workstation for display.

Finally, each segment address record includes a stats_pointer field 126 for a pointer to a DLL segment statistics data structure 130 which contains all of the statistics that are maintained for the segment address. If the bits in parse_control field 116 are all set to off, indicating that no statistics are to be maintained for the address, then the pointer in stats_pointer field 126 is a null pointer.

The list of events shown in data structure 130 of Fig. 7a illustrates the type of data that is collected for this address when the parse control field bits are set to on. Some of the entries in DLL segment statistics data structure 130 are pointers to buckets for historical data. In the case where buckets are maintained, there are twelve buckets each of which represents a time period of five minutes duration and each of which generally contains two items of information, namely, a count for the corresponding five minute time period and a MAX rate for that time period. MAX rate records any spikes which have occurred during the period and which the user may not have observed because he was not viewing that particular statistic at the time.

At the end of DLL segment statistics data structure 130, there is a protocol_Q pointer 132 to a linked list 134 of protocol statistics records 136 identifying all of the protocols which have been detected running on top of the DLL layer for the segment. Each record 136 includes a link 138 to the next record in the list, the identity of the protocol (field 140), a frames count for the number of frames detected for the identified protocol (field 142); and a frame rate (field 144).

The MAC address data structure is organized in a similar manner to that of the segment data structure (see Fig. 7b). There is a doubly linked list 146 of MAC address records 148, each of which contains the same type of information as is stored in DLL segment address records 104. A pointer 150 at the end of each MAC address record 148 points to a DLL address statistics data structure 152, which like the DLL segment address data structure 130, contains fields for all of the statitics that are gathered for that DLL MAC address. Examples of the particular statistics are shown in Fig. 7b.

At the end of DLL address statistics data structure 152, there are two pointer fields 152 and 154, one for a pointer to a record 158 in a dialog link queue 160, and the other for a pointer to a linked list 162 of protocol statistics records 164. Each dialog link queue entry 158 contains a pointer to the next entry (field 168) in the queue and it contains a dialog_addr pointer 170 which points to an entry in the DLL dialog queue which involves the MAC address. (see Fig. 7c). Protocol statistics records 164 have the same structure and contain the same categories of information as their counterparts hanging off of DLL segment statistics data structure 130.

The above-described design is repeated in the DLL dialog data structures. That is, dialog record 172 includes the same categories of information as its counterpart in the DLL segment address data structure and the MAC address data structure. The address field 174 contains the addresses of both ends of the dialog concatenated together to form a single address. The first and second addresses within the single address are arbitrarily designated nodes 1 and 2, respectively. In the stats_pointer field 176 there is a pointer to a dialog statistics data structure 178 containing the relevant statistics for the dialog. The entries in the first two fields in this data structure (i.e., fields 180 and 182) are designated protocol entries and protocols. Protocol entries is the number of different protocols which have been seen between the two MAC addresses. The protocols that have been seen are enumerated in the protocols field 182.

DLL dialog statistics data structure 178, illustrated by Fig. 7c, includes several additional fields of information which only appear in these structures for dialogs for which state information can be kept (e.g. TCP connection). The additional fields identify the transport protocol (e.g., TCP) (field 184) and the application which is running on top of that protocol (field 186). They also include the identity of the initiator of the connection (field 188), the state of the connection (field 190) and the reason that the connection was closed, when it is closed (field 192). Finally, they also include a state_pointer (field 194) which points to a history data structure that will be described in greater detail later. Suffice it to say, that the history data structure contains a short history of events and states for each end of the dialog. The state machine uses the information contained in the history data structure to loosely determine what the state of each of the end nodes is throughout the course of the connection. The qualifier "loosely" is used because the state machine does not closely shadow the state of the connection and thus is capable of recovering from loss of state due to lost packets or missed communications.

The above-described structures and organization are used for all layers and all protocols within STATS.

<u>Real Time Parser (RTP)</u>

The RTP runs as an application task. It is scheduled by the Real Time Kernel scheduler when received frames are detected. The RTP parses the frames and causes statistics, state tracking, and tracing operations to be performed.

The functions of the RTP are:

* obtain frames from the RTP Input Queue;
* parse the frames;
* maintain statistics using routines supplied by the STATS module;
* maintain protocol state information;

* notify the MTM via an ITM if a frame has been received with the Network Monitor's address as the destination address; and
* notify the EM via an ITM if a frame has been received with any Network Monitor's address as the source address.

The design of the RTP is straightforward. It is a collection of routines which perform protocol parsing. The RTP interfaces to the Real Time Kernel in order to perform RTP initialization, to be scheduled in order to parse frames, to free frames, to obtain and send an ITM to another task; and to report fatal errors. The RTP is invoked by the scheduler when there is at least one frame to parse. The appropriate parse routines are executed per frame. Each parse routine invokes the next level parse routine or decides that parsing is done. Termination of the parse occurs on an error or when the frame has been completely parsed.

Each parse routine is a separately compilable module. In general, parse routines share very little data. Each knows where to begin parsing in the frame and the length of the data remaining in the frame.

The following is a list of the parse routines that are available within RTP for parsing the different protocols at the various layers.

Data Link Layer Parse - rtp_dll_parse:

This routine handles Ethernet, IEEE 802.3, IEEE 802.2, and SNAP. See RFC 1010, Assigned Numbers for a description of SNAP (Subnetwork Access Protocol).

Address Resolution Protocol Parse - rtp_arp_parse

ARP is parsed as specified in RFC 826.

Internet Protocol Parse - rtp_ip_parse

IP Version 4 is parsed as specified in RFC 791 as amended by RFC 950, RFC 919, and RFC 922.

Internet Control Message Protocol Parse - rtp_icmp_parse

ICMP is parsed as specified in RFC 792.

Unit Data Protocol Parse - rtp_udp_parse

UDP is parsed as specified in RFC 768.

Transmission Control Protocol Parse - rtp_tcp_parse

TCP is parsed as specified in RFC 793.

Simple Mail Transfer Protocol Parse - rtp_smtp_parse

SMTP is parsed as specified in RFC 821.

File Transfer Protocol Parse - rtp_ftp_parse

FTP is parsed as specified in RFC 959.

Telnet Protocol Parse - rtp_telnet_parse

The Telnet protocol is parsed as specified in RFC 854.

Network File System Protocol Parse - rpt_nfs_parse

The NFS protocol is parsed as specified in RFC 1094.

The RTP calls routines supplied by STATS to look up data structures. By calling these lookup routines, global pointers to data structures are set up. Following are examples of the pointers to statistics data structures that are set up when parse routines call Statistics module lookup routines.

mac_segment, mac_dst_segment, mac_this_segment,
mac_src, mac_dst, mac_dialog
ip_src_segment, ip_dst_segment, ip_this_segment,
ip_src, ip_dst, ip_dialog
tcp_src_segment, tcp_dst_segment,
tcp_this_segment,
tcp_src, tcp_dst, tcp_src_socket, tcp_dst_socket,
tcp_connection

The mac_src and mac_dst routines return pointers to the data structures within STATS for the source MAC address and the destination MAC address, respectively. The lookup_mac_dialog routine returns a pointer to the data structure within STATS for the dialog between the two nodes on the MAC layer. The other STATS routines supply similar pointers for data structures relevant to other protocols.

The RTP routines are aware of the names of the statistics that must be manipulated within the data base (e.g. frames, bytes) but are not aware of the structure of the data. When a statistic is to be manipulated, the RTP routine invokes a macro which manipulates the appropriate statistics in data structures. The macros use the global pointers which were set up during the lookup process described above.

After a frame has been parsed (whether the parse was successful or not), the RTP routine examines the destination mac and ip addresses. If either of the addresses is that of the Network Monitor, RTP obtains a low priority ITM, initializes it, and sends the ITM to the MTM task. One of the fields of the ITM contains the address of the buffer containing the frame.

The RTP must hand some received frames to the EM in order to accomplish the autotopology function (described later). After a frame has been parsed (whether the parse was successful or not), the RTP routine examines the source mac and ip addresses. If either of the addresses is that of another Network Monitor, RTP obtains a low priority ITM, initializes it and sends the ITM to the EM task. The address data structure (in particular, the flags field of the parse control record) within STATS for the MAC or the IP address indicates whether the source address is that of another Network Monitor. One of the fields of the ITM contains the address of the buffer containing the frame.

The RTP receives traffic frames from the network for analysis. RTP operation may be modified by sending control messages to the Monitor. RTP first parses these messages, then detects that the messages are destined for the Monitor and passes them to the MTM task. Parameters which affect RTP operation may be changed by such control messages.

The general operation of the RTP upon receipt of a traffic frame is as follows:

```
Get next frame from input queue
get address records for these stations
For each level of active parsing
{
get pointer to start of protocol header
call layer parse routine
determine protocol at next level
set pointer to start of next layer protocol

}end of frame parsing
if this is a monitor command add to MTM input
queue
if this frame is from another monitor, pass
to EM
check for overload -if yes tell control
```

<u>The State Machine</u>:

In the described embodiment, the state machine determines and keeps state for both addresses of all TCP connections. TCP is a connection oriented transport protocol, and TCP clearly defines the connection in terms of states of the connection. There are other protocols which do not explicitly define the communication in terms of state, e.g. connectionless protocols such as NFS. Nevertheless, even in the connectionless protocols there is implicitly the concept of state because there is an expected order to the events which will occur during the course of the communication. That is, at the very least, one can identify a beginning and an end of the communication, and usually some sequence of events which will occur during the course of the communication. Thus, even though the described embodiment involves a connection oriented protocol, the principles are applicable to many connectionless protocols or for that matter any protocol for which one can identify a beginning and an end to the communication under that protocol.

Whenever a TCP packet is detected, the RTP parses the information for that layer to identify the event associated with that packet. It then passes the identified event along with the dialog identifier to the state machine. For each address of the two parties to the communication, the state machine determines what the current state of the node is. The code within the state machine determines the state of a connection based upon a set of rules that are illustrated by the event/state table shown in Fig. 8.

The interpretation of the event/state table is as follows. The top row of the table identifies the six possible states of a TCP connection. These states are not the states defined in the TCP protocol specification. The left most column identifies the eight events which may occur during the course of a connection. Within the table is an array of boxes, each of which sits at the intersection of a particular event/state combination. Each box specifies the actions taken by the state machine if the identified event occurs while the connection is in the identified state. When the state machine receives a new event, it may perform three types of action. It may change the recorded state for the node. The state to which the node is changed is specified by the S="STATE" entry located at the top of the box. It may increment or decrement the appropriate counters to record the information relevant to that event's occurrence. (In the table, incrementing and decrementing are signified by the ++ and the -- symbols, respectively, located after the identity of the variable being updated.) Or the state machine may take other actions such as those specified in the table as start close timer, Look_for_Data_State, or Look_at_History (to be described shortly). The particular actions which the state machine takes are specified in each box. An empty box indicates that no action is taken for that particular event/state combination. Note, however, that the occurrence of an event is also likely to have caused the update of statistics within STATS, if not by the state machine, then by some other part of the RTP. Also note that it may be desirable to have the state machine record other events, in which case the state table would be modified to identify those other actions.

Two events appearing on the table deserve further explanation, namely, close timer expires and inactivity timer expires. The close timer, which is specified by TCP, is started at the end of a connection and it establishes a period during which any old packets for the connection which are received are thrown away (i.e., ignored). The inactivity timer is not specified by TCP but rather is part of the Network Monitor's resource management functions. Since keeping statistics for dialogs (especially old dialogs) consumes resources, it is desirable to recycle resources for a dialog if no activity has been seen for some period of time. The inactivity timer provides the mechanism for accomplishing this. It is restarted each time an event for the connection is received. If the inactivity timer expires (i.e., if no event is received before the timer period ends), the connection is assumed to have gone inactive and all of the resources associated with the dialog are recycled. This involves freeing them up for use by other dialogs.

The other states and events within the table differ from but are consistent with the definitions provided by TCP and should be self evident in view of that protocol specification.

The event/state table can be read as follows. Assume, for example, that node 1 is in DATA state and the RTP receives another packet from node 1 which it determines to be a TCP FIN packet. According to the entry in the table at the intersection of FIN/DATA (i.e., event/state), the state machine sets the state of the connection for node 1 to CLOSING, it decrements the active connections counter and it starts the close timer. When the close timer expires, assuming no other events over that connection have occurred, the state machine sets node 1's state to CLOSED and it starts the inactivity timer. If the RTP sends another SYN packet to reinitiate a new connection before the inactive timer expires, the state machine sets node 1's state to CONNECTING (see the SYN/CLOSED entry) and it increments an after close counter.

When a connection is first seen, the Network Monitor sets the state of both ends of the connection to UNKNOWN state. If some number of data and acknowledgment frames are seen from both connection ends, the states of the connection ends may be promoted to DATA state. The connection history is searched to make this determination as will be described shortly.

Referring to Figs. 9a-b, within STATS there is a history data structure 200 which the state machine uses to remember the current state of the connection, the state of each of the nodes participating in the connection and a short history of state related information. History data structure 200 is identified by a state_pointer found at the end of the associated dialog statistics data structure in STATS (see Fig. 7c). Within history data structure 200, the state machine records the current state of node 1 (field 202), the current state of node 2 (field 206) and other data relating to the corresponding node (fields 204 and 208). The other data includes, for example, the window size for the receive and transmit communications, the last detected sequence numbers for the data and acknowledgment frames, and other data transfer information.

History data structure 200 also includes a history table (field 212) for storing a short history of events which have occurred over the connection and it includes an index to the next entry within the history table for storing the information about the next received event (field 210). The history table is implemented as a circular buffer which includes sufficient memory to store, for example, 16 records. Each record, shown in Fig. 9b, stores the state of the node when the event was detected (field 218), the event which was detected (i.e., received) (field 220), the data field length (field 222), the sequence number (field 224), the acknowledgment sequence number (field 226) and the identity of the initiator of the event, i.e., either node 1 or node 2 or 0 if neither (field 228).

Though the Network Monitor operates in a promiscuous mode, it may occasionally fail to detect or it may, due to overload, lose a packet within a communication. If this occurs the state machine may not be able to accurately determine the state of the connection upon receipt of the next event. The problem is evidenced by the fact that the next event is not what was expected. When this occurs, the state machine tries to recover state by relying on state history information stored in the history table in field 212 to deduce what the state is. To deduce the current state from historical information, the state machine uses one of the two previously mentioned routines, namely, Look_for_Data_State and Look_at_History.

Referring to Fig. 10, Look_for_Data_State routine 230 searches back through the history one record at a time until it finds evidence that the current state is DATA state or until it reaches the end of the circular buffer (step 232). Routine 230 detects the existence of DATA state by determining whether node 1 and node 2 each have had at least two data events or two acknowledgment combinations with no intervening connect, disconnect or abort events (step 234). If such a sequence of events is found within the history, routine 230 enters both node 1 and node 2 into DATA state (step 236), it increments the active connections counter (step 238) and then it calls a Look_for_Initiator routine to look for the initiator of the connection (step 240). If such a pattern of events is not found within the history, routine 230 returns without changing the state for the node (step 242).

As shown in Fig. 11, Look_for_Initiator routine 240 also searches back through the history to detect a telltale event pattern which identifies the actual initiator of the connection (step 244). More specifically, routine 240 determines whether nodes 1 and 2 each sent connect-related packets. If they did, routine 240 identifies the initiator as the first node to send a connect-related packet (step 246). If the search is not successful, the identity of the connection initiator remains unknown (step 248).

The Look_at_History routine is called to check back through the history to determine whether data transmissions have been repeated. In the case of retransmissions, the routine calls a Look_for_Retransmission routine 250, the operation of which is shown in Fig. 12. Routine 250 searches back through the history (step 252) and checks whether the same initiator node has sent data twice (step 254). It detects this by comparing the current sequence number of the packet as provided by the RTP with the sequence numbers of data packets that were previously sent as reported in the history table. If a retransmission is spotted, the retransmission counter in the dialog statistics data structure of STATS is incremented (step 256). If the sequence number is not found within the history table, indicating that the received packet does not represent a retransmission, the retransmission counter is not incremented (step 258).

Other statistics such as Window probes and keep alives may also be detected by looking at the received frame, data transfer variables, and, if necessary, the history.

Even if frames are missed by the Network Monitor, because it is not directly "shadowing" the connection, the Network Monitor still keeps useful statistics about the connection. If inconsistencies are detected the Network Monitor counts them and, where appropriate, drops back to UNKNOWN state. Then, the Network Monitor waits for the connection to stabilize or deteriorate so that it can again determine the appropriate state based upon the history table.

Principal Transactions of Network Monitor Modules:

The transactions which represent the major portion of the processing load within the Monitor, include monitoring, actions on threshold alarms, processing database get/set requests from the Management Workstation, and processing monitor control requests from the Management Workstation. Each of these mechanisms will now be briefly described.

Monitoring involves the message sequence shown in Fig. 13. In that figure, as in the other figures involving message sequences, the numbers under the heading SEQ. identify the major steps in the sequence. The following steps occur:

1. ISR puts Received traffic frame ITM on RTP input queue
2. request address of pertinent data structure from STATS (get parse control record for this station)
3. pass pointer to RTP
4. update statistical objects by call to statistical update routine in STATS using pointer to pertinent data structure
5. parse completed - release buffers

The major steps which follow a statistics threshold event (i.e., an alarm event) are shown in Fig. 14. The steps are as follows:

1. statistical object update causes threshold alarm
2. STATS generates threshold event ITM to event manager (EM)
3. look up appropriate action for this event
4. perform local event processing
5. generate network alarm ITM to MTM Xmit (if required)
6. format network alarm trap for Workstation from event manager data
7. send alarm to Workstation

The major steps in processing of a database update request (i.e., a get/set request) from the Management Workstation are shown in Fig. 15. The steps are as follows:

1. LAN ISR receives frame from network and passes it to RTP for parsing
2. RTP parses frame as for any other traffic on segment.
3. RTP detects frame is for monitor and sends received Workstation message over LAN ITM to MTM Recv.

4. MTM Recv processes protocol stack.
5. MTM Recv sends database update request ITM to EM.
6. EM calls STATS to do database read or database write with appropriate IMPB
7. STATS performs database access and returns response to EM.
8. EM encodes response to Workstation and sends database update response ITM to MTM Xmit
9. MTM Xmit transmits.

The major steps in processing of a monitor control request from the Management Workstation are shown in Fig. 16. The steps are as follows:

1. Lan ISR receives frame from network and passes received frame ITM to RTP for parsing.
2. RTP parses frame as for any other traffic on segment.
3. RTP detects frame is for monitor and sends received workstation message over LAN ITM to MTM Recv.
4. MTM Recv processes protocol stack and decodes workstation command.
5. MTM Recv sends request ITM to EM.
6. EM calls Control with monitor control IMPB.
7. Control performs requested operation and generates response to EM.
8. EM sends database update response ITM to MTM Xmit.
9. MTM Xmit encodes response to Workstation and transmits.

<u>The Monitor/Workstation Interface</u>:

The interface between the Monitor and the Management Workstation is based on the SNMP definition (RFC 1089 SNMP; RFC 1065 SMI; RFC 1066 SNMP MIB - Note: RFC means Request for Comments). All five SNMP PDU types are supported:

get-request

get-next-request
get-response
set-request
trap

The SNMP MIB extensions are designed such that where possible a user request for data maps to a single complex MIB object. In this manner, the get-request is simple and concise to create, and the response should contain all the data necessary to build the screen. Thus, if the user requests the IP statistics for a segment this maps to an IP Segment Group.

The data in the Monitor is keyed by addresses (MAC, IP) and port numbers (telnet, FTP). The user may wish to relate his data to physical nodes entered into the network map. The mapping of addresses to physical nodes is controlled by the user (with support from the Management Workstation system where possible) and the Workstation retains this information so that when a user requests data for node 'Joe' the Workstation asks the Monitor for the data for the appropriate address(es). The node to address mapping need not be one to one.

Loading and dumping of monitors uses TFTP (Trivial File Transfer Protocol). This operates over UDP as does SNMP. The Monitor to Workstation interface follows the SNMP philosophy of operating primarily in a polled mode. The Workstation acts as the master and polls the Monitor slaves for data on a regular (configurable) basis.

The information communicated by the SNMP is represented according to that subset of ASN.1 (ISO 8824 Specification of ASN.1) defined in the Internet standard Structure of Management Information (SMI - RFC 1065). The subset of the standard Management Information Base (MIB) (RFC 1066 SNMP MIB) which is supported by the Workstation is defined in Appendix III. The added value provided by the Workstation is encoded as enterprise specific extensions to the MIB as defined in Appendix IV. The format for these extensions follows the SMI recomendations for object identifiers so that the Workstation extensions fall in the subtree 1.3.6.1.4.1.x.1. where x is an enterprise specific node identifier assigned by the IAB.

Appendix V is a summary of the network variables for which data is collected by the Monitor for the extended MIB and which can be retrieved by the Workstation. The summary includes short decriptions of the meaning and significance of the variables, where appropriate.

The Management Workstation:

The Management Workstation is a SUN Sparcstation (also referred to as a Sun) available from Sun Microsystems, Inc. It is running the Sun flavor of Unix and uses the Open Look Graphical User Interface (GUI) and the SunNet Manager as the base system. The options required are those to run SunNet Manager with some additional disk storage requirement.

The network is represented by a logical map illustrating the network components and the relationships between them, as shown in Fig. 17. A hierarchical network map is supported with navigation through the layers of the hierarchy, as provided by SNM. The Management Workstation determines the topology of the network and informs the user of the network objects and their connectivity so that he can create a network map. To assist with the map creation process, the Management Workstation attempts to determine the stations connected to each LAN segment to which a Monitor is attached. Automatic determination of segment topology by detecting stations is performed using the autotopology algorithms as described in copending U.S. Patent Application S.N. ***,*** entitled "Automatic Topology Monitor for Multi-

Segment Local Area Network" filed on January 14, 1991 (Attorney Docket No. 13283-NE.APP), incorporated herein by reference.

In normal operation, each station in the network is monitored by a single Monitor that is located on its local segment. The initial determination of the Monitor responsible for a station is based on the results of the autotopology mechanism. The user may override this initial default if required.

The user is informed of new stations appearing on any segment in the network via the alarm mechanism. As for other alarms, the user may select whether stations appearing on and disappearing from the network segment generate alarms and may modify the times used in the aging algorithms. When a new node alarm occurs, the user must add the new alarm to the map using the SNM tools. In this manner, the SNM system becomes aware of the nodes.

The sequence of events following the detection of a new node is:

1. the location of the node is determined automatically for the user.
2. the Monitor generates an alarm for the user indicating the new node and providing some or all of the following information:
    mac address of node
    ip address of node
    segment that the node is believed to be
        located on
    Monitor to be responsible for the node
3. the user must select the segment and add the node manually using the SNM editor

4. The update to the SNM database will be detected and the file reread. The Workstation database is reconstructed and the parse control records for the Monitors updated if required.
5. The Monitor responsible for the new node has its parse control record updated via SNMP set request(s).

An internal record of new nodes is required for the autotopology. When a new node is reported by a Network Monitor, the Management Workstation needs to have the previous location information in order to know which Network Monitors to involve in autotopology. For example, two nodes with the same IP address may exist in separate segments of the network. The history makes possible the correlation of the addresses and it makes possible duplicate address detection.

Before a new Monitor can communicate with the Management Workstation via SNMP it needs to be added to the SNM system files. As the SNM files are cached in the database, the file must be updated and the SNM system forced to reread it.

Thus, on the detection of a new Monitor the following events need to occur in order to add the Monitor to the Workstation:

1. The Monitor issues a trap to the Management Workstation software and requests code to be loaded from the Sun Microsystems boot/load server.
2. The code load fails as the Monitor is not known to the unix networking software at this time.
3. The Workstation confirms that the new Monitor does not exceed the configured system limits (e.g. 5 Monitors per

Workstation) and terminates the initialization sequence if limits are exceeded. An alarm is issued to the user indicating the presence of the new Monitor and whether it can be supported.

4. The user adds the Monitor to the SNMP.HOSTS file of the SNM system, to the etc/hosts file of the Unix networking system and to the SNM map.
5. When the files have been updated the user resets the Monitor using the set tool (described later).
6. The Monitor again issues a trap to the Management Workstation software and requests code to be loaded from the Sun boot/load server.
7. The code load takes place and the Monitor issues a trap requesting data from the Management Workstation.
8. The Monitor data is issued using SNMP set requests.

Note that on receiving the set request, the SNMP proxy rereads in the (updated) SNMP.HOSTS file which now includes the new Monitor. Also note that the SNMP hosts file need only contain the Monitors, not the entire list of nodes in the system.

9. On completion of the set request(s) the Monitor run command is issued by the Workstation to bring the Monitor on line.

The user is responsible for entering data into the SNM database manually. During operation, the Workstation monitors the file write date for the SNM database. When this is different from the last date read, the SNM database is reread and the Workstation database reconstructed. In this manner, user updates to the SNM database are incorporated into the Workstation database as quickly as possible without need for the user to take any action.

When the Workstation is loaded, the database is created from the data in the SNM file system (which the user has possibly updated). This data is checked for consistency and for conformance to the limits imposed by the Workstation at this time and a warning is generated to the user if any problems are seen. If the data errors are minor the system continues operation; if they are fatal the user is asked to correct them and Workstation operation terminates.

The monitoring functions of the Management Workstation are provided as an extension to the SNM system. They consist of additional display tools (i.e., summary tool, values tool, and set tool) which the user invokes to access the Monitor options and a Workstation event log in which all alarms are recorded.

As a result of the monitoring process, the Monitor makes a large number of statistics available to the operator. These are available for examination via the Workstation tools that are provided. In addition, the Monitor statistics (or a selected subset thereof) can be made visible to any SNMP manager by providing it with knowledge of the extended MIB. A description of the statistics maintained are described elswhere.

Network event statistics are maintained on a per network, per segment and per node basis. Within a node, statistics are maintained on a per address (as appropriate to the protocol layer - IP address, port number, ...) and per connection basis. Per network statistics are always derived by the Workstation from the per segment variables maintained by the Monitors. Subsets of the basic statistics are maintained on a node to node and segment to segment basis.

If the user requests displays of segment to segment traffic, the Workstation calculates this data as follows. The inter segment traffic is derived from the node to node statistics for the intersecting set of nodes. Thus, if segment A has nodes 1, 2, and 3 and segment B has nodes 20, 21, and 22, then summing the node to node traffic for

1 -> 20,21,22
2 -> 20,21,22
3 -> 20,21,22

produces the required result. On-LAN/off-LAN traffic for segments is calculated by a simply summing node to node traffic for all stations on the LAN and then subtracting this from total segment counts.

Alarms are reported to the user in the following ways:

1. Alarms received are logged in a Workstation log.
2. The node which the alarm relates to is highlighted on the map.
3. The node status change is propagated up through the (map) hierarchy to support the case where the node is not visible on the screen. This is as provided by SNM.

Summary Tool

After the user has selected an object from the map and invokes the display tools, the summary tool generates the user's initial screen at the Management Workstation. It presents a set of statistical data selected to give an overview of the operational status of the object (e.g., a selected node or segment). The Workstation polls the Monitor for the data required by the Summary Tool display screens.

The Summary Tool displays a basic summary tool screen such as is shown in Fig. 18. The summary tool screen has three panels, namely, a control panel 602, a values panel 604, and a dialogs panel 606. The control panel includes the indicated mouse activated bottons. The functions of each of the buttons is as follows. The file button invokes a traditional file menu. The view button invokes a view menu which allows the user to modify or tailor the visual protperties of the tool. The properties button invokes a properties menu containing choices for viewing and sometimes modifying the properties of objects. The tools button invokes a tools menu which provides access to the other Workstation tools, e.g. Values Tool.

The Update Interval field allows the user to specify the frequency at which the displayed statistics are updated by polling the Monitor. The Update Once button enables the user to retrieve a single screen update. When the Update Once button is invoked not only is the screen updated but the update interval is automatically set to "none".

The type field enables the user to specify the type of network objects on which to operate, i.e., segment or node.

The name button invokes a pop up menu containing an alphabetical list of all network objects of the type selected and apply and reset buttons. The required name can then be selected from the (scrolling) list and it will be entered in the name field of the summary tool when the apply button is invoked. Alternatively, the user may enter the name directly in the summary tool name field.

The protocol button invokes a pop up menu which provides an exclusive set of protocol layers which the user may select. Selection of a layer copies the layer name into the displayed field of the summary tool when the apply operation is invoked. An example of a protocol selection menu is shown in Fig. 19. It displays the available protocols in the form of a protocol tree with multiple protocol familes. The protocol selection is two dimensional. That is, the user first selects the protocol family and then the particular layer within that family.

As indicated by the protocol trees shown in Fig. 19, the capabilities of the Monitor can be readily extended to handle other protocol families. The particular ones which are implemented depend upon the needs of the particular network environment in which the Monitor will operate.

The user invokes the apply button to indicate that the selection process is complete and the type, name, protocol, etc. should be applied. This then updates the screen using the new parameter set that the user selected. The reset button is used to undo the selections and restore them to their values at the last apply operation.

The set of statistics for the selected parameter set is displayed in values panel 604. The members of the sets differ depending upon, for example, what protocol was selected. Figs. 20a-g present examples of the types of statistical variables which are displayed for the DLL, IP, UDP, TCP, ICMP, NFS, and ARP/RARP protocols, respectively. The meaning of the values display fields are described in Appendix I, attached hereto.

Dialogs panel 606 contains a display of the connection statistics for all protocols for a selected node. Within the Management Workstation, connection lists are maintained per node, per supported protocol. When connections are displayed, they are sorted on "Last Seen" with the most current displayed first. A single list returned from the Monitor contains all current connection. For TCP, however, each connection also contains a state and TCP connections are displayed as

Past and Present based upon the returned state of the connection. For certain dialogs, such as TCP and NFS over UDP, there is an associated direction to the dialog, i.e., from the initiator (source) to the receiver (sink). For these dialogs, the direction is identified in a DIR. field. A sample of information that is displayed in dialogs panel 606 is presented in Fig. 21 for current connections.

Values Tool

The values tool provides the user with the ability to look at the statistical database for a network object in detail. When the user invokes this tool, he may select a basic data screen containing a rate values panel 620, a count values panel 622 and a protocols seen panel 626, as shown in Fig. 22, or he may select a traffic matrix screen 628, as illustrated in Fig. 23.

In rate values and count values panels 620 and 622, value tools presents the monitored rate and count statistics, respectively, for a selected protocol. The parameters which are displayed for the different protocols (i.e., different groups) are listed in Appendix II. In general, a data element that is being displayed for a node shows up in three rows, namely, a total for the data element, the number into the data element, and the number out of the data element. Any exceptions to this are identified in Appendix II. Data elements that are displayed for segments, are presented as totals only, with no distinction between Rx and Tx.

When invoked the Values Tool displays a primary screen to the user. The primary screen contains what is considered to be the most significant information for the selected object. The user can view other information for the object (i.e., the statistics for the other parameters) by scrolling down.

The displayed information for the count values and rate values panels 620 and 622 includes the following. An alarm field reports whether an alarm is currently active for this item. It displays as "*" if active alarm is present. A Current Value/Rate field reports the current rate or the value of the counter used to generate threshold alarms for this item. This is reset following each threshold trigger and thus gives an idea of how close to an alarm threshold the variable is. A Typical Value field reports what this item could be expected to read in a "normal" operating situation. This field is filled in for those items where this is predictable and useful. It is maintained in the Workstation database and is modifiable by the user using the set tool. An Accumulated Count field reports the current accumulated value of the item or the current rate. A Max Value field reports the highest value recently seen for the item. This value is reset at intervals defined by a user adjustable parameter (default 30 minutes). This is not a rolling cycle but rather represents the highest value since it was reset which may be from 1 to 30 minutes ago (for a rest period of 30 minutes). It is used only for rates. A Min Value field reports the lowest value recently seen for the item. This operates in the same manner as Max Value field and is used only for rates.

A Percent (%) field reports only for the following variables:

off seg counts:

100(in count / total off seg count)

100(out count / total off seg count)

100(transit count / total off seg count)

100(local count / total off seg count)

off seg rates

100(transit rate / total off seg rate), etc.

protocols

100(frame rate this protocol / total frame rate)

On the right half of the basic display, there the following addtional fields: a High Threshold field and a Sample period for rates field.

Set Tool

The set tool provides the user with the ability to modify the parameters controling the operation of the Monitors and the Management Workstation. These parameters affect both user interface displays and the actual operation of the Monitors. The parameters which can be operated on by the set tool can be divided into the following categories: alarm thresholds, monitoring control, segment Monitor administration, and typical values.

The monitoring control variables specify the actions of the segment Monitors and each Monitor can have a distinct set of control variables (e.g., the parse control records that are described elsewhere). The user is able to define those nodes, segments, dialogs and protocols in which he is interested so as to make the best use of memory space available for data storage. This mechanism allows for load sharing, where mulitple Monitors on the same segment can divide up the total number of network objects which are to be monitored so that no duplication of effort between them takes place.

The monitor administration variables allow the user to modify the operation of the segment Monitor in a more direct manner than the monitoring control variables. Using the set tool, the user can perform those operations such as reset, time changes etc. which are normally the prerogative of a system administrator.

Note that the above descriptions of the tools available through the Management Workstation are not meant to imply that other choices may not be made regarding the particular information which is displayed and the manner in which it is displayed.

Adaptively Setting Network Monitor Thresholds:

The Workstation sets the thresholds in the Network Monitor based upon the performance of the system as observed over an extended period of time. That is, the Workstation periodically samples the output of the Network Monitors and assembles a model of a normally functioning network. Then, the Workstation sets the thresholds in the Network Monitors based upon that model. If the observation period is chosen to be long enough and since the model represents the "average" of the network performance over the observation period, temporary undesired deviations from normal behavior are smoothed out over time and model tends to accurately reflect normal network behavior.

Referring the Fig. 24, the details of the training procedure for adaptively setting the Network Monitor thresholds are as follows. To begin training, the Workstation sends a start learning command to the Network Monitors from which performance data is desired (step 302). The start learning command disables the thresholds within the Network Monitor and causes the Network Monitor to periodically send data for a predefined set of network parameters to the Management Workstation. (Disabling the thresholds, however, is not necessary. One could have the learning mode operational in parallel with monitoring using existing thresholds.) The set of parameters may be any or all of the previously mentioned parameters for which thresholds are or may be defined.

Throughout the learning period, the Network Monitor sends "snapshots" of the network's performance to the Workstation which, in turn, stores the data in a performance history database 306 (step 304). The network manager sets the length of the learning period.

Typically, it should be long enough to include the full range of load conditions that the network experiences so that a representative performance history is generated. It should also be long enough so that short periods of overload or faulty behavior do not distort the resulting averages.

After the learning period has expired, the network manager, through the Management Workstation, sends a stop learning command to the Monitor (step 308). The Monitor ceases automatically sending further performance data updates to the Workstation and the Workstation processes the data in its performance history database (step 310). The processing may involve simply computing averages for the parameters of interest or it may involve more sophisticated statistical analysis of the data, such as computing means, standard deviations, maximum and minimum values, or using curve fitting to compute rates and other pertinent parameter values.

After the Workstation has statistically analyzed the performance data, it computes a new set of thresholds for the relevant performance parameters (step 312). To do this, it uses formulas which are appropriate to the particular parameter for which a threshold is being computed. That is, if the parameter is one for which one would expect to see wide variations in its value during network monitoring, then the threshold should be set high enough so that the normal expected variations do not trigger alarms. On the other hand, if the parameter is of a type for which only small variations are expected and larger variations indicate a problem, then the threshold should be set to a value that is close to the average observed value. Examples of formulae which may be used to compute thresholds are:

* Highest value seen during learning period;

* Highest value seen during learning period + 10%;
* Highest value seen during learning period + 50%;
* Highest value seen during learning period + user-defined percent;
* Any value of the parameter other than zero;
* Average value seen during learning period + 50%; and
* Average value seen during learning period + user-defined percent.

As should be evident from these examples, there is a broad range of possibilities regarding how to compute a particular threshold. The choice, however, should reflect the parameter's importance in signaling serious network problems and its normal expected behavior (as may be evidenced from the performance history acquired for the parameter during the learning mode).

After the thresholds are computed, the Workstation loads them into the Monitor and instructs the Monitor to revert to normal monitoring using the new thresholds (step 314).

This procedure provides a mechanism enabling the network manager to adaptively reset thresholds in response to changing conditions on the network, shifting usage patterns and evolving network topology. As the network changes over time, the network manager merely invokes the adaptive threshold setting feature and updates the thresholds to reflect those changes.

<u>The Diagnostic Analyzer Module</u>:

The Management Workstation includes a diagnostic analyzer module which automatically detects and diagnoses the existence and cause of certain types of network problems. The functions of the diagnostic module may actually be distributed among the Workstation and the

Network Monitors which are active on the network. In principle, the diagnostic analyzer module includes the following elements for performing its fault detection and analysis functions.

The Management Workstation contains a reference model of a normally operating network. The reference model is generated by observing the performance of the network over an extended period of time and computing averages of the performance statistics that were observed during the observation period. The reference model provides a reference against which future network performance can be compared so as to diagnose and analyze potential problems. The Network Monitor (in particular, the STATS module) includes alarm thresholds on a selected set of the parameters which it monitors. Some of those thresholds are set on parameters which tend to be indicative of the onset or the presence of particular network problems.

During monitoring, when a Monitor threshold is exceeded, thereby indicating a potential problem (e.g. in a TCP connection), the Network Monitor alerts the Workstation by sending an alarm. The Workstation notifies the user and presents the user with the option of either ignoring the alarm or invoking a diagnostic algorithm to analyze the problem. If the user invokes the diagnostic algorithm, the Workstation compares the current performance statistics to its reference model to analyze the problem and report its results. (Of course, this may also be handled automatically so as to not require user intervention.) The Workstation obtains the data on current performance of the network by retrieving the relevant performance statistics from all of the segment Network Monitors that may have information useful to diagnosing the problem.

The details of a specific example involving poor TCP connection performance will now be described. This example refers to a typical network on which the diagnostic analyzer resides, such as the network illustrated in Fig. 25. It includes three segments labelled S1, S2, and S3, a router R1 connecting S1 to S2, a router R2 connecting S2 to S3, and at least two nodes, node A on S1 which communicates with node B on S3. On each segment there is also a Network Monitor 324 to observe the performance of its segment in the manner described earlier. A Management Workstation 320 is also located on S1 and it includes a diagnostic analyzer module 322. For this example, the sympton of the network problem is degraded peformance of a TCP connection between Nodes A and B.

A TCP connection problem may manifest itself in a number of ways, including, for example, excessively high numbers for any of the following:

errors
packets with bad sequence numbers
packets retransmitted
bytes retransmitted
out of order packets
out of order bytes
packets after window closed
bytes after window closed
average and maximum round trip times

or by an unusually low value for the current window size. By setting the appropriate thresholds, the Monitor is programmed to recognize any one or more of these symptons. If any one of of the thresholds is exceeded, the Monitor sends an alarm to the Workstation. The Workstation is programmed to recognize the particular alarm as related to an event which can be further analyzed by its diagnostic analyzer module 322. Thus, the Workstation presents the user with the option of invoking its diagnostic capabilities (or automatically invokes the diagnostic capabilities).

In general terms, when the diagnostic analyzer is invoked, it looks at the performance data that the segment Monitors produce for the two nodes, for the dialogs between them and for the links that interconnect them and compares that data to the reference model for the network. If a significant divergence from the reference model is identified, the diagnostic analyzer informs the Workstation (and the user) about the nature of the divergence and the likely cause of the problem. In conducting the comparison to "normal" network performance, the network circuit involved in communications between nodes A and B is decomposed into its individual components and diagnostic analysis is performed on each link individually in the effort to isolate the problem further.

The overall structure of the diagnostic algorithm 400 is shown in Fig. 26. When invoked for analyzing a possible TCP problem between nodes A and B, diagnostic analyzer 322 checks for a TCP problem at node A when it is acting as a source node (step 402). To perform this check, diagnostic algorithm 400 invokes a source node analyzer algorithm 450 shown in Fig. 27. If a problem is identified, the Workstation reports that there is a high probability that node A is causing a TCP problem when operating as a source node and it reports the results of the investigation performed by algorithm 450 (step 404).

If node A does not appear to be experiencing a TCP problem when acting as a source node, diagnostic analyzer 322 checks for evidence of a TCP problem at node B when it is acting as a sink node (step 406). To perform this check, diagnostic algorithm 400 invokes a sink node analyzer algorithm 470 shown in Fig. 28. If a problem is identified, the Workstation reports that there is a high probability that node B is causing a TCP problem when operating as a sink node and it reports the results of the investigation performed by algorithm 470 (step 408).

Note that source and sink nodes are concepts which apply to those dialogs for which a direction of the communication can be defined. For example, the source node may be the one which initiated the dialog for the purpose of sending data to the other node, i.e., the sink node.

If node B does not appear to be experiencing a TCP problem when acting as a sink node, diagnostic analyzer 322 checks for evidence of a TCP problem on the link between Node A and Node B (step 410). To perform this check, diagnostic algorithm 400 invokes a link analysis algorithm 550 shown in Fig. 29. If a problem is identified, the Workstation reports that there is a high probability that a TCP problem exists on the link and it reports the results of the investigation performed by link analysis algorithm 550 (step 412).

If the link does not appear to be experiencing a TCP problem, diagnostic analyzer 322 checks for evidence of a TCP problem at node B when it is acting as a source node (step 414). To perform this check, diagnostic algorithm 400 invokes the previously mentioned source algorithm 450 for Node B. If a problem is identified, the Workstation reports that there is a medium probability that node B is causing a TCP problem when operating as a source node and it reports the results of the investigation performed by algorithm 450 (step 416).

If node B does not appear to be experiencing a TCP problem when acting as a source node, diagnostic analyzer 322 checks for a TCP problem at node A when it is acting as a sink node (step 418). To perform this check, diagnostic algorithm 400 invokes sink node analyzer algorithm 470 for Node A. If a problem is identified, the Network Monitor reports that there is a medium probability that node A is causing a TCP problem when operating as a sink node and it reports the results of the investigation performed by algorithm 470 (step 420).

Finally, if node A does not appear to be experiencing a TCP problem when acting as a sink node, diagnostic analyzer 322 reports that it was not able to isolate the cause of a TCP problem (step 422).

The algorithms which are called from within the above-described diagnostic algorithm will now be described. Referring to Fig. 27, source node analyzer algorithm 450 checks whether a particular node is causing a TCP problem when operating as a source node. The strategy is as follows. To determine whether a TCP problem exists at this node which is the source node for the TCP connection, look at other connections for which this node is a source. If other TCP connections are okay, then there is probably not a problem with this node. This is an easy check with a high probability of being correct. If no other good connections exist, then look at the lower layers for possible reasons. Start at DLL and work up as problems at lower layers are more fundamental, i.e., they cause problems at higher layers whereas the reverse is not true.

In accordance with this approach, algorithm 450 first determines whether the node is acting as a source node in any other TCP connection and, if so, whether the other connection is okay (step 452). If the node is performing satisfactorily as a source node in another TCP connection, algorithm 450 reports that there is no problem at the source node and returns to diagnostic algorithm 400 (step 454). If algorithm 450 cannot identify any other TCP connections involving this node that are okay, it moves up through the protocol stack checking each level for a problem. In this case, it then checks for DLL problems at the node when it is acting as a source node by calling an DLL problem checking routine 510 (see Fig. 30) (step 456). If a DLL problem is found, that fact is reported (step 458). If no DLL problems are found, algorithm 450 checks for an IP problem at the node when it is acting as a source by calling an IP problem checking routine 490 (see Fig. 31) (step 460). If an IP problem is found, that fact is reported (step 462). If no IP problems are found, algorithm 450 checks whether any other TCP connection in which the node participates as a source is not okay (step 464). If another TCP connection involving the node exists and it is not okay, algorithm 450 reports a TCP problem at the node (step 466). If no other TCP connections where the node is acting as a source node can be found, algorithm 450 exits.

Referring to Fig. 28, sink node analyzer algorithm 470 checks whether a particular node is causing a TCP problem when operating as a sink node. It first determines whether the node is acting as a sink node in any other TCP connection and, if so, whether the other connection is okay (step 472). If the node is performing satisfactorily as a sink node in another TCP connection, algorithm 470 reports that there is no problem at the source node and returns to diagnostic algorithm 400 (step 474). If algorithm 470 cannot identify any other TCP connections involving this node that are okay, it then checks for DLL problems at the node when it is acting as a sink node by calling DLL problem checking routine 510 (step 476). If a DLL problem is found, that fact is reported (step 478). If no DLL problems are found, algorithm 470 checks for an IP problem at the node when it is acting as a sink by calling IP problem checking routine 490 (step 480). If an IP problem is found, that fact is reported (step 482). If no IP problems are found, algorithm 470 checks whether any other TCP connection in which the node participates as a sink is not okay (step 484). If another TCP connection involving the node as a sink exists and it is not okay, algorithm 470 reports a TCP problem at the node (step 486). If no other TCP connections where the node is acting as a sink node can be found, algorithm 470 exits.

Referring to Fig. 31, IP problem checking routine 490 checks for IP problems at a node. It does this by comparing the IP performance statistics for the node to the reference model (steps 492 and 494). If it detects any significant deviations from the reference model, it reports that there is an IP problem at the node (step 496). If no significant deviations are noted, it reports that there is no IP problem at the node (step 498).

As revealed by examining Fig. 30, DLL problem checking routine 510 operates in a similar manner to IP problem checking routine 490, with the exception that it examines a different set of parameters (i.e., DLL parameters) for significant deviations.

Referring the Fig. 29, link analysis logic 550 first determines whether any other TCP connection for the link is operating properly (step 552). If a properly operating TCP connection exists on the link, indicating that there is no link problem, link analysis logic 550 reports that the link is okay (step 554). If a properly operating TCP connection cannot be found, the link is decomposed into its constituent components and an IP link component problem checking routine 570 (see Fig. 32) is invoked for each of the link components (step 556). IP link component problem routine 570 evaluates the link component by checking the IP layer statistics for the relevant link component.

The decomposition of the link into its components arranges them in order of their distance from the source node and the analysis of the components proceeds in that order. Thus, for example, the link components which make up the link between nodes A and B include in order: segment S1, router R1, segment S2, router R2, and segment S3. The IP data for these various components are analyzed in the following order:

IP data for segment S1
IP data for address R1
IP data for source node to R1
IP data for S1 to S2
IP data for S2
IP data for address R2
IP data for S3
IP data for S2 to S3
IP data for S1 to S3

As shown in Fig. 32, IP link component problem checking routine 570 compares IP statistics for the link component to the reference model (step 572) to determine whether network performance deviates significantly from that specified by the model (step 574). If significant deviations are detected, routine 570 reports that there is an IP problem at the link component (step 576). Otherwise, it reports that it found no IP problem (step 578).

Referring back to Fig. 29, after completing the IP problem analysis for all of the link components, logic 550 then invokes a DLL link component problem checking routine 580 (see Fig. 33) for each link component to check its DLL statistics (step 558).

DLL link problem routine 580 is similar to IP link problem routine 570. As shown in Fig. 33, DLL link problem checking routine 580 compares DLL statistics for the link to the reference model (step 582) to determine whether network performance at the DLL deviates significantly from that specified by the model (step 584). If significant deviations are detected, routine 580 reports that there is a DLL problem at the link component (step 586). Otherwise, it reports that no DLL problems were found (step 588).

Referring back to Fig. 29, after completing the DLL problem analysis for all of the link components, logic 550 checks whether there is any other TCP on the link (step 560). If another TCP exists on the link (which implies that the other TCP is also not operating properly), logic 550 reports that there is a TCP problem on the link (step 562). Otherwise, logic 550 reports that there was not enough information from the existing packet traffic to determine whether there was a link problem (step 564)

If the analysis of the link components does not isolate the source of the problem and if there were components for which sufficient information was not available (due possibly to lack of traffic over through that component), the user may send test messages to those components to generate the information needed to evaluate its performance.

The reference model against which comparisons are made to detect and isolate malfunctions may be generated by examining the behavior of the network over an extended period of operation or over multiple periods of operation. During those periods of operation, average values and maximum excursions (or standard deviations) for observed statistics are computed. These values provide an initial estimate of a model of a properly functioning system. As more experience with the network is obtained and as more historical data on the various statistics is accumulated the thresholds for detecting actual malfunctions or imminent malfunctions and the reference model can be revised to reflect the new experience.

What constitutes a significant deviation from the reference model depends upon the particular parameter involved. Some parameters will not deviate from the expected norm and thus any deviation would be considered to be significant, for example, consider ICMP messages of type "destination unreachable," IP errors, TCP errors. Other parameters will normally vary within a wide range of acceptable values, and only if they move outside of that range should the deviation be considered significant. The acceptable ranges of variation can be determined by watching network performance over a sustained period of operation.

The parameters which tend to provide useful information for identifying and isolating problems at the node level for the different protocols and layers include the following.

<u>TCP</u>
error rate
header byte rate
packets retransmitted
bytes retransmitted
packets after window closed
bytes after window closed

<u>UDP</u>
error rate
header byte rate

<u>IP</u>
error rate
header byte rate
fragmentation rate
all ICMP messages of type destination

unreachable, parameter problem, redirection

DLL
error rate
runts

For diagnosing network segment problems, the above-identified parameters are also useful with the addition of the alignment rate and the collision rate at the DLL. All or some subset of these parameters may be included among the set of parameters which are examined during the diagnostic procedure to detect and isolate network problems.

The above-described technique can be applied to a wide range of problems on the network, including among others, the following:

TCP Connection fails to establish
UDP Connection performs poorly
UDP not working at all
IP poor performance/high error rate
IP not working at all
DLL poor performance/high error rate
DLL not working at all

For each of these problems, the diagnostic approach would be similar to that described above, using, of course, different parameters to identify the potential problem and isolate its cause.

The Event Timing Module

Referring again to Fig. 5, the RTP is programmed to detect the occurrence of certain transactions for which timing information is desired. The transactions typically occur within a dialog at a particular layer of the protocol stack and they involve a first event (i.e., an initiating event) and a subsequent partner event or response. The events are protocol messages that arrive at the Network Monitor, are parsed by the RTP and then passed to Event Timing Module (ETM) for processing. A transaction of interest might be, for example, a read of a file on a server. In that case, the initiating event is the read request and the partner event is the read response. The time of interest is the time required to receive a response to the read request (i.e., the transaction time). The transaction time provides a useful measure of network performance and if measured at various times throughout the day under different load conditions gives a measure of how different loads affect network response times. The layer of the communicaton protocol at which the relevant dialog takes place will of course depend upon the nature of the event.

In general, when the RTP detects an event, it transfers control to the ETM which records an arrival time for the event. If the event is an initiating event, the ETM stores the arrival time in an event timing database 300 (see Fig. 34) for future use. If the event is a partner event, the ETM computes a difference between that arrival time and an earlier stored time for the initiating event to determine the complete transaction time.

Event timing database 300 is an array of records 302. Each record 302 includes a dialog field 304 for identifying the dialog over which the transactions of interest are occurring and it includes an entry type field 306 for identifying the event type of interest. Each record 302 also includes a start time field 308 for storing the arrival time of the initiating event and an average delay time field 310 for storing the computed average delay for the transactions. A more detailed description of the operation of the ETM follows.

Referring to Fig. 35, when the RTP detects the arrival of a packet of the type for which timing information is being kept, it passes control to the ETM along with relevant information from the packet, such as the dialog identifier and the event type (step 320). The ETM then determines whether it is to keep timing information for that particular event by checking the event timing database (step 322). Since each event type can have multiple occurrences (i.e., there can be multiple dialogs at a given layer), the dialog identifier is used to distinguish between events of the same type for different dialogs and to identify those for which information has been requested. All of the dialog/events of interest are identified in the event timing database. If the current dialog and event appear in the event timing database, indicating that the event should be timed, the ETM determines whether the event is a starting event or an ending event so that it may be processed properly (step 324). For certain events, the absence of a start time in the entry field of the appropriate record 302 in event timing database 300 is one indicator that the event represents a start time; otherwise, it is an end time event. For other events, the ETM determines if the start time is to be set by the event type as specified in the packet being parsed. For example, if the event is a file read a start time is stored. If the event is the read completion it represents an end time. In general, each protocol event will have its own intrinsic meaning for how to determine start and end times.

Note that the arrival time is only an estimate of the actual arrival time due to possible queuing and other processing delays. Nevertheless, the delays are generally so small in comparison to the transaction times being measured that they are of little consequence.

In step 324, if the event represents a start time, the ETM gets the current time from the kernal and stores it in start time field 308 of the appropriate record in event timing database 300 (step 326). If the event represents an end time event, the ETM obtains the current time from the kernel and computes a difference between that time and the corresponding start time found in event timing database 300 (step 328). This represents the total time for the transaction of interest. It is combined with the stored average transaction time to compute a new running average transaction time for that event (step 330).

Any one of many different methods can be used to compute the running average transaction time. For example, the following formula can be used:

New Avg. = [(5 * Stored Avg.) + Transaction Time]/6.

After six transaction have been timed, the computed new average becomes a running average for the transaction times. The ETM stores this computed average in the appropriate record of event timing database 300, replacing the previous average transaction time stored in that record, and it clears start time entry field 308 for that record in preparation for timing the next transaction.

After processing the event in steps 322, 326, and 330, the ETM checks the age of all of the start time entries in the event timing database 300 to determine if any of them are too "old" (step 332). If the difference between the current time and any of the start times exceeds a preselected threshold, indicating that a partner event has not occurred within a reasonable period of time, the ETM deletes the old start time entry for that dialog/event (step 334). This insures that a missed packet for a partner event does not result in an erroneously large transaction time which throws off the running average for that event.

If the average transaction time increases beyond a preselected threshold set for timing events, an alarm is sent to the Workstation.

Two examples will now be described to illustrate the operation of the ETM for specific event types. In the first example, Node A of Fig. 25 is communicating with Node B using the NFS protocol. Node A is the client while Node B is the server. The Network Monitor resides on the same segment as node A, but this is not a requirement. When Node A issues a read request to Node B, the Network Monitor sees the request and the RTP within the Network Monitor transfers control to the ETM. Since it is a read, the ETM stores a start time in the Event Timing Database. Thus, the start time is the time at which the read was initiated.

After some delay, caused by the transmission delays of getting the read message to node B, node B performs the read and sends a response back to node A. After some further transmission delays in returning the read response, the Network Monitor receives the second packet for the event. At the time, the ETM recognizes that the event is an end time event and updates the average transaction time entry in the appropriate record with a new computed running average. The ETM then compares the average transaction time with the threshold for this event and if it has been exceeded, issues an alarm to the Workstation.

In the second example, node A is communicating with Node B using the Telnet protocol. Telnet is a virtual terminal protocol. The events of interest take place long after the initial connection has been established. Node A is typing at a standard ASCII (VT100 class) terminal which is logically (through the network) connected to Node B. Node B has an application which is receiving the characters being typed on Node A and, at appropriate times, indicated by the logic of the applications, sends characters back to the terminal located on Node A. Thus, every time node A sends characters to B, the Network Monitor sees the transmission.

In this case, there are several transaction times which could provide useful network performance information. They include, for example, the amount of time it takes to echo characters typed at the keyboard through the network and back to the display screen, the delay between typing an end of line command and seeing the completion of the application event come back or the network delays incurred in sending a packet and receiving acknowledgment for when it was received.

In this example, the particular time being measured is the time it takes for the network to send a packet and receive an acknowledgement that the packet has arrived. Since Telnet runs on top of TCP, which in turn runs on top of IP, the Network Monitor monitors the TCP acknowledge end-to-end time delays.

Note that this is a design choice of the implementation and that all events visible to the Network Monitor by virtue of the fact that information is in the packet could be measured.

When Node A transmits a data packet to Node B, the Network Monitor receives the packet. The RTP recognizes the packet as being part of a timed transaction and passes control to the ETM. The ETM recognizes it as a start time event, stores the start time in the event timing database and returns control to the RTP after checking for aging.

When Node B receives the data packet from Node A, it sends back an acknowledgment packet. When the Network Monitor sees that packet, it delivers the event to the ETM, which recognizes it as an end time event. The ETM calculates the delay time for the complete transaction and uses that to update the average transaction time. The ETM then compares the new average transaction time with the threshold for this event. If it has been exceeded, the ETM issues an alarm to the Workstation.

Note that this example is measuring something very different than the previous example. The first example measures the time it takes to traverse the network, perform an action and return that result to the requesting node. It measures performance as seen by the user and it includes delay times from the network as well as delay times from the File Server.

The second example is measuring network delays without looking at the service delays. That is, the ETM is measuring the amount of time it takes to send a packet to a node and receive the acknowledgement of the receipt of the message. In this example, the ETM is measuring transmissions delays as well as processing delays associated with network traffic, but not anything having to do with non-network processing.

As can be seen from the above examples, the ETM can measure a broad range of events. Each of these events can be measured passively and without the cooperation of the nodes that are actually participating in the transmission.

The Address Tracker Module (ATM)

Address tracker module (ATM) 43, one of the software modules in the Network Monitor (see Fig. 5), operates on networks on which the node addresses for particular node to node connections are assigned dynamically. An Appletalk® Network, developed by Apple Computer Company, is an example of a network which uses dynamic node addressing. In such networks, the dynamic change in the address of a particular service causes difficulty troubleshooting the network because the network manager may not know where the various nodes are and what they are called. In addition, foreign network addresses (e.g., the IP addresses used by that node for communication over an IP network to which if is connected) can not be relied upon to point to a particular node. ATM 43 solves this problem by passively monitoring the network traffic and collecting a table showing the node address to node name mappings.

In the following description, the network on which the Monitor is located is assumed to be an Appletalk® Network. Thus, as background for the following discussion, the manner in which the dynamic node addressing mechanism operates on that network will first be described.

When a node is activated on the Appletalk® Network, it establishes its own node address in accordance with protocol referred to as the Local Link Access Protocol (LLAP). That is, the node guesses its own node address and then verifies that no other node on the network is using that address. The node verifies the uniqueness of its guess by sending an LLAP Enquiry control packet informing all other nodes on the network that it is going to assign itself a particular address unless another node responds that the address has already been assigned. If no other node claims that address as its own by sending an LLAP acknowledgment control packet, the first node uses the address which it has selected. If another node claims the address as its own, the first node tries another address. This continues until, the node finds an unused address.

When the first node wants to communicate with a second node, it must determine the dynamically assigned node address of the second node. It does this in accordance with another protocol referred to as the Name Binding Protocol (NBP). The Name Binding Protocol is used to map or bind human understandable node names with machine understandable node addresses. The NBP allows nodes to dynamically translate a string of characters (i.e., a node name) into a node address. The node needing to communicate with another node broadcasts an NBP Lookup packet containing the name for which a node address is being requested. The node having the name being requested responds with its address and returns a Lookup Reply packet containing its address to the original requesting node. The first node then uses that address its current communications with the second node.

Referring to Fig. 36, the network includes an Appletalk® Network segment 702 and a TCP/IP segment 704, each of which are connected to a larger network 706 through their respective gateways 708. A Monitor 710, including a Real Time Parser (RTP) 712 and an Address Tracking Module (ATM) 714, is located on Appletalk network segment 702 along with other nodes 711. A Management Workstation 716 is located on segment 704. It is assumed that Monitor 710 has the features and capabilities previously described; therefore, those features not specifically related to the dynamic node addressing capability will not be repeated here but rather the reader is referred to the earlier discussion. Suffice it to say that Monitor 710 is, of course, adapted to operate on Appletalk Network segment 702, to parse and analyze the packets which are transmitted over that segment according to the Appletalk® family of protocols and to communicate the information which it extracts from the network to Management Workstation 716 located on segment 704.

Within Monitor 710, ATM 714 maintains a name table data structure 730 such as is shown in Fig. 37. Name Table 720 includes records 722, each of which has a node name field 724, a node address field 726, an IP address field 728, and a time field 729. ATM 714 uses Name Table 720 to keep track of the mappings of node names to node address and to IP address. The relevance of each of the fields of records 722 in Name Table 720 are explained in the following description of how ATM 714 operates.

In general, Monitor 710 operates as previously described. That is, it passively monitors all packet traffic over segment 702 and sends all packets to RTP 712 for parsing. When RTP 712 recognizes an Appletalk packet, it transfers control to ATM 714 which analyzes the packet for the presence of address mapping information.

The operation of ATM 714 is shown in greater detail in the flow diagram of Fig. 38. When ATM 714 receives control from RTP 712, it takes the packet (step 730 and strips off the lower layers of the protocol until it determines whether there is a Name Binding Protocol message inside the packet (step 732). If it is a NBP message, ATM 714 then determines whether it is new name Lookup message (step 734). If it is a new name Lookup message, ATM 714 extracts the name from the message (i.e., the name for which a node address is being requested) and adds the name to the node name field 724 of a record 722 in Name Table 720 (step 736).

If the message is an NBP message but it is not a Lookup message, ATM 714 determines whether it is a Lookup Reply (step 738). If it is a Lookup Reply, signifying that it contains a node name/node address binding, ATM 714 extracts the name and the assigned node address from the message and adds this information to Name Table 720. ATM 714 does this by searching the name fields of records 722 in Name Table 720 until it locates the name. Then, it updates the node address field of the identified record to contain the node address which was extracted from the received NBP packet. ATM 714 also updates time field 729 to record the time at which the message was processed.

After ATM 714 has updated the address field of the appropriate record, it determines whether any records 722 in Name Table 720 should be aged out (step 742). ATM 714 compares the current time to the times recorded in the time fields. If the elapsed time is greater than a preselected time period (e.g. 48 hours), ATM 714 clears the record of all information (step 744). After that, it awaits the next packet from RTP 712.

As ATM 714 is processing each a packet and it determines either that it does not contain an NBP message (step 732) or it does not contain a Lookup Reply message (step 738), ATM 714 branches to step 742 to perform the age out check before going on to the next packet from RTP 712.

The Appletalk to IP gateways provide services that allow an Appletalk Node to dynamically connect to an IP address for communicating with IP nodes. This service extends the dynamic node address mechanism to the IP world for all Appletalk nodes. While the flexibility provided is helpful to the users, the network manager is faced with the problem of not knowing which Appletalk Nodes are currently using a particular IP address and thus, they can not easily track down problems created by the particular node.

ATM 714 can use passive monitoring of the IP address assignment mechanisms to provide the network manager a Name-to-IP address mapping.

If ATM 714 is also keeping IP address information, it implements the additional steps shown in Fig. 39 after completing the node name to node address mapping steps. ATM 714 again checks whether it is an NBP message (step 748). If it is an NBP message, ATM 714 checks whether it is a response to an IP address request (step 750). IP address requests are typically implied by an NBP Lookup request for an IP gateway. The gateway responds by supplying the gateway address as well as an IP address that is assigned to the requesting node. If the NBP message is an IP address response, ATM 714 looks up the requesting node in Name Table 720 (step 752) and stores the IP address assignment in the IP address field of the appropriate record 722 (step 754).

After storing the IP address assignment information, ATM 714 locates all other records 722 in Name Table 720 which contain that IP address. Since the IP address has been assigned to a new node name, those old entries are no longer valid and must be eliminated. Therefore, ATM 714 purges the IP address fields of those records (step 756). After doing this cleanup step, ATM 714 returns control to RTP 712.

Other embodiments are within the following claims. For example, the Network Monitor can be adapted to identify node types by analyzing the type of packet traffic to or from the node. If the node being monitored is receiving mount requests, the Monitor would report that the node is behaving like node a file server. If the node is issuing routing requests, the Monitor would report that the node is behaving like a router. In either case, the network manager can check a table of what nodes are permitted to provide what functions to determine whether the node is authorized to function as either a file server or a router, and if not, can take appropriate action to correct the problem.

APPENDIX I

SNMP MIB Subset Supported

This is the subset of the standard MIB which can be obtained by monitoring.

Refer to RFC 1066 Management Information Base for an explanation on the items which follow.

System group:
none

Interfaces group
ifType
ifPhysAddress
ifOperStatus
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts

Address Translation group
none

IP group
ipForwarding
ipDefaultTTL
ipInReceives
ipInHdrErrors
ipInAddrErrors
ipForwDatagrams
ipReasmReqds
ipFragCreates

IP Address Table
ipAddress
ipAdEntBcastAddr

IP Routing Table
none

ICMP group
icmpInMsgs
icmpInErrors
icmpInDestUnreachs
icmpInTimeExcds
icmpInParmProbs
icmpInSrcQuenchs
icmpInRedirects
icmpInEchoes

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/721,316	09/25/96	MATTAWAY	S

LM51/0420

BRUCE D JOBSE
BOOKSTEIN & KUDIRKA
ONE BEACON STREET
BOSTON MA 02108

EXAMINER	
WALLACE,G	
ART UNIT	**PAPER NUMBER**
2751	5

DATE MAILED: 04/20/98

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 08/721,316	Applicant(s) Mattaway et al.
	Examiner George F. Wallace	Group Art Unit 2751

[X] Responsive to communication(s) filed on *Sept 25, 1996, Dec 22, 1996 and Mar 30, 1998*

[ ] This action is **FINAL.**

[ ] Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle* 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

[X] Claim(s) *1-6* is/are pending in the applicat

Of the above, claim(s) ______ is/are withdrawn from consideration

[ ] Claim(s) ______ is/are allowed.

[X] Claim(s) *1-6* is/are rejected.

[ ] Claim(s) ______ is/are objected to.

[ ] Claims ______ are subject to restriction or election requirement.

Application Papers

[X] See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

[ ] The drawing(s) filed on ______ is/are objected to by the Examiner.

[ ] The proposed drawing correction, filed on ______ is [ ] approved [ ] disapproved.

[X] The specification is objected to by the Examiner.

[ ] The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

[ ] Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

[ ] All [ ] Some* [N] None of the CERTIFIED copies of the priority documents have been

[ ] received.

[ ] received in Application No. (Series Code/Serial Number) ______ .

[ ] received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______

[ ] Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

[X] Notice of References Cited, PTO-892

[X] Information Disclosure Statement(s), PTO-1449, Paper No(s). *3-4*

[ ] Interview Summary, PTO-413

[X] Notice of Draftsperson's Patent Drawing Review, PTO-948

[ ] Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

Part III. DETAILED ACTION

Drawings

1. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required if and when the application is allowed.

Specification Objections

2. The disclosure is objected to because of the following informalities: on pages 2-3 and elsewhere within the specification, references made to patent applications must be updated to reflect their respective Serial and Patent Numbers, insofar as possible; on page 5 line 8, "a such a" appears to have been intended as "such a;" and on page 27 line 25, "Winsoc 1.1" appears to have been intended as "Winsock 1.1."

The above objections are merely illustrative and do not represent all errors contained in the specification. Applicants are required to proof read the specification and make all necessary corrections.

Claim Objections

3. Claims 1-4 are objected to because of the following informalities: Claim 1 appears to read more clearly and consistently if on line 8, applicants inserted --,-- after "means" and "commands." In Claims 2 and 3, "first processor" and "second processor" have no antecedent basis. They would read more clearly if in Claim 1 "processors" were associated with the computer systems claimed. In Claims 1, 3 and 4 "server" is unclear in light of reference to both a "global server"

and a "connection server" on page 35 of the Specification. In Claim 4, "email signal" appears to read more clearly as "email address." In Claim 5, "processing" would read more clearly if applicants specified the functions intended.

The claims have been examined insofar as clarity and reasonable certainty permits. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1-3 and 5-6 are rejected under 35 U.S.C. 102(a) as being anticipated by VocalTec Internet Phone™ Version 2.5 (hereinafter "IPHONE").

IPHONE is Internet telephony software with a graphic user interface that allows real-time Internet voice communication between two computers--having one or more speakers and at least one microphone--via a direct computer-to-computer link using TCP/IP or SLIP/PPP. IPHONE utilizes IRCs (Internet Relay Servers) as Internet Phone Directories to remedy the difficulty arising from identifying another's dynamically assigned IP address, which changes each time a user logs into his or her Internet Service Provider.

As to Claim 1, IPHONE is *a computer program product for use with a computer system having a display and an audio transducer*--it is software inherently for use with the computer systems of two users, with each system having a display, and at least one speaker and microphone.

Moreover, each system is *operatively coupled to other computers and a server over a computer network.* Inherently the systems of each user is connected to the Internet, through which they each are coupled to a plurality of computers and an IRC (Internet Relay Server) server.

IPHONE, *a computer program product*, inherently provides *a computer usable medium* (one or more floppy disks, a CD-ROM, etc...) *having computer readable code means* (executable code) *embodied in the medium.*

Furthermore, IPHONE, *a computer program product*, provides *means, responsive to user input commands, for establishing a point-to-point communications link with another computer over the computer network.* Inherently, IPHONE contains executable code, which when executed, receives a user input (the clicking of the left button of a mouse whose pointer is above a "Quick Dial Button," see Internet Phone Help Index, Using Internet Phone (link), Setting a Quick Dial Button (link)) and establishes a direct (see Readme.txt file, which is bundled with iphone25.exe, § *About The Internet Phone and IRC*, "The actual talk is done directly between the PC's running the Internet Phone, and NOT via the IRC.") point-to-point communications link with another computer over the Internet. And as noted supra, IPHONE utilizes IRCs as Internet Phone Directories to remedy the difficulty arising from identifying another's dynamically assigned IP address, which changes each time a user logs in to his or her Internet Service Provider.

Furthermore, IPHONE, *a computer program product*, provides *means, responsive to audio data from the audio transducer, for transmitting the audio data over the communications link to the other computer*. Inherently, when one of the two users with an established point-to-point communications link speaks into his or her microphone, the analog audio signal is converted by software or hardware means to a digital signal and then sent through the Internet to the computer of the other user.

Lastly, IPHONE provides *means for generating a user-interface through which a user may coact with the computer system*. IPHONE, as *a computer program product*, inherently contains executable code. This code, when executed, generates a plurality of windows with menu bars and icons through which a user fully interacts with the software to fully effectuate Internet telephony through his or her computer system. The user, as noted *supra*, may click the left button of a mouse whose pointer is above a "Quick Dial Button," which initiates and establishes a point-to-point communications link with another computer (inherently, via its IP address) over the Internet.

As to Claim 2, which depends on Claim 1, IPHONE, *a computer program product*, provides, in conjunction with its *means for establishing a point-to-point communication link, program code means, responsive to the network protocol address of a second processor, for establishing a point-to-point communication link between a first processor and a second processor over the computer network.*

Inherently, IPHONE, *a computer program product*, provides program code, which in conjunction with its *means for establishing a point-to-point communication link*, when executed, initiates and establishes, in response to a user clicking the left button of a mouse, whose pointer is above a "Quick Dial Button" (see cite supra) a point-to-point communication link with another's computer, which is either a TCP/IP or SLIP/PPP communication link via the other's IP address over the Internet (see Internet Phone Help Index, Quick Tour (link), 4th page thereof).

As to Claim 3, which depends on Claim 2, IPHONE, *a computer program product*, provides, in conjunction with its *means for establishing a point-to-point communication link*, *program code means for transmitting, from a first processor to a server, a query as to whether a second processor is connected to the computer network*; and *program code means for receiving a network protocol address of the second processor from the server, when the second processor is connected to the computer network.*

IPHONE, *a computer program product*, provides program code, which in conjunction with its *means for establishing a point-to-point communication link,* when executed, inherently transmits, from a first processor to an IRC server, a query as to whether another user, whose identity (name and email address) is contained in a Quick Dial Button, is connected to the IRC network; and program code, which receives another's IP address from an IRC server, when the other is connected to the IRC network.

As to Claim 5, which depends on Claim 1, IPHONE, *a program product*, inherently provides program code means for processing audio data. The analog audio data captured by a microphone is inherently converted to digital format before transmission across the Internet to another user, where it is converted back to analog before directed to one or more speakers.

As to Claim 6, which depends on Claim 5, IPHONE teaches the use of VOCALTEC's VC Card, a voice compression card, by its users to increase the efficiency and quality of communication (see *Internet Phone Help Index*, *Using Internet Phone* (link), *What is Internet Phone* (link), last paragraph).

Claim Rejections - 35 USC § 102/103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 4 is rejected under 35 U.S.C. 102(b) as anticipated by IPHONE or, in the alternative, under 35 U.S.C. 103(a) as obvious over IPHONE.

8. As to Claim 4, which depends on Claim 2, IPHONE provides, in conjunction with its means for establishing a point-to-point communication link, *program code means for receiving a second network protocol address from a second processor over the computer network,* **inherently**; and **appears** to provide *program code means for transmitting an E-mail signal containing a network protocol address from a first processor to a server over a computer network.*

IPHONE, when executed, inherently provides program code means for receiving the IP address from a second processor over the computer network, since a direct Internet connection between the second and first processors is ultimately achieved. However as to the 102/103 issue, it appears likely that IPHONE, when executed, provides program code for transmitting an E-mail signal (E-mail address) containing a network protocol address (IP address) from a first processor (a first user's computer) to a server (an IRC server) over the computer network (the Internet). Clearly, IPHONE allows a first user to query an IRC server to discover whether a particular user is "on-line." A user of IPHONE supplies the program with "user information" including his or her email address, name and other information. When the user "logs on" to an IRC server, inherently the user's IP address and some type of identifying information is sent to the server, since another user is able to locate the former user via a query containing some identifying information. An email address is sufficiently unique to be efficient search criteria for locating a specific record (user) against a list of records (users) for identification of whether a particular user is on-line, i.e.) available to receive a "call." It is highly likely that a user's E-mail address is used by IPHONE as search criteria.

Insofar as IPHONE does not use an E-mail address as search criteria, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to have used an E-mail address as unique search criteria for determining whether a user associated with the E-mail address was "on-line." It would have been highly desirable to locate a specific user rather than a plurality of users, arising from use of common search criteria, so that a correct communication link could be established in a minimal amount of time.

Conclusion

9. The following prior art made of record and not relied upon is considered pertinent to applicants' disclosure:

a. Netscape Conference and Cooltalk Meeting Room, www.q5.com. Examiner considers this website, which works in conjunction with the Internet telephony software product Netscape®Cooltalk™, as a potential 102(a)/102(b) bar to applicants' claims and as a highly probative 103(a) reference.

b. Gull, *Re: Getting IP address of PPP-connected Mac*, <jgull-0304951005350001@pm012-11.dialip.mich.net>.
Examiner considers this 103(a) reference as strong motivation to combine with prior art-Internet telephony software, such as Netscape®Cooltalk™, both a central Internet database for the storage and dissemination of dynamically assigned IP addresses of Internet telephony software users wishing to disseminate their IP addresses to others connected to the Internet, as well as program code to operatively interact with said database.

c. Gull, *Re: Internet Phone for Mac?*, <jgull-1704950116450001@pm049-28.dialip.mich.net>.
Examiner considers this 103(a) reference as strong motivation to combine with prior art Internet telephony software both software and/or hardware-based compression means, as well as a central Internet database for the storage and dissemination of the dynamically assigned IP addresses of Internet telephony software users wishing to disseminate their IP addresses to others connected to the Internet, and program code to operatively interact with said database.

10. Please address inquiries concerning this and earlier communications from the examiner to **George F. Wallace**, whose telephone number is **703/305-2277**. Examiner can be reached M-F from 9:00 a.m. to 5:00 p.m. EST.

If attempts to reach the examiner by phone fail, **Eddie P. Chan**, examiner's supervisor, can be reached at **703/305-9712**.

The **fax** number for Art Unit 2751 is **703/308-6606**.

Any inquiry of a general nature or relating to the status of this application should be directed to the **Group receptionist** at **703/305-3900**.

George F. Wallace, J.D.
March 26, 1998

TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700

Notice of References Cited

Application No.	Applicant(s)	
08/721,316	Mattaway et al.	
Examiner	**Group Art Unit**	
George F. Wallace	2751	Page 1 of 1

U.S. PATENT DOCUMENTS

	DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					
K					
L					
M					

FOREIGN PATENT DOCUMENTS

	DOCUMENT NO.	DATE	COUNTRY	NAME	CLASS	SUBCLASS
N						
O						
P						
Q						
R						
S						
T						

NON-PATENT DOCUMENTS

	DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
U	VocalTec Internet Phone (TM) Version 2.5, www.cox.smu.edu/class/mis6386/people/stort/iphone25.exe	02/95
V	Weinberg, Netscape Conference and Cooltalk Meeting Room, www.q5.com	2/22/96
W	Gull, Re: Getting IP address of PPP-connected Mac, <jgull-0304951005350001@pm012-11.dialip.mich.net>	4/03/95
X	Gull, Re: Internet Phone for Mac?, >jgull-1704950116450001@pm049-28.dialip.mich.net>	4/17/95

Form PTO-1449 INFORMATION DISCLOSURE STATEMENT	Docket No.: N0003/7002	Serial No. 08/721,316
	Applicant: Shane D. Mattaway et al.	
	Filed: September 25, 1996	Group:

MAIL ROOM
DEC 23 1996
PAT. & TRADEMARK

U.S. Patent Documents

Ex.		Doc. No.	Date	Name	Class	Subcl.	Filed
DN	*	5400335	3/21/95	Yamada	370	524	
	*	5357571	10/18/94	Banwart	380	21	
	*	5150360	9/22/92	Perlman et al.	370	402	
	*	5204669	4/20/93	Dorfe et al.	340	825.52	
	*	5321813	6/14/94	McMillen et al.	714	798	
	*	5309433	5/3/94	Cidon et al.	370	390	
	*	5291554	3/1/94	Morales	380	5	
	*	5224095	6/29/93	Woest et al.	370	401	
	*	5457738	10/10/95	Sylvan	379	93.23	1/95
	*	5455854	10/3/95	Dilts et al.	379	201	10/93
	*	5465286	11/7/95	Clare et al.	379	34	5/94
	*	5475741	12/12/95	Davis et al.	379	102.06	6/94
	*	5509058	4/16/96	Sestak et al.	379	201	9/93
	*	5524141	6/4/96	Braun et al.	379	93.25	9/94
	*	5432846	7/11/95	Norio	379	266	
	*	5309437	5/3/94	Perlman et al.	370	401	
	*	5430727	7/4/95	Callon	370	401	
	*	5442633	8/15/95	Perkins et al.	370	331	
	*	5463625	10/31/95	Yasrebi	370	401	10/93
	*	5166931	11/24/92	Riddle	370	401	
	*	5452296	9/19/95	Shimizu	370	399	
	*	5469500	11/21/95	Satter et al.	379	201	11/93
	*	5430709	7/4/95	Galloway	370	241	
	*	5479411	12/26/95	Klein	379	88.13	3/93
	*	5533110	7/2/96	Pinard et al.	379	201	11/94

Ex.		Doc. No.							Date	Name	Class	Subcl.	
DW	*	5	0	9	5	4	8	0	3/10/92	Fenner	370	238	
	*	5	5	2	6	4	8	9	6/11/96	Nilakantan et al.	709	228	3/93
	*	5	5	4	6	5	8	2	8/13/96	Brockmeyer et al.	709	300	2/95
	*	5	4	5	7	6	8	3	10/10/95	Robins	370	258	5/93
	*	5	5	4	4	3	0	3	8/6/96	Maroteaux et al.	345	326	11/93
	*	5	5	1	7	4	9	4	5/14/96	Green	370	408	9/94
	*	5	5	2	4	1	1	0	6/4/96	Danneels et al.	709	204	11/94

Foreign Patent Documents

Ex.		Doc. No.							Date	Name	Class	Subcl.	

OTHER DOCUMENTS (including, Author, Title, Date, Pages, Etc.)

Examiner: George Wallace | Date considered 3/20/98

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. An * indicates references that do not require a copy to be provided under 37 C.F.R. §1.98(d) because a copy was previously cited or submitted in a prior application, which is relied upon under 35 U.S.C. §120.

H:\BDJ\N0003\7002\1449.WPD

Form PTO-1449 INFORMATION DISCLOSURE STATEMENT	Docket No.: N0003/7002	Serial No. 08/721,316
	Applicant: Shane D. Mattaway, et al.	
	Filed: September 25, 1996	Group: 2751

OIPE JC44 MAR 30 1998 PATENT & TRADEMARK OFFICE

U.S. Patent Documents

Ex.		Doc. No.	Date	Name	Class	Subcl.	Filed
		5425028	06/13/95	K.H. Britton et al.	370	389	07/16/92

Foreign Patent Documents

Ex.		Doc. No.	Date	Name	Class	Subcl.	Filed
EP	A2	0445402	06/11/91	J.C. Wu			~~23/04/91~~
EP	A2	0556012	18/08/93	H. Wada et al.			~~09/02/93~~
WO		9219054	29/10/92	E. Ferdinand et al.			~~10/04/92~~

OTHER DOCUMENTS (including, Author, Title, Date, Pages, Etc.)

		Internetworking with TCP/IP, Volume I, Second Edition, Principles, Protocols, and Architecture, by Douglas E. Comer.

RECEIVED
APR -2 98
GROUP 2600

Examiner: George Wallace	Date considered 4/16/98

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. An * indicates references that do not require a copy to be provided under 37 C.F.R. §1.98(d) because a copy was previously cited or submitted in a prior application, which is relied upon under 35 U.S.C. §120.

H:\BDJ\N0003\7002\1449FRM2.WPD

OIPE JC25
OCT 2 6 1998
PATENT & TRADEMARK OFFICE

Attorney Docket No. N0003/7002

7/a
LK
10-30-98

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Shane D. Mattaway, et al.
Serial No.: 08/721,316
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: George F. Wallace
Art Unit: 2751

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 20th day of October, 1998

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
Washington, D.C. 20231

AMENDMENT

In response to the Office Action dated April 20, 1998, please amend the above-identified patent application, as follows:

In the Specification

Page 2, line 8, change " XX/XXX,XXX" to -- 08/523,115 --;
line 10, change " XX/XXX,XXX" to -- 60/024,251 --;
line 16, change " XX/XXX,XXX" to -- 08/719,894 --;
line 19, change " XX/XXX,XXX" to -- 08/719,554 --;
line 22, change " XX/XXX,XXX" to -- 08/719,640 --;
Page 3, line 1, change " XX/XXX,XXX" to -- 08/719,891 --;
line 4, change " XX/XXX,XXX" to -- 08/719,898 --.
line 7, change " XX/XXX,XXX" to -- 08/718,911 --.
line 10, change " XX/XXX,XXX" to -- 08/719,639 --.
Page 8, line 5, change "a such" to --such--;

RECEIVED
98 OCT 29 AM 9:45
GROUP 2700

Page 27, line 25, change "Winsoc" to --Winsock--.

Page 28, line 11, change "XX/XXX,XXX" to --08/719,554 --.

Page 39, line 11, change"XX/XXX,XXX" to -- 08/719,891 --.

Page 46, line 23, change "XX/XXX,XXX" to -- 08/719,898 --.

In the Claims

Sub B1

1. (Amended) A computer program product for use with a computer system having a display and an audio transducer, the computer system capable of executing one or more processes and [operatively coupled] connecting to other [computers] processes and a server process over a computer network, the computer program product comprising a computer usable medium having computer readable code means embodied in the medium comprising:

a1

a. program code means for generating a user-interface through which a user may control a first process executing on [coact with] the computer system and coupled to the computer network;

b. program code means for determining the currently assigned network protocol address of the first process upon connection to the computer network;

c. program code means, responsive to the currently assigned network protocol address of the first process, for establishing a communication connection with the server process and for forwarding the assigned network protocol address of the first process and a unique identifier of the first process to the server process upon establishing a communication connection with the server process; and

[b.]d. program code means, responsive to user input commands, for establishing a point-to-point communications [link] with another [computer] process over the computer network[; and].

[c. program code means, responsive to audio data from the audio transducer, for transmitting the audio data over the communication link to the other computer.]

2. (Amended) The computer program product of claim 1 wherein the program code means for establishing a point-to-point communication link further comprises:

[c.1] d.1 program code means, responsive to the network protocol address of a second process [the second processor], for establishing a point-to-point communication link between the first [processor] process and the second [processor] process over the computer network.

3. (Amended) The computer program product of claim 2 wherein the program code means for establishing a point-to-point communication link further comprise:

[c.2] d.2 program code means for transmitting, from the first [processor] process to the server process, a query as to whether the second [processor] process is connected to the computer network; and

[c.3] d.3 program code means for receiving a network protocol address of the second [processor] process from the server process, when the second [processor] process is connected to the computer network.

CK B\

4. (Amended) The computer program product of claim 2 wherein the program code means for establishing a point-to-point communication link further comprises:

[c.2] d.2 program code means for transmitting an E-mail [signal] message containing a network protocol address from the first [processor] process to the server process over the computer network;

[c.3]d.3 program code means for receiving a second network protocol address from the second [processor] process over the computer network.

Please cancel claims 5-6 without prejudice.

Please add the following claims:

Sub B2

7. In a computer system having a display and an audio transducer, the computer system capable of executing one or more processes and communicating with other processes and a server process over a computer network, a method for establishing point-to-point communications with other processes comprising:

A. determining the currently assigned network protocol address of the first process upon connection to the computer network;

B. establishing a communication connection with the server process once the assigned network protocol of the first process is known;

C. forwarding the assigned network protocol address of the first process to the server process upon establishing a communication connection with the server process; and

D. establishing a point-to-point communication with another process over the computer network.

a2

8. The method of claim 7 wherein the program step D comprises:

D.1 transmitting, from the first process to the server process, a query as to whether a second process is connected to the computer network; and

D.2 receiving a network protocol address of the second process from the server process, when the second process is connected to the computer network.

9. The method of claim 7 wherein the program step D comprises:

D.1 transmitting an E-mail message containing a network protocol address from the first process to the server process over the computer network;

D.2 receiving a second network protocol address from a second process over the computer network.

10. A method for establishing a point-to-point communication from a caller process to a callee process over a computer network, the caller process having a user interface and being operatively coupled to the callee process and a server process over the

computer network, the method comprising the steps of:

A. generating an element representing a first communication line;

B. generating an element representing a first callee process;

C. establishing a point-to-point communication link from the caller process to the first callee process, in response to a user associating the element representing the first callee process with the element representing the first communication line.

11. The method of claim 10 wherein step C further comprises the steps of:

C.1 querying the server process as to the on-line status of the first callee process; and

C.2 receiving a network protocol address of the first callee process over the computer network from the server process.

12. The method of claim 10 further comprising the step of:

D. generating an element representing a second communication line.

13. The method of claim 10 further comprising the step of:

E. terminating the point-to-point communication from the caller process to the first callee process, in response to the user disassociating the element representing the first callee process from the element representing the first communication line; and

F. establishing a different point-to-point communication from the caller process to the first callee process, in response to the user associating the element representing the first callee process with the element representing the second communication line.

14. The method of claim 10 further comprising the steps of:

D. generating an element representing a second callee process; and

E. establishing a conference point-to-point communication between the caller process and the first and second callee processes, in response to the user associating the element representing the second callee process with the element representing the first communication line.

15. The method of claim 10 further comprising the step of:

F. removing the second callee process from the conference point-to-point communication in response to the user disassociating the element representing the second callee process from the element representing the first communication line.

16. The method of claim 10 further comprising the steps of:

D. generating an element representing a communication line having a temporarily disabled status; and

E. temporarily disabling the point-to-point communication between the caller process and the first callee process, in response to the user associating the element representing the first callee process with the element representing the communication line having a temporarily disabled status.

17. The method of claim 16 wherein the element generated in step D represents a communication line on hold status.

18. The method of claim 17 wherein the element generated in step D represents a communication line on mute status.

19. The method of claim 10 wherein the caller process further comprises a visual display and the user interface comprises a graphic user interface.

20. The method of claim 19 wherein the user interface is a graphic user interface and the elements generated in steps A and B are graphic elements.

REMARKS

Applicants have carefully considered the Office Action dated April 20, 1998 and the references cited therein. In response, the specification and claims have been amended. New claims 7-20 have been added to more particularly point out and distinctly claim the subject matter which Applicants regard as their invention. Applicants respectfully request reexamination and reconsideration.

Applicants have amended the specification to supply the serial numbers of all patent applications referenced in the specification. In addition, minor grammatical errors have been corrected to over come the Examiner's objections to the specification.

Claims 1-4 have been objected to as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. In response, claims 1-4 has been amended, where appropriate, in a manner which is believed to overcome the objections of the Examiner.

Claims 1-3 and 5-6 have been rejected under 35 USC §102(a) as being anticipated by Vocal Tec Internet Phone Version 2.5 (hereafter "IPHONE"). Prior to discussing the specific amendments to the claims, Applicants would like to briefly discuss the subject invention in light of the rejections.

As stated in the Background of the Invention section of the subject specification, the locating users over a computer network has been difficult without knowing the temporary or dynamically assigned Internet Protocol address of the user. The subject application discloses a client and server system and a protocol in which client processes, upon connection to an Internet Protocol based network, forward their current dynamically assigned Internet Protocol address to a global server which acts as a repository of directory information for all other client processes. In addition, the global server associates with the Internet Protocol address of a particular client process, a unique handle, e.g. the client's e-mail address. With this technique, the on-line status of prospective callees may be determined even though the callee is not currently connected to the network. More specifically, each client process, upon receiving an Internet Protocol address after connection to an IP-based network, automatically and transparently notifies the global server that it is currently on line, its E-mail address and the network protocol address at which the client process may be contacted. Thereafter, the global server monitors the status of the client process and is capable of providing directory information including the Internet Protocol address of the client process to other clients processes who wish to communicate therewith. In order for a WebPhone caller to initiate a point-to-point communication connection with a callee having an unknown Internet Protocol address, the WebPhone caller merely selects either an entry representing the prospective callee from the caller's personal directory or submits a query to the global server process, the query including information identifying the prospective callee. The global server utilizes the handle, e.g. the E-mail address, or other identifier contained in the query, and determines whether the callee is currently connected to the network. If so, the current dynamically assigned Internet Protocol address of the callee is then returned to the caller's WebPhone and a point-to-point communication is initiated. The whole process occurs transparently to the WebPhone caller user.

Conversely, the Vocal Tec IPhone literature cited by the Examiner, as well as the NetScape Cool Talk product utilize servers executing the Internet Relay Chat (IRC) protocol, such protocol provides an impractical solution to the problem of locating a user's dynamically assigned Internet Protocol address. Specifically, the IRC protocol is defined in the Internet Engineer Task Force (IETF) Standard RFC 1459 available at <http://info.internet.isi.edu/in-notes/rfc/files/rfc1459.txt>. Briefly, a typical server adhering to the IRC protocol supports approximately 24 users who are "joined" on an individual "channel". To initiate communications with a callee, a caller has to manually search one or more IRC servers for the desired callee. Specifically, to locate a particular callee, a caller needs to know (1) the server which that callee is connected to and (2) the "channel" or "topic" that callee has "joined". Practically, in order to find a particular individual a prospective callee, the caller would need to know which of many IRC servers around the world the callee frequented in an attempt to connect to the proper IRC server. If the IRC server already had 24 users connected, any attempt to contact that particular IRC server would be rejected until one or more users drop off the server. If connection to the IRC server is established, the caller would need to browse through any "channels" in which the prospective callee may be located.

According to the IRC protocol, there is no field or identifier which "uniquely" identifies an IRC server user. Each user connects to an IRC server using a "nickname" which can be any character string up to nine characters in length. Note that duplicate nicknames are possible. Accordingly, such nicknames are not unique. The IPhone Version 2.5 provides no functionality beyond that of a conventional IRC client. A user is presented with a list of "joined" IRC users from which a selection can be made. Once a nickname is selected from the IRC server, information about the user, including an Internet Protocol address are provided to the selecting party.

In contrast, the present invention provides a global server that can be queried to locate any user anywhere using a known unique identifier or handle, e.g. the user's e-mail address. A perspective caller does not have to go through the time-consuming and annoying task of hunting for the correct IRC server and sifting through all joined users and topics in search of the person to whom he or she wishes to communicate. As disclosed in the specification, a Webphone user merely selects information identifying the user from either a personal directory or the results of a query from the global server to establish a point-to-point communication connection with the desired callee.

Claim 1 has been amended to now recite the above-identified aspects of Applicants' invention. Specifically, claim 1 now recites a computer program product containing program code for "determining the currently assigned network protocol address of the first process upon connection to the computer network" (claim 1, lines 10-12). Claim 1 further recites program code for "establishing a communication connection with the server process and for forwarding the assigned network protocol address of the first process and a unique identifier of the first process to the server process upon establishing a communication with the server" (claim 1, lines 10-17). All client processes whether callers or callees "register" with the server in such a manner. Claim 1, as amended, is neither anticipated nor made obvious in light of the IPhone by Vocal Tec. Specifically, the IPhone does not disclose ore suggest program code means for forwarding to a server process the network protocol address and other information identifying a process once the process is coupled to the network, as now recited in claim 1. Claims 2-4 include all the limitations of claim 1 and are likewise believed to be patentable over the IPhone literature for the same reasons as claim 1.

The Examiner will note that the limitations recited in claim 4 are further refinements of limitation D of claim 1, as amended. Specifically, the subject specification discloses two techniques for establishing a point-to-point communication with another process. A first technique, as described in the specification (pp. 12-14) utilizes a query to the directory server. A second technique contemplates the caller process sending its network protocol address to the prospective callee process directly in an e-mail message, as described in the specification (pp.15-18).

Claims 5-6 have been cancelled, without prejudice.

To more particularly point out and distinctly claim the subject matter which Applicants regard as the invention, new claims 7-20 have been added to the specification. Claims 7-9 include limitation similar to claims 1-4 and are believed patentable for the same reasons. The subject matter of claims 10-20 are directed to a user interface in which establishment of calls, conferencing of parties, transferring of parties among calls and disabling of calls are achieved using elements representing communication lines and parties. Support for these claims can be found in the specification, (pp. 49-58). Applicants respectfully assert that none of the art of record, whether considered singularly or in combination, disclose or suggest the subject matter as recited in claims 10-20.

In light of the foregoing amendments and remarks, the claims are believed allowable over any of the references of record, whether considered singularly or in combination. Accordingly, Applicants believe this application is in condition for allowance and a notice to that effect is respectfully requested. If the Examiner has any questions regarding this amendment or the application in general he is invited to call the Applicants' attorney at the number listed below.

The Commissioner is hereby authorized to charge any fees or credits under 37 C.F.R. §1.16 and 1.17 to our deposit account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse, Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Two Center Plaza
Boston, MA 02108
(617) 367-4600

#6

Attorney Docket No. N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Shane D. Mattaway, et al.
Serial No.: 08/721,316
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: George F. Wallace
Art Unit: 2751

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 20th day of October, 1998

Frances M. Cunningham

Frances M. Cunningham

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir/Madam:

PETITION FOR EXTENSION OF TIME

Please extend the time for response to the Office Action dated April 20, 1998 for three months to and including October 20, 1998. Enclosed is a check in the amount of $950.00 for the extension fee.

The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §1.16 and 1.17 that may be required, or credit any overpayment, to our Deposit Account No. 02-3038.

Respectfully submitted,

10/27/1998 RMAGAT 00000126 08721316
01 FC:117 950.00 OP

Bruce D. Jobse

Bruce D. Jobse, Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Two Center Plaza
Boston, MA 02108
(617) 367-4600

GP- 2751

OIPE JC25 OCT 26 1998 PATENT & TRADEMARK OFFICE

Attorney Docket No. N0003/7002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Shane D. Mattaway, et al.
Serial No.:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	George F. Wallace
Art Unit:	2751

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on the 20th day of October, 1998

Frances M. Cunningham

Frances M. Cunningham

Assistant Commissioner for Patents
Washington, D.C. 20231

RECEIVED 98 OCT 29 AM 9:45 GROUP 2700

Sir/Madam:

Transmitted herewith for filing is the following:

X Amendment
X Three-Month Petition for Extension of Time (fee of $950.00)

The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §§1.16 and 1.17 that may be required, or credit any overpayment, to our Deposit Account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse

Bruce D. Jobse, Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Two Center Plaza
Boston, MA 02108
(617) 367-4600

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address : COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

p5

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/721,316	09/25/96	MATTAWAY S	

LM02/0203

BRUCE D JOBSE
BOOKSTEIN & KUDIRKA
ONE BEACON STREET
BOSTON MA 02108

EXAMINER	
CHAN,E	
ART UNIT	PAPER NUMBER
2751	8

DATE MAILED: 02/03/99

This is a communication from the examiner in charge of your application.

COMMISSIONER OF PATENTS AND TRADEMARKS

1. [x] The communication filed 10-26-98 is informal/non-responsive for the reason(s) checked below and should be corrected. **APPLICANT IS GIVEN ONE MONTH FROM THE DATE OF THIS LETTER OR UNTIL THE EXPIRATION OF THE PERIOD FOR RESPONSE SET IN THE LAST OFFICE ACTION (WHICHEVER IS LONGER) WITHIN WHICH TO CORRECT THE INFORMALITY.**

   a. [ ] The amendment to claim(s) ______, filed ______, fails to comply with the provisions of 37 C.F.R. 1.121 and is accordingly held to be non-responsive. A supplemental paper correcting the informal portions and complying with the rule is required.

   b. [ ] The paper is unsigned. A duplicate paper or ratification, properly signed, is required.

   c. [ ] The paper is signed by ______, who is not of record. A ratification or a new power of attorney with a ratification, or a duplicate paper signed by a person of record, is required.

   d. [ ] The communication is presented on paper which will not provide a permanent copy. A permanent copy, or a request that a permanent copy be made by the Office at applicant's expense, is required, see M.P.E.P. 714.07.

   e. [x] Other See attached pages.

2. [ ] In accordance with applicant's request, **THE PERIOD FOR RESPONSE FROM THE OFFICE ACTION DATED** ______
IS EXTENDED TO RUN ______ **MONTH(S).**
No further extension will be granted unless approved by the Commissioner. 37 C.F.R. 1.136 (b)

3. [ ] Receipt is acknowledged of papers submitted under 35 U.S.C. 119 which papers have been made of record in the file.

4. [ ] Other

PTOL-327 (rev. 10-79)

NOTICE TO APPLICANT

OIPE JC52
MAR 0 8 1999
PATENT & TRADEMARK OFFICE

#9/B
SSK.
4-9-99

AMENDMENT	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, et al.	RECEIVED
Serial No.	08/721,316	
Filed:	September 25, 1996	MAR 10 1999
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION	Group 2700
Examiner:	E. Chan	
Art Unit:	2751	

3/9/99

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)
The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Box Non-Fee Amendment Washington, DC 20231 on March 3, 1999.

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
Washington, D.C. 20231
Box Non-Fee Amendment

In response to the office communication dated February 3, 1999, please amend the above-identified application as follows:

In the Claims:

Sub C1

1. (Twice Amended) A computer program product for use with a computer system having a display and an audio transducer, the computer system capable of executing [one or more processes] <u>a first process</u> and connecting to other processes and a server process over a computer network, the computer program product comprising a computer usable medium having computer readable code means embodied in the medium comprising:

   a. program code [means] for generating a user-interface <u>enabling</u> [through which a user may] control a first process executing on the computer system [and coupled to the computer network];

   b. program code [means] for determining the currently assigned network protocol address of the first process upon connection to the computer network;

79

c. program code [means,] responsive to the currently assigned network protocol address of the first process, for establishing a communication connection with the server process and for forwarding the assigned network protocol address of the first process and a unique identifier of the first process to the server process upon establishing a communication connection with the server process; and

d. program code means, responsive to user input commands, for establishing a point-to-point communications with another process over the computer network.

2. (Twice Amended) The computer program product of claim 1 wherein the program code [means] for establishing a point-to-point communication link further comprises:

d.1 program code [means], responsive to the network protocol address of a second process, for establishing a point-to-point communication link between the first process and the second process over the computer network.

3. (Twice Amended) The computer program product of claim 2 wherein the program code [means] for establishing a point-to-point communication link further comprise:

d.2 program code [means] for transmitting, from the first process to the server process, a query as to whether the second process is connected to the computer network; and

d.3 program code means for receiving a network protocol address of the second process from the server process, when the second process is connected to the computer network.

4. (Twice Amended) The computer program product of claim 2 wherein the program code [means] for establishing a point-to-point communication link further comprises:

c2

B1

d.2 program code means for transmitting an E-mail message containing a network protocol address from the first process to the server process over the computer network;

d.3 program code means for receiving a second network protocol address from the second process over the computer network.

Sub B3 ~~7~~. (Amended) In a computer system having a display and an audio transducer, the computer system capable of executing [one or more processes] a first process and communicating with other processes and a server process over a computer network, a method for establishing point-to-point communications with other processes comprising:

A. determining the currently assigned network protocol address of the first process upon connection to the computer network;

B. establishing a communication connection with the server process once the assigned network protocol of the first process is known;

B2.

C. forwarding the assigned network protocol address of the first process to the server process upon establishing a communication connection with the server process; and

D. establishing a point-to-point communication with another process over the computer network.

6 ~~8~~. The method of claim 5 ~~7~~ wherein the program step D comprises:

D.1 transmitting, from the first process to the server process, a query as to whether a second process is connected to the computer network; and

D.2 receiving a network protocol address of the second process from the server process, when the second process is connected to the computer network.

81

~~9~~ 7. The method of claim ~~7~~ 5 wherein the program step D comprises:

D.1 transmitting an E-mail message containing a network protocol address from the first process to the server process over the computer network;

D.2 receiving a second network protocol address from a second process over the computer network.

~~10~~ 8. (Amended) In a computer system having a display and capable of executing a process, a [A] method for establishing a point-to-point communication from a caller process to a callee process over a computer network, the caller process [having] capable of generating a user interface and being operatively [coupled] connected to the callee process and a server process over the computer network, the method comprising the steps of:

22

A. generating [an] a user-interface element representing a first communication line;

B. generating [an] a user interface element representing a first callee process;

C. querying the server process to determine if the first callee process is accessible; and

[C.] D. establishing a point-to-point communication link from the caller process to the first callee process, in response to a user associating the element representing the first callee process with the element representing the first communication line.

~~11~~ 9. The method of claim ~~10~~ 8 wherein step C further comprises the steps of:

C.1 querying the server process as to the on-line status of the first callee process; and

C.2 receiving a network protocol address of the first callee process over the computer network from the server process.

82

10 ~~12~~. (Amended) The method of claim 8 ~~10~~ further comprising the step of:

[D.] E. generating [an] a user-interface element representing a second communication line.

11 ~~13~~. (Amended) The method of claim 8 ~~10~~ further comprising the step of:

[E.] F. terminating the point-to-point communication from the caller process to the first callee process, in response to the user disassociating the element representing the first callee process from the element representing the first communication line; and

[F.] G. establishing a different point-to-point communication from the caller process to the first callee process, in response to the user associating the element representing the first callee [processor] process with the element representing the second communication line.

82

12 ~~14~~. (Amended) The method of claim 8 ~~10~~ further comprising the steps of:

[D.] E. generating [an] a user interface element representing a second callee process; and

[E.] F. establishing a conference point-to-point communication between the caller process and the first and second callee processes, in response to the user associating the element representing the second callee process with the element representing the first communication line.

13 ~~15~~. (Amended) The method of claim 8 ~~10~~ further comprising the step of:

[F.] G. removing the second callee process from the conference point-to-point communication in response to the user disassociating the element representing the second callee process from the element representing the first communication line.

14 ~~16~~. (Amended) The method of claim 8 ~~10~~ further comprising the steps of:

[D.] E. generating [an] a user interface element representing a communication line having a temporarily disabled status; and

[E.] F. temporarily disabling the point-to-point communication between the caller process and the first callee process, in response to the user associating the element representing the first callee process with the element representing the communication line having a temporarily disabled status.

15 ~~17~~. (Amended) The method of claim 14 ~~16~~ wherein the element generated in step [D] E represents a communication line on hold status.

B2

16 ~~18~~. (Amended) The method of claim 15 ~~17~~ wherein the element generated in step [D] E represents a communication line on mute status.

17 ~~19~~. (Amended) The method of claim 8 ~~10~~ wherein the [caller process] display further comprises a visual display [and the user interface comprises a graphic user interface].

18 ~~20~~. (Amended) The method of claim 17 ~~19~~ wherein the user interface is a graphic user interface and the user-interface elements generated in steps A and B are graphic elements.

Remarks

Applicants have considered carefully the Office communication dated February 3, 1999 (Paper No. 8). In response, Applicants have made minor amendments to the claims and set forth the following remarks to supplement the response submitted on October 26, 1999.

The preambles of claims 1 and 7 have been amended to provide proper antecedent basis for all terms used in the claims. In addition, claims 1-4 have been amended to eliminate the term "means" from the claim language. These amendments are offered to conform the claims to 35 U.S.C. §112 and are not necessitated or made in response to any rejection by the Examiner, or, in light of any reference cited by the Examiner.

Claims 1-4 were originally filed with the application and amended in the response of October 26, 1998. Remarks distinguishing claims 1-4 over the cited references are set forth in detail in the prior response of October 26, 1998.

Claims 7-9 include limitation similar to claims 1-4 and are believed patentable for the same reasons as claims 1-4, as set forth in the Remarks section of the previous response. Specifically, claim 7 recites a method for establishing a point-to-point communication comprising the step of "determining the currently assigned network protocol address of the first process upon connection to the computer network" (claim 7, lines 6-7). Claim 7 further recites the steps of "establishing a communication connection with the server process once the assigned network protocol address of the first process is know " (claim 7, lines 8-9) and " forwarding the assigned network protocol address of the first process to the server process upon establishing a communication with the server" (claim 7, lines 10-12). Claim 7, as amended, is believed neither anticipated nor made obvious in light of the IPhone by Vocal Tec. Specifically, the IPhone literature does not disclose or suggest a method comprising the steps of i) determining the currently assigned network protocol address of the first process upon connection to the computer network, ii) establishing a communication connection with the server process once the assigned network protocol address of the first process is know; and iii) forwarding the assigned network protocol address of the first process to the server process upon establishing a communication with the, as now recited in claim 7. Claims 8-9 include all the limitations of claim 7 and are likewise believed to be patentable over the IPhone literature for the same reasons as claim 7.

In addition to claims 1-4 as originally filed, the Summary of the Invention section of the specification (pages 5-6) set forth embodiments of the invention. The specification discloses a client/server system, including a client process having a user interface which is capable of interacting with a directory server process and establishing point-to-point communication connections with other processes over a computer network. Claims 1-4, as amended, are computer program product claims which recite program code limitations for performing the client functions as disclosed. Claims 7-9 are method limitation counterparts to the program code limitations recited in claims 1-4.

Claims 10-20 are directed to a method for establishing various point-to-point communications with a client process utilizing a graphic user interface.

The subject application discloses a client and server system and a protocol in which client processes, upon connection to an Internet Protocol based network, forward their current dynamically assigned network protocol address to a global server which acts as a repository of directory information for all other client processes. The global server associates with the network protocol address of a particular client process, a unique handle, e.g. the client's e-mail address. With this technique, the on-line status of prospective callees may be determined even though the callee is not currently connected to the network.

The subject matters of claims 10-20 are directed to a method performed by a caller process having a user interface to establishment of calls, conferencing of parties, transferring of parties among calls and disabling of calls are achieved using elements representing communication lines and parties.

Applicants respectfully assert that none of the art of record, whether considered singularly or in combination, disclose or suggest the subject matter as recited in claims 10-20. Specifically, claim 10 recites a method for establishing a point-to-point communication from a caller process to a callee process with a caller process capable of generating a user interface. Claim 10 specifically recites the method step of generating a user interface element representing a first communication line, generating a user interface element representing a first callee process, querying the server process to determine if the first callee process is accessible, and establishing a point-to-point communication link from the caller process to the callee process in response to a user associating the element representing the first callee process with the element representing the first communication line (claim 10, lines 7-12). The IPhone literature from Vocal Tec does not disclose or suggest a method including the step of querying a server process to determine the availability of another process and establishing a communication with the callee process by manipulating user interface elements, as now recited in claim 10.

As discussed in the previous response, the Vocal Tec Internet Phone version 2.5 as well as the NetScape Cool Talk product utilize servers executing the IRC protocol which, for the reasons set forth previously, does not provide a teaching or suggestion as to how to query a server process to determine if a first callee process is accessible, i.e. on-line and current network protocol address. None of the art of record currently are believed to recite the specific limitations of claim 10, as now amended. Claims 11-20 include all the limitations of claim 10 and are likewise believed patentable for the same reasons.

In light of the foregoing amendments to the claims, Applicants respectfully assert that all claims currently under consideration now patentably distinguish over the art of record, including the cited references, whether considered singularly or in combination. The Examiner is respectfully requested to advance this case to issuance and send a notice to that effect. In the event that outstanding issues remain following the Examiner's review of this response, Applicants' attorney requests that the Examiner contact Applicants' attorney at the number listed below to set up a telephone interview to attempt to resolve any outstanding issues with the claims and before any further Office Actions are issued.

The Commissioner is hereby authorized to charge any fees or credits under 37 C.F.R. §1.16 and 1.17 to our deposit account No. 02-3038.

Respectfully submitted

Bruce D. Jobse ________________ Date: 3/3/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

OIPE JC52
MAR 0 8 1999
PATENT & TRADEMARK OFFICE

GAU 2751

AMENDMENT TRANSMITTAL	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, Et Al.
Serial No.	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Chan
Art Unit:	2751

Assistant Commissioner for Patents
Washington, DC 20231
Box Non-Fee Amendment

RECEIVED
MAR 1 0 1999
Group 2700

Transmitted herewith for filing is the following:

Enclosures

- ☒ Amendment
- ☐ Petition for a month Extension of Time
- ☐ Return Receipt Postcard

Small Entity

- ☐ A small entity statement under 37 C.F.R. §1.27 has already been filed.
- ☐ A small entity statement under 37 C.F.R. §1.27 is attached

Fees

Claims as Filed					
	Claims Filed	Highest Number Paid for	Number of Extra Claims	Rate	Additional Fees Due
Total Claims (37 CFR §1.16(c))	18	- 20 =	0 X	\$18.00 =	\$ 0.00
Independent Claims (37 CFR §1.16(b))	3	- 3 =	0 X	\$78.00 =	\$ 0.00
Extension Fee					\$ 0.00
Reduction by 50% for filing by small entity					\$ 0.00
Total Filing Fee					**\$ 0.00**

Payment

☐ Check in the amount of the total filing fee.

☐ Charge Account No. 02-3038 in the amount of the total filing fee. A duplicate of this transmittal sheet is attached.

Authorization to Charge Additional Fees

☒ The Commissioner is hereby authorized to charge any additional fees under 37 C.F.R. §1.16 and §1.17 required by the attached paper and during the entire pendency of this application to Account No. 02-3038.

Bruce D. Jobse ______________________ Date: 3/3/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

UNITED STAT[illegible] [illegible]EPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

021127 LM51/0622
KUDIRKA & JOBSE
TWO CENTER PLAZA
BOSTON MA 02108

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
08/721,316	09/25/96	018	RAMIREZ, E	2757	06/22/99

First Named Applicant MATTAWAY, 35 USC 154(b) term ext. = 0 Days.

TITLE OF INVENTION GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2	709-227.000	U91	UTILITY	NO	$1210.00	09/22/99

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED.

HOW TO RESPOND TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or
B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number.
Please direct all communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

***IMPORTANT REMINDER:** Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.*

PATENT AND TRADEMARK OFFICE COPY

PTOL-85 (REV. 10-96) Approved for use through 06/30/99. (0651-0033)

UNITED STATE, [illegible]EPARTMENT OF COMMERCE
Patent and Tra[illegible]ark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO
08/721,316	09/25/96	MATTAWAY	

EXAMINER

021127 LMS1/0622
KUDIRKA & JOBSE
TWO CENTER PLAZA
BOSTON MA 02108

ART UNIT	PAPER NUMBER

DATE MAILED: 06/22/99

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

NOTICE OF ALLOWABILITY

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to Amendment B filed on 3/8/99.

☒ The allowed claim(s) is/are 1-4, and 7-28.

☐ The drawings filed on ______ are acceptable.

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) ______.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______.

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

☐ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

☐ because the originally filed drawings were declared by applicant to be informal.

☐ including changes required by the Notice of Draftperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. ______.

☐ including changes required by the proposed drawing correction filed on ______, which has been approved by the examiner.

☐ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftperson.

☐ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

☐ Interview Summary, PTO-413

☐ Examiner's Amendment/Comment

☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

☐ Examiner's Statement of Reasons for Allowance

ELLIS B. RAMIREZ
PRIMARY EXAMINER

PTOL-37 (Rev. 10/95)
*U.S. GPO 1997-417-381/62714

1. The response filed on October 26, 1998 is informal or not fully responsive to the prior Office action because of the following omission(s) or matter(s):

Applicants have failed to clearly point out the patentable novelty which they think each of the claims presents, particularly newly added claims 10-20, in view of the state of the art disclosed by the references cited, as required by 37 CFR 1.111.

Applicants are respectfully reminded that they must present arguments pointing out the specific distinctions believed to render the claims, including any newly presented claims, patentable over any applied references. A general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references is not sufficient. See 37 CFR 1.111, as well as MPEP 714.02 and 714.04.

In the present case, despite the substantial differences in claim language, applicants generally state that "none of the art of record ... disclose or suggest the subject matter as recited in claims 10-20" (response at page 10). Applicants only generally discuss claims 10-20 as being directed to a "user interface" and refer to a passage spanning nine pages in the specification as providing support for these claims, but do not discuss the references at all, and do not point out the specific claim language believed to render the claims patentable.

Also, given the differences in claim language, applicants should also point out how the newly added claims are related to the original claims, i.e., why the newly added claims including claims directed to a "method for establishing point to point communications," including steps of generating "elements" and establishing a communication link, are believed to be directed to the same invention as the original claims, which are directed to a computer program product including program code means for generating a user interface, establishing point to point communications, transmitting audio data, etc. [Note that claim 1 appears to provide evidence that the combination of clam 1, including "means for establishing point to point communications," does not require the details of the subcombination (a "method for establishing point to point communications"), for patentability. See MPEP 806.05, as well as MPEP 821.03.]

Since the above-mentioned reply appears to be *bona fide*, but through an apparent oversight or inadvertence failed to provide a complete response, applicant is required to complete the response within a TIME LIMIT of ONE MONTH from the date of this letter. EXTENSIONS OF THIS TIME LIMIT MAY BE GRANTED UNDER EITHER 37 CFR 1.136(a).

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Glenn Gossage whose telephone number is (703) 305-3820.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

GLENN GOSSAGE
PRIMARY EXAMINER
ART UNIT 2751

OIPE JC78 JUL 20 1999 PATENT & TRADEMARK OFFICE

#13/(AE.
c
SSK
11-8-99

AMENDMENT AFTER ALLOWANCE UNDER 37 CFR §1.312(a)	Docket No. N0003/7002

Applicant: Shane D. Mattaway, et al.
Serial No. 08/721,316
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: E. Ramirez
Art Unit: 2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL445948665US
Date of Deposit: **July 20, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, BOX ISSUE FEE, Washington, D.C. 20231.

Frances M. Cunningham

Frances M. Cunningham

OK to enter MMM 11/10/99

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to issuance, Applicants request the above-identified application be amended as follows:

In the Claims

C1

1. (Thrice Amended) A computer program product for use with a computer system having a display [and an audio transducer], the computer system capable of executing a first process and connecting to other processes and a server process over a computer network, the computer program product comprising a computer usable medium having computer readable code means embodied in the medium comprising:

   a. program code for generating a user-interface enabling control a first process executing on the computer system;

b. program code for determining the currently assigned network protocol address of the first process upon connection to the computer network;

c. program code responsive to the currently assigned network protocol address of the first process, for establishing a communication connection with the server process and for forwarding the assigned network protocol address of the first process and a unique identifier of the first process to the server process upon establishing a communication connection with the server process; and

c1

d. program code [means], responsive to user input commands, for establishing a point-to-point communications with another process over the computer network.

3. (Thrice Amended) The computer program product of claim 2 wherein the program code for establishing a point-to-point communication link further comprise:

d.2 program code for transmitting, from the first process to the server process, a query as to whether the second process is connected to the computer network; and

C2

d.3 program code [means] for receiving a network protocol address of the second process from the server process, when the second process is connected to the computer network.

4. (Thrice Amended) The computer program product of claim 2 wherein the program code for establishing a point-to-point communication link further comprises:

d.2 program code [means] for transmitting an E-mail message containing a network protocol address from the first process to the server process over the computer network;

d.3 program code [means] for receiving a second network protocol address from the second process over the computer network.

5

~~7.~~ (Twice Amended) In a computer system having a display [and an audio transducer], the computer system capable of executing a first process and communicating with other processes and a server process over a computer network, a method for establishing point-to-point communications with other processes comprising:

A. determining the currently assigned network protocol address of the first process upon connection to the computer network;

B. establishing a communication connection with the server process once the assigned network protocol of the first process is known;

C. forwarding the assigned network protocol address of the first process to the server process upon establishing a communication connection with the server process; and

D. establishing a point-to-point communication with another process over the computer network.

Remarks

This application is currently under Allowance. A Notice of Allowance dated June 22, 1999 was mailed indicating that claims 1-4 and 7-20 are allowed. Applicants submit this Amendment to resolve minor informalities in the claim language.

Applicants have amended claims 1 and 7 to eliminate superfluous language. Specifically, the phrase "and an audio transducer" provided a basis for limitations recited in claims 5-6, previously cancelled. This term does not occur elsewhere in claims 1-4 and should be deleted. A similar change has been made to claim 7. The phrase "and an audio transducer" does not occur elsewhere in claims 7-9 and should be deleted. In the previous response mailed March 3,1999, claims 1-4 were amended to eliminate the term "means" from the claim language, however, several occurrences were overlooked. Applicant's submit additional amendments to claims 1, 3 and 4 to eliminate the term "means" from the claim language. These amendments are offered to conform the claims to 35 U.S.C. §112, 2nd paragraph, and are not necessitated or made in response to any rejection by the Examiner, or, in light of any reference cited by the Examiner.

No new matter or substantive issues are believed raised by this amendment. In light of the foregoing amendments and remarks, this application is now believed in condition for issuance and the Examiner is respectfully requested to advance this application to issuance. If the Examiner has any further questions regarding this Amendment, he is invited to call Applicants' attorney at the number listed below.

The Commissioner is hereby authorized to charge any fees or credits under 37 C.F.R. §1.16 and 1.17 to our deposit account No. 02-3038.

Respectfully submitted

Bruce D. Jobse ____________________ Date: 7/20/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

B

OIPE JC78
JUL 20 1999
PATENT & TRADEMARK OFFICE

AMENDMENT TRANSMITTAL	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, et al.
Serial No.	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

RECEIVED
JUL 23 1999
Publishing Division
05

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL445948665US
Date of Deposit: July 20, 1999

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, Box Issue Fee, Washington, D.C. 20231.

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
BOX ISSUE FEE
Washington, DC 20231

RECEIVED
JUL 30 1999
Publishing Division
Corres/Allowed Files (05)

Transmitted herewith for filing is the following:

Enclosures

- ☒ Amendment After Allowance
- ☐ Petition for a month Extension of Time
- ☒ Return Receipt Postcard

Small Entity

- ☐ A small entity statement under 37 C.F.R. §1.27 has already been filed.
- ☐ A small entity statement under 37 C.F.R. §1.27 is attached

Fees

Claims as Filed					
	Claims Filed	Highest Number Paid for	Number of Extra Claims	Rate	Additional Fees Due
Total Claims (37 CFR §1.16(c))	18	- 20 =	0 X	$18.00 =	$ 0.00
Independent Claims (37 CFR §1.16(b))	3	- 3 =	0 X	$78.00 =	$ 0.00
Extension Fee					$ 0.00
Reduction by 50% for filing by small entity					$ 0.00
Total Filing Fee					**$ 0.00**

Payment

☐ Check in the amount of the total filing fee.

☐ Charge Account No. 02-3038 in the amount of the total filing fee. A duplicate of this transmittal sheet is attached.

Authorization to Charge Additional Fees

☒ The Commissioner is hereby authorized to charge any additional fees under 37 C.F.R. §1.16 and §1.17 required by the attached paper and during the entire pendency of this application to Account No. 02-3038.

Bruce D. Jobse Date: 7/20/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

PART B—ISSUE FEE TRANSMITTAL

Complete and mail this form, together with applicable fees, to: **Box ISSUE FEE**
Assistant Commissioner for Patents
Washington, D.C. 20231

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Issue Fee Receipt, the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

021127
KUDIRKA & JOBSE
TWO CENTER PLAZA
BOSTON MA 02108

AUG 0 4 1999

Note: The certificate of mailing below can only be used for domestic mailings of the Issue Fee Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing.

Certificate of Mailing

I hereby certify that this Issue Fee Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Box Issue Fee address above on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
08/721,316	09/25/96	018	RAMIREZ, E	2757	06/22/99

First Named Applicant MATTAWAY, 35 USC 154(b) term ext. = 0 Days.

TITLE OF INVENTION GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 N0003/7002	709-227.000	U91	UTILITY	NO	$1210.00	09/22/99

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363). Use of PTO form(s) and Customer Number are recommended, but not required.

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47) attached.

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 **KUDIRKA & JOBSE, LLP**
2 ____
3 ____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropiate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a subsitiue for filing an assignment.

(A) NAME OF ASSIGNEE
NetSpeak Corporation
(B) RESIDENCE: (CITY & STATE OR COUNTRY)
Boca Raton, Florida

Please check the appropriate assignee category indicated below (will not be printed on the patent)
☐ individual ☒ corporation or other private group entity ☐ government

4a. The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):
☒ Issue Fee
☒ Advance Order - # of Copies 10

4b. The following fees or deficiency in these fees should be charged to:
DEPOSIT ACCOUNT NUMBER ____
(ENCLOSE AN EXTRA COPY OF THIS FORM)
☐ Issue Fee
☐ Advance Order - # of Copies ____

The COMMISSIONER OF PATENTS AND TRADEMARKS IS requested to apply the Issue Fee to the application identified above.

(Authorized Signature) Bruce D. Jobse (Date) 8/4/99

NOTE; The Issue Fee will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending on the needs of the individual case. Any comments on the amount of time required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND FEES AND THIS FORM TO: Box Issue Fee, Assistant Commissioner for Patents, Washington D.C. 20231

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

RECEIVED
AUG 0 6 1999
Publishing Division
16

08/06/1999 TTRAN2 00000017 08721316
01 FC:142 1210.00 OP
02 FC:561 30.00 OP

TRANSMIT THIS FORM WITH FEE

PTOL-85B (REV.10-96) Approved for use through 06/30/99. OMB 0651-0033

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

KS 7580 7/29/99 B $

ISSUE FEE TRANSMITTAL	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, et al.
Serial No.	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

AUG 04 1999

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL107667370US
Date of Deposit: **August 4, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, BOX ISSUE FEE, Washington, D.C. 20231.

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
Box Issue Fee
Washington, D.C. 20231

In response to the Notice of Allowance and Base Issue Fee Due dated June 22, 1999 for the above-identified application, enclosed are the following documents (indicated by a checked box):

Documents

- ☒ Issue Fee Transmittal
- ☐ Letter to Official Draftsperson accompanied by formal drawings of Figures 1-20D comprising drawing sheets.
- ☒ Advance order of 10 soft copies of letters patent

Small Entity

- ☐ A small entity statement under 37 C.F.R. §1.27 has already been filed.
- ☐ A small entity statement under 37 C.F.R. §1.27 is attached.
- ☐ Small entity status is no longer claimed.

Payment

- ☒ A check in the amount of **$1,240.00** is enclosed to cover the issue fee due and advance order of patent copies.
- ☐ The Commissioner is hereby authorized to charge any fees under 37 C.F.R. 1.16-1.19 to Deposit Account No. 02-3038. A duplicate of this sheet is attached.

The Commissioner is hereby authorized to charge any additional fees under 37 C.F.R. §§1.16-1.19 that may be required, or credit any overpayment, to Deposit Account No. 02-3038.

Bruce D. Jobse ______________________ Date: 8/4/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

7530
9/1/99

95

OIPE JC16
AUG 2 4 1999
PATENT & TRADEMARK OFFICE

B

#11
SSK
10-13-99

TRANSMITTAL LETTER	Docket No. N0003/7002

Applicant: Shane D. Mattaway, et al.
Serial No. 08/721,316
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: E. Ramirez
Art Unit: 2757

RECEIVED
AUG 2 7 1999
Publishing Division

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL401821635US
Date of Deposit: **August 24, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, Box Issue Fee, Washington, D.C. 20231.

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
Box Issue Fee
Washington, D.C. 20231

Enclosures

- ☐ Affidavit under 37 C.F.R. 1.131
- ☐ Assignment Papers
- ☐ Change of Correspondence Address
- ☐ Extension of Time Request
- ☐ Declaration/Power of Attorney
- ☐ Fee Transmittal Form
- ☐ Information Disclosure Statement
- ☐ Invention Disclosure Document
- ☐ Notice of Appeal
- ☐ Petition and Petition Routing Slip
- ☐ Power of Attorney Form
- ☐ PTO-1449 Form(s)
- ☐ Request for Certified Copies
- ☐ Request for Reconsideration
- ☐ Request for Refund
- ☐ Response to Missing Parts
- ☒ Return Receipt Postcard
- ☒ 27 Sheets Formal Drawing(s)
- ☐ Small Entity Statement
- ☐ Status Letter
- ☐ Terminal Disclaimer
- ☒ Letter to Official Draftsperson

Bruce D. Jobse

Date: 8/24/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

OIPE JC16
AUG 24 1999
PATENT & TRADEMARK OFFICE

LETTER TO OFFICIAL DRAFTSPERSON	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, et al.
Serial No	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL401821635US
Date of Deposit: August 24, 1999

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, Box Issue Fee, Washington, D.C. 20231.

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
BOX ISSUE FEE
Washington, DC 20231

1. Upon approval of the Examiner in charge of the above-identified application, please substitute the enclosed drawing sheets containing formal versions of Figures 1-20D for the corresponding drawing sheets currently in the application.

2. The Commissioner is hereby authorized to charge any other fees under 37 CFR §1.16 and §1.17 that may be required, or credit any overpayment, to our Deposit Account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse Date: 8/24/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

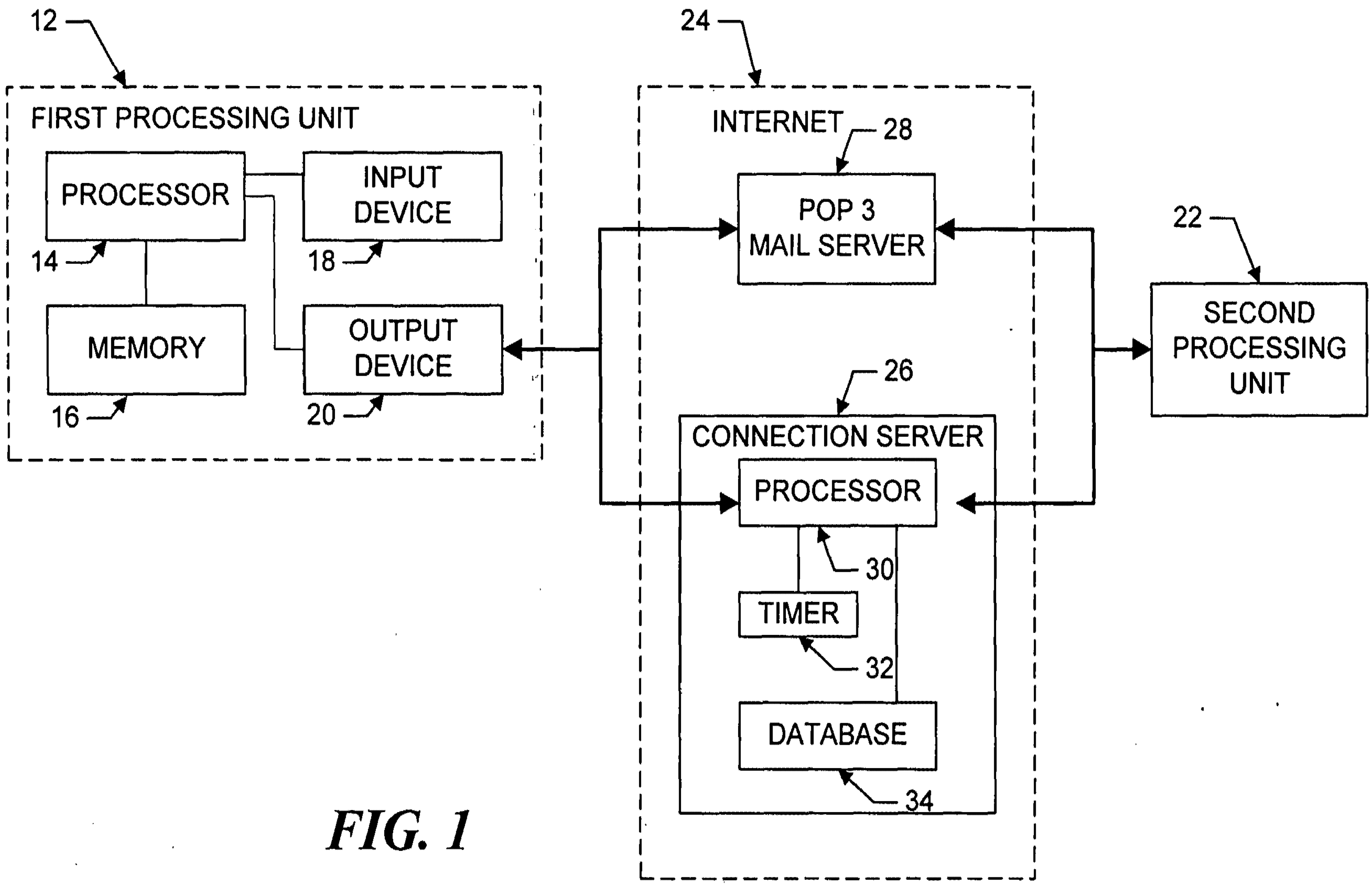

12
FIRST PROCESSING UNIT
PROCESSOR
14
INPUT DEVICE
18
MEMORY
16
OUTPUT DEVICE
20
24
INTERNET
28
POP 3 MAIL SERVER
26
CONNECTION SERVER
PROCESSOR
30
TIMER
32
DATABASE
34
22
SECOND PROCESSING UNIT

FIG. 1

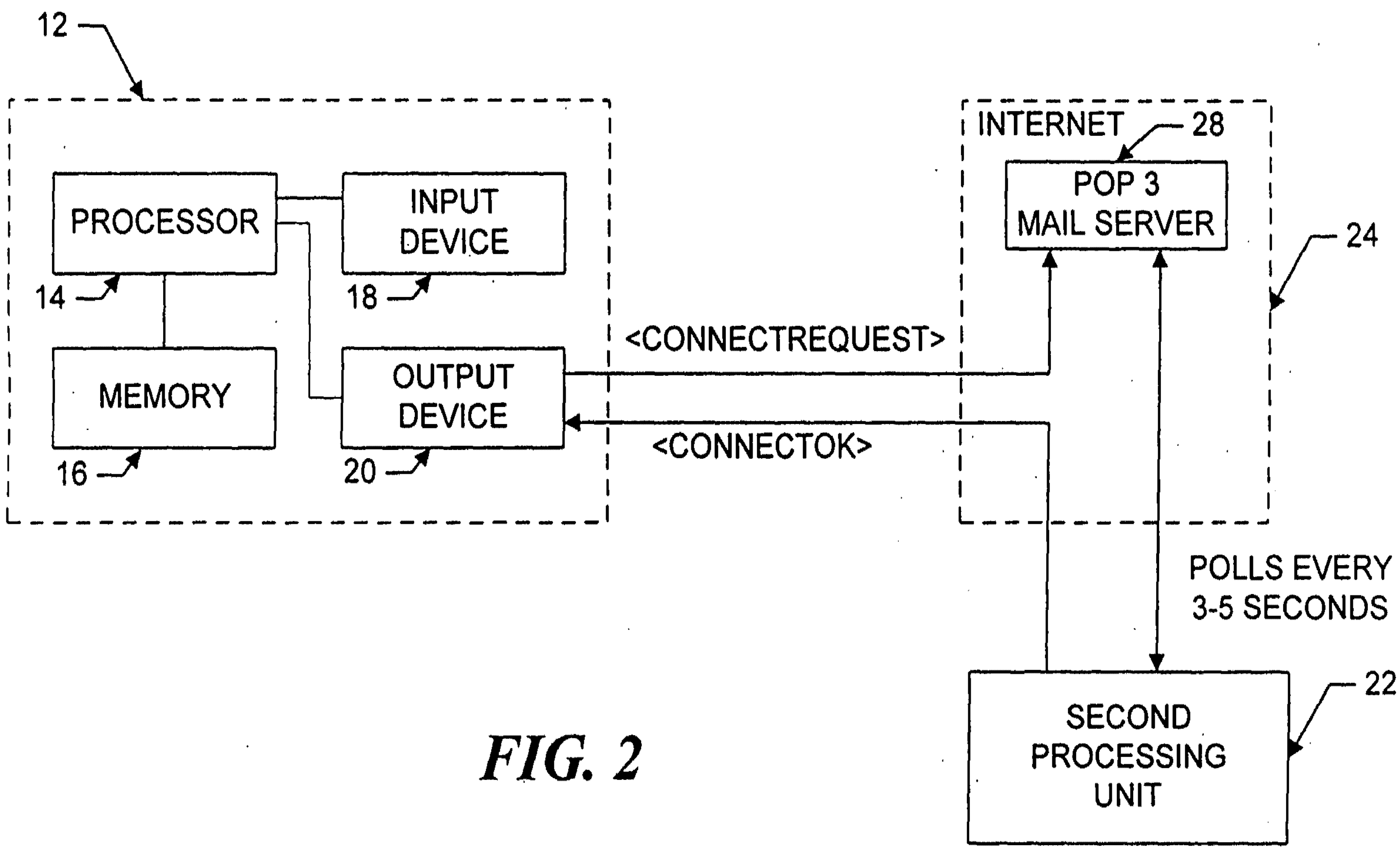

12
PROCESSOR
14
INPUT DEVICE
18
MEMORY
16
OUTPUT DEVICE
20
<CONNECTREQUEST>
<CONNECTOK>
INTERNET
28
POP 3 MAIL SERVER
24
POLLS EVERY 3-5 SECONDS
22
SECOND PROCESSING UNIT

FIG. 2

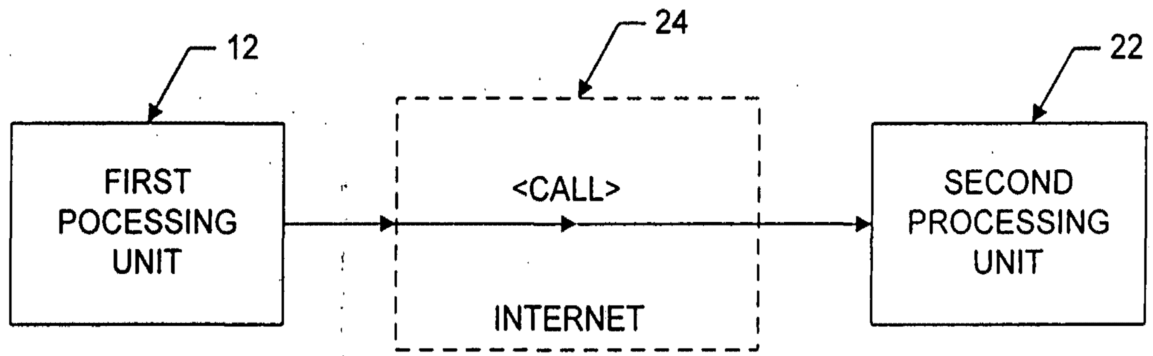

12
24
22
FIRST
POCESSING
UNIT
<CALL>
INTERNET
SECOND
PROCESSING
UNIT

FIG. 3

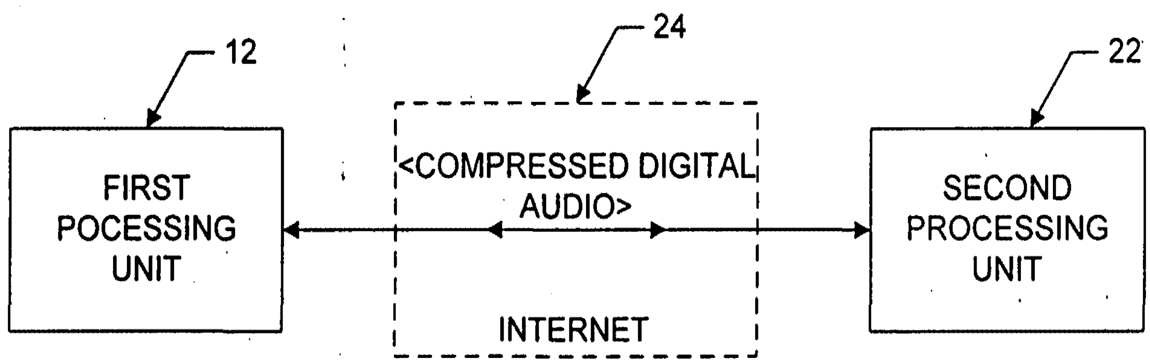

12
24
22
FIRST
POCESSING
UNIT
<COMPRESSED DIGITAL
AUDIO>
INTERNET
SECOND
PROCESSING
UNIT

FIG. 4

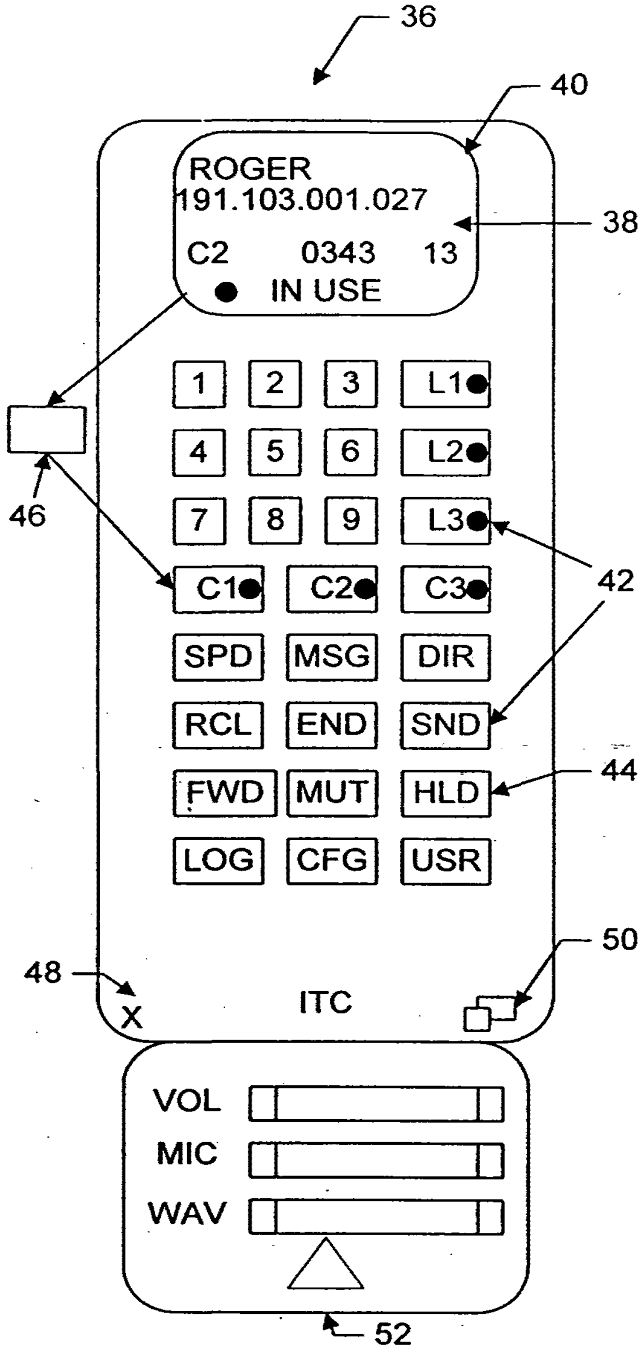

36
40
ROGER
191.103.001.027
38
C2 0343 13
IN USE
1 2 3 L1
4 5 6 L2
7 8 9 L3
46
C1 C2 C3
42
SPD MSG DIR
RCL END SND
FWD MUT HLD
44
LOG CFG USR
48
50
X
ITC
VOL
MIC
WAV
52

FIG. 5

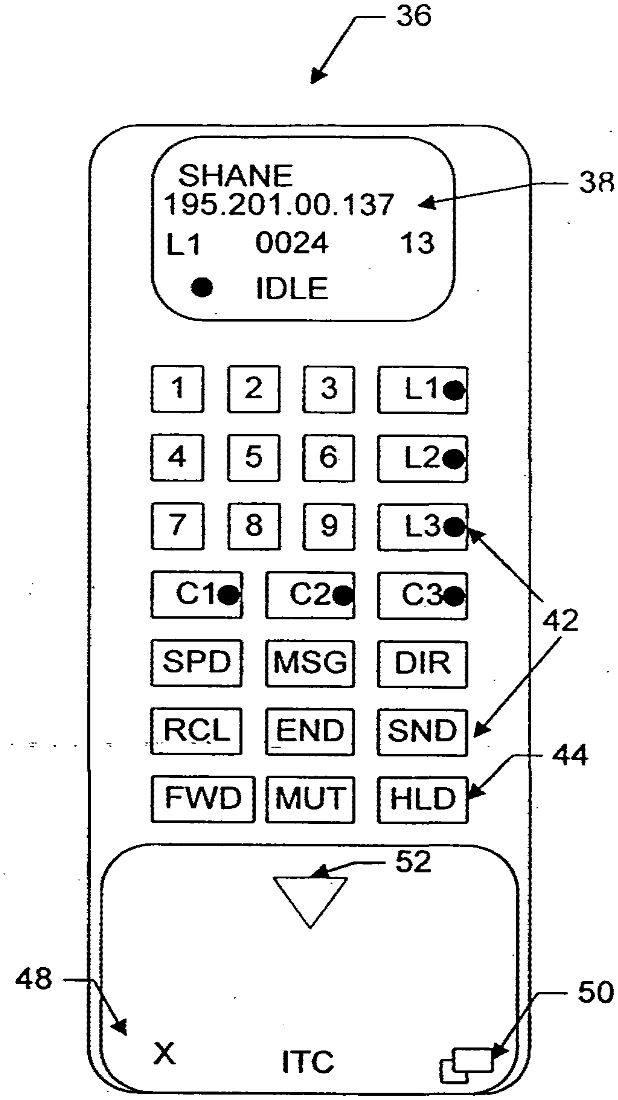
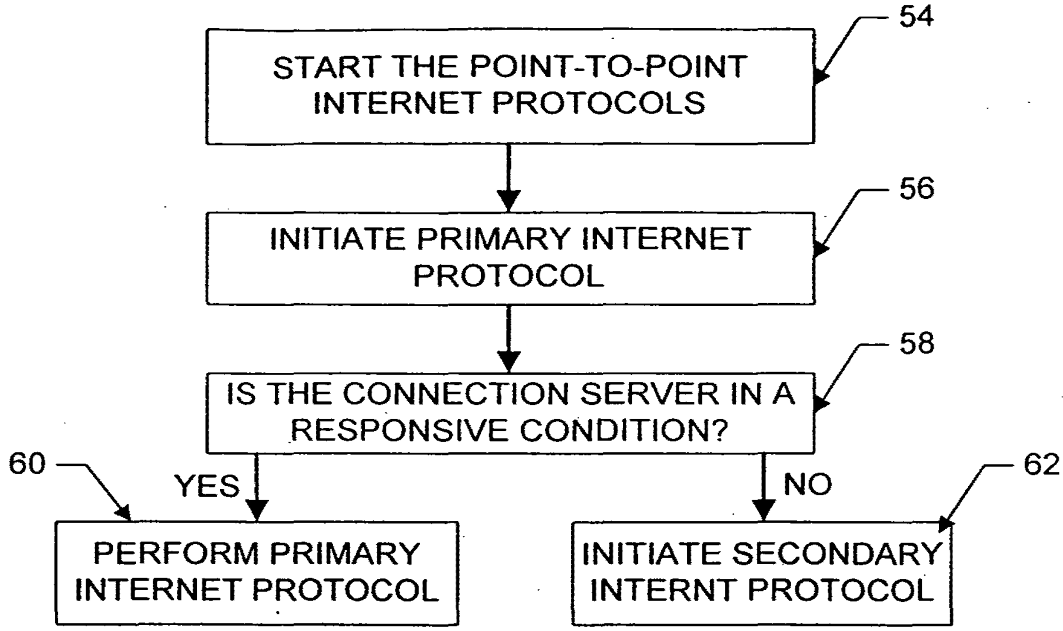
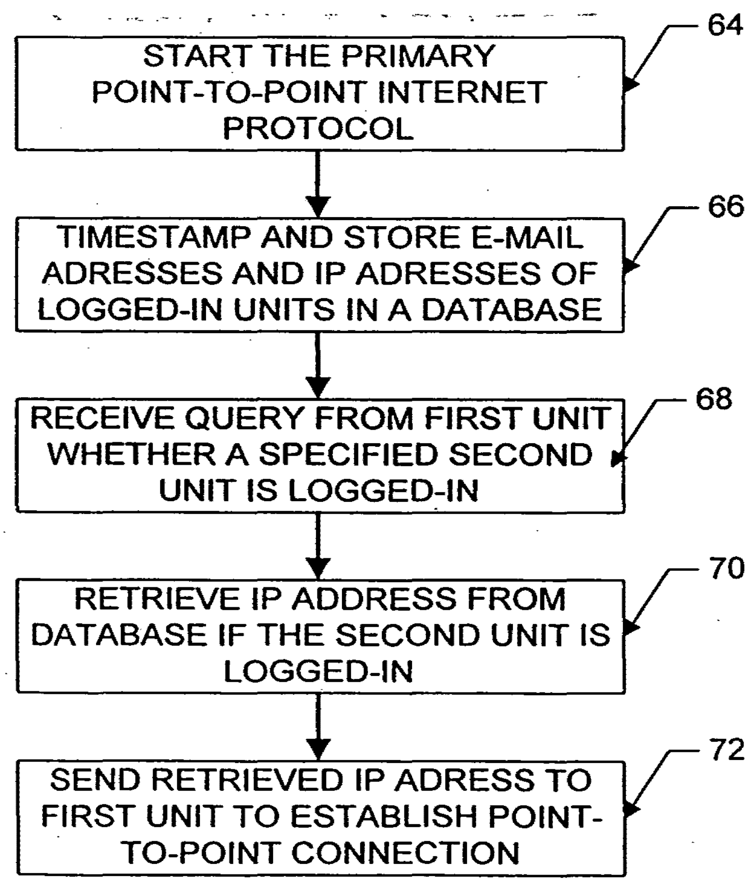

36
SHANE
195.201.00.137
38
L1 0024 13
IDLE
1 2 3 L1
4 5 6 L2
7 8 9 L3
C1 C2 C3
42
SPD MSG DIR
RCL END SND
FWD MUT HLD
44
52
48
50
X
ITC

FIG. 6



54
START THE POINT-TO-POINT INTERNET PROTOCOLS
56
INITIATE PRIMARY INTERNET PROTOCOL
58
IS THE CONNECTION SERVER IN A RESPONSIVE CONDITION?
60
YES
NO
62
PERFORM PRIMARY INTERNET PROTOCOL
INITIATE SECONDARY INTERNT PROTOCOL

FIG. 7



64
START THE PRIMARY POINT-TO-POINT INTERNET PROTOCOL
66
TIMESTAMP AND STORE E-MAIL ADRESSES AND IP ADRESSES OF LOGGED-IN UNITS IN A DATABASE
68
RECEIVE QUERY FROM FIRST UNIT WHETHER A SPECIFIED SECOND UNIT IS LOGGED-IN
70
RETRIEVE IP ADDRESS FROM DATABASE IF THE SECOND UNIT IS LOGGED-IN
72
SEND RETRIEVED IP ADRESS TO FIRST UNIT TO ESTABLISH POINT-TO-POINT CONNECTION

FIG. 8

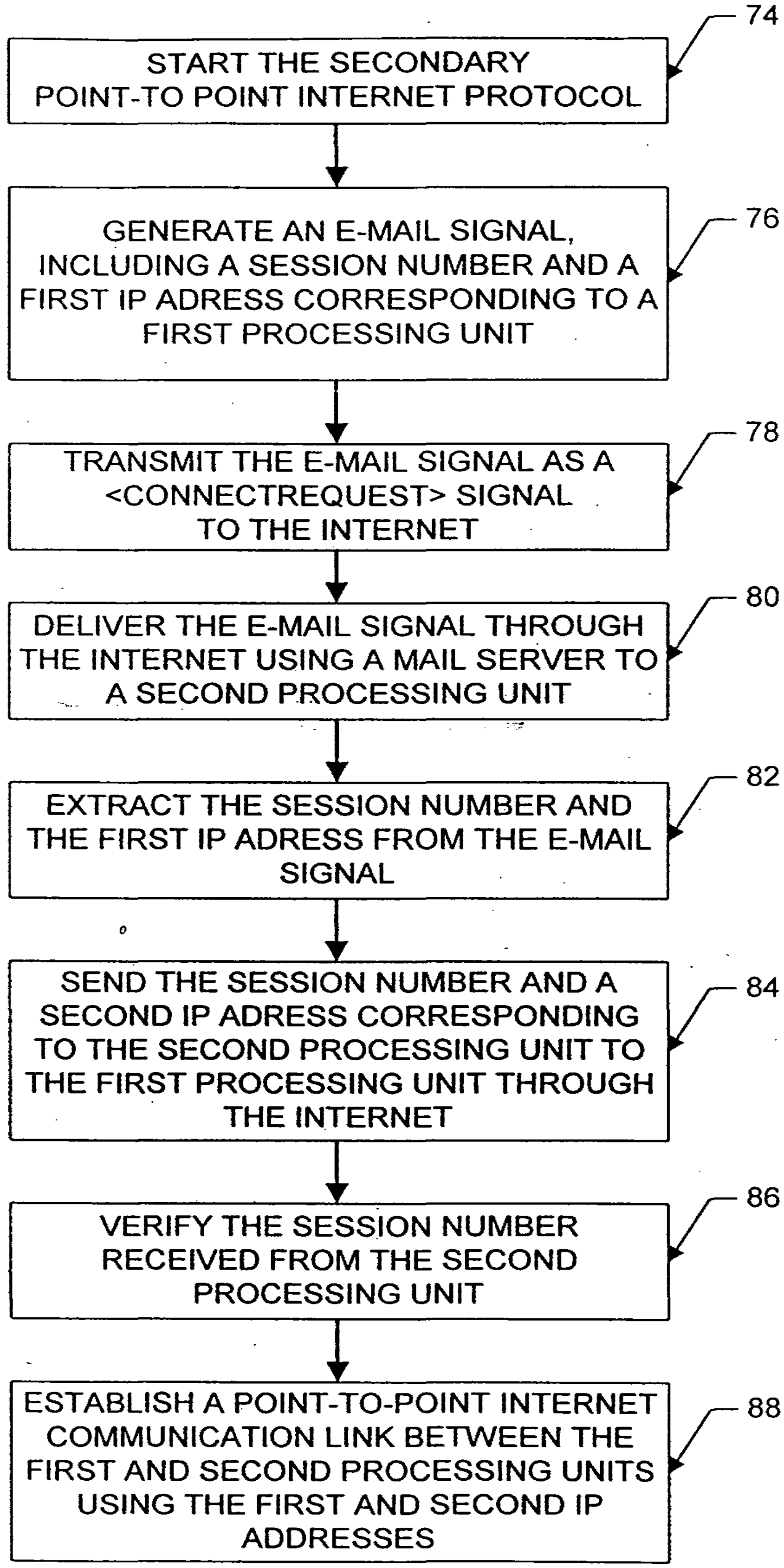

74
START THE SECONDARY POINT-TO POINT INTERNET PROTOCOL
76
GENERATE AN E-MAIL SIGNAL, INCLUDING A SESSION NUMBER AND A FIRST IP ADRESS CORRESPONDING TO A FIRST PROCESSING UNIT
78
TRANSMIT THE E-MAIL SIGNAL AS A <CONNECTREQUEST> SIGNAL TO THE INTERNET
80
DELIVER THE E-MAIL SIGNAL THROUGH THE INTERNET USING A MAIL SERVER TO A SECOND PROCESSING UNIT
82
EXTRACT THE SESSION NUMBER AND THE FIRST IP ADRESS FROM THE E-MAIL SIGNAL
84
SEND THE SESSION NUMBER AND A SECOND IP ADRESS CORRESPONDING TO THE SECOND PROCESSING UNIT TO THE FIRST PROCESSING UNIT THROUGH THE INTERNET
86
VERIFY THE SESSION NUMBER RECEIVED FROM THE SECOND PROCESSING UNIT
88
ESTABLISH A POINT-TO-POINT INTERNET COMMUNICATION LINK BETWEEN THE FIRST AND SECOND PROCESSING UNITS USING THE FIRST AND SECOND IP ADDRESSES

FIG. 9

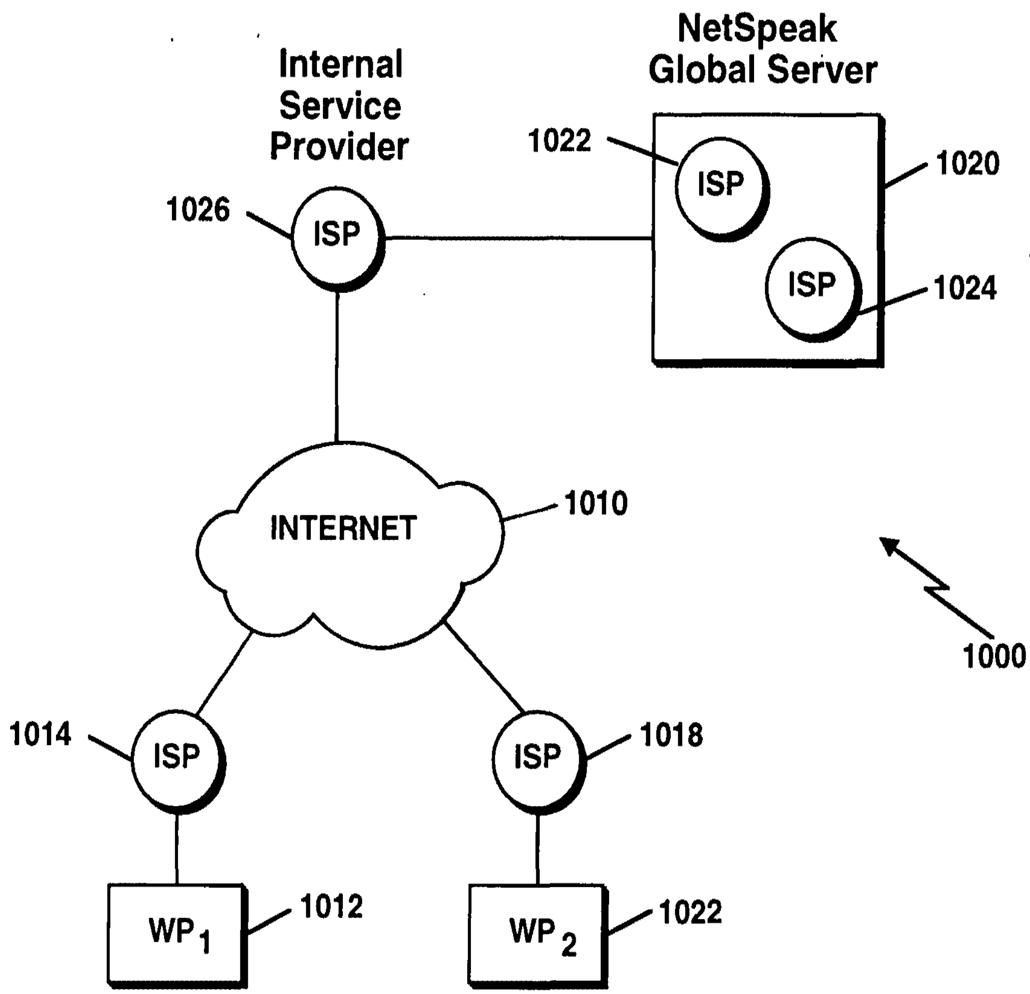

NetSpeak
Global Server
Internal
Service
Provider
1022
ISP
1020
1026
ISP
ISP
1024
INTERNET
1010
1000
1014
ISP
ISP
1018
WP1
1012
WP2
1022

Figure 10

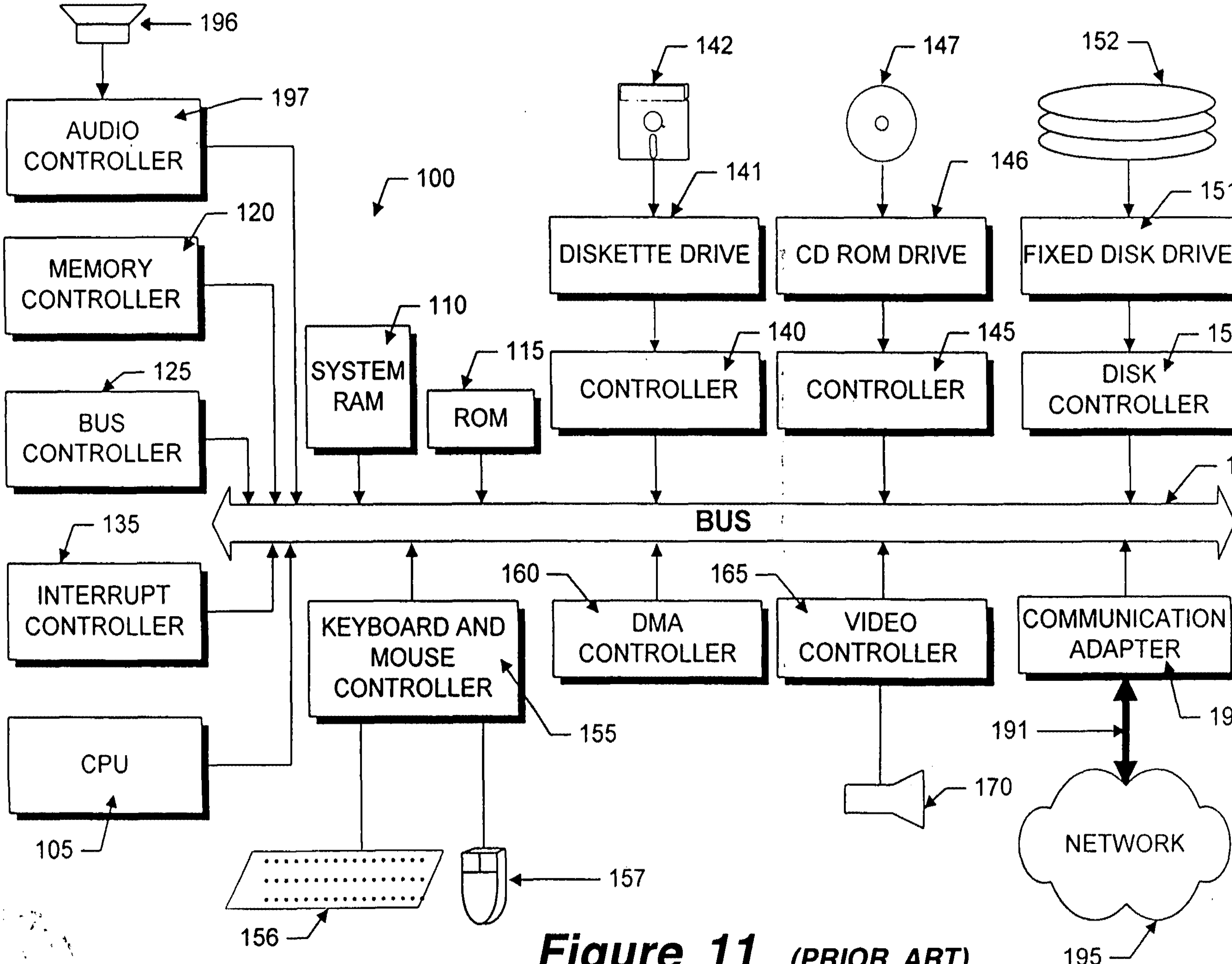


Figure 11 *(PRIOR ART)*

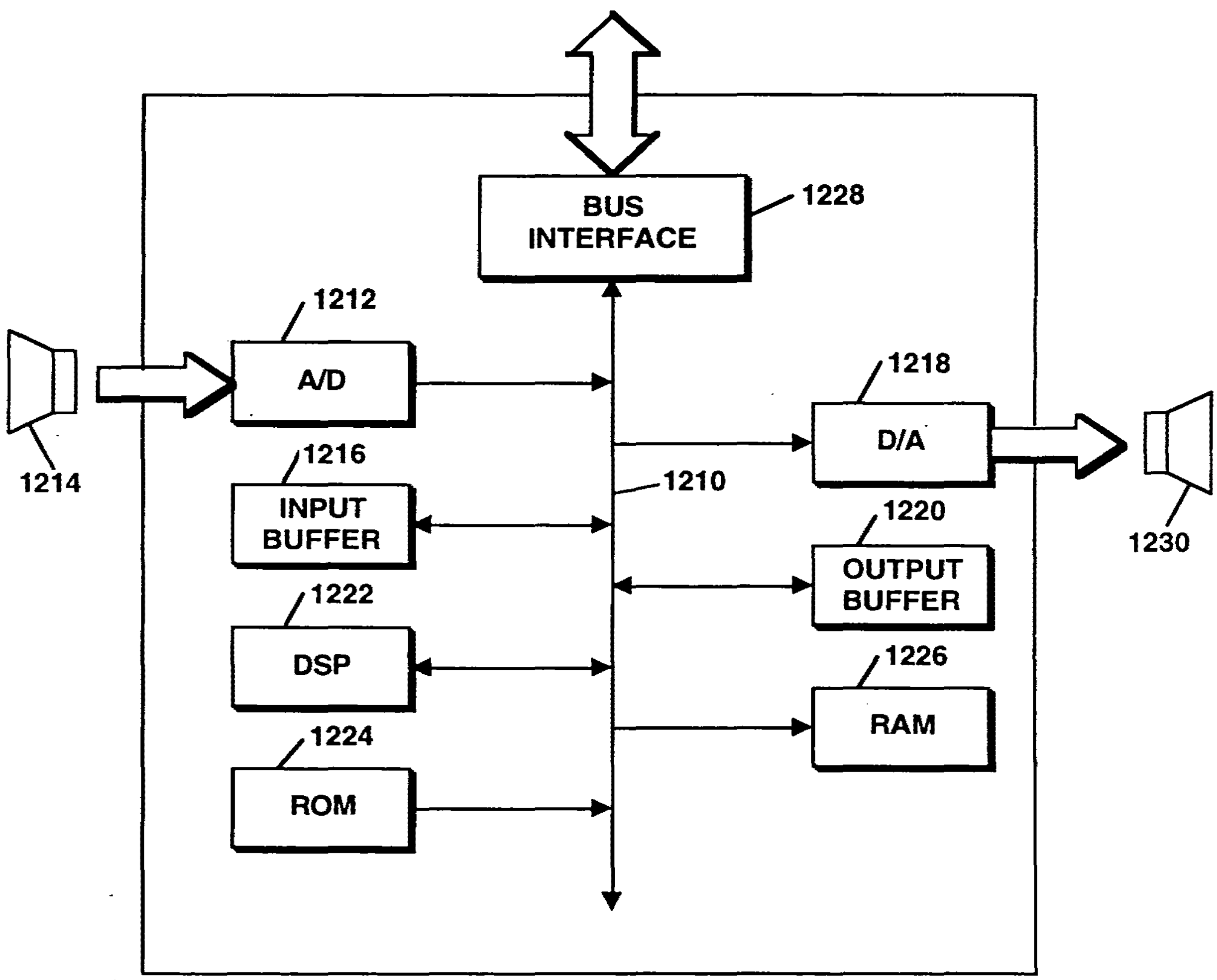


FIGURE 12 (PRIOR ART)

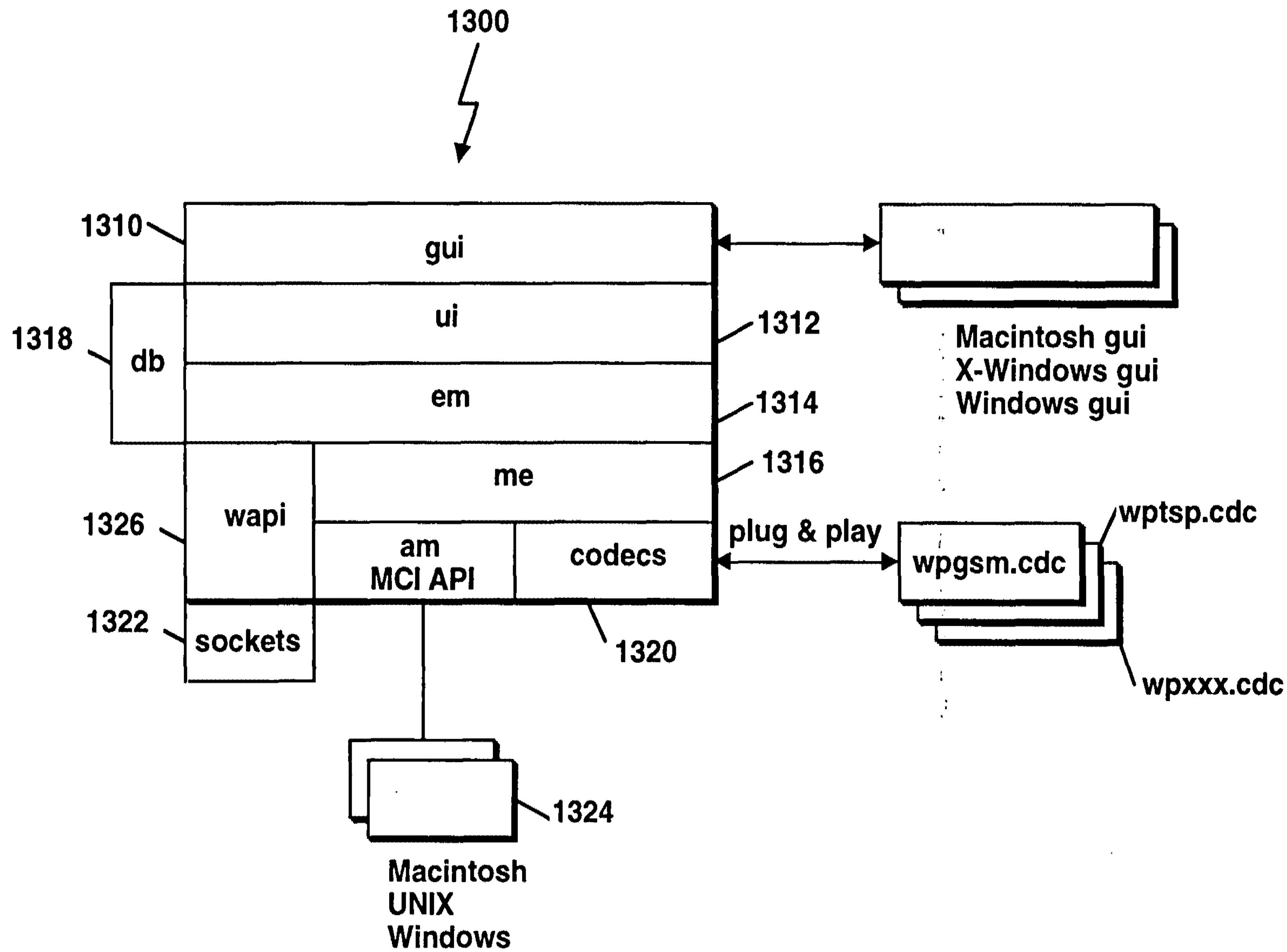

1300
1310
gui
ui
1318
db
em
1312
1314
1316
me
wapi
1326
am
MCI API
codecs
1322
sockets
1320
Macintosh gui
X-Windows gui
Windows gui
plug & play
wpgsm.cdc
wptsp.cdc
wpxxx.cdc
1324
Macintosh
UNIX
Windows

Figure 13 A

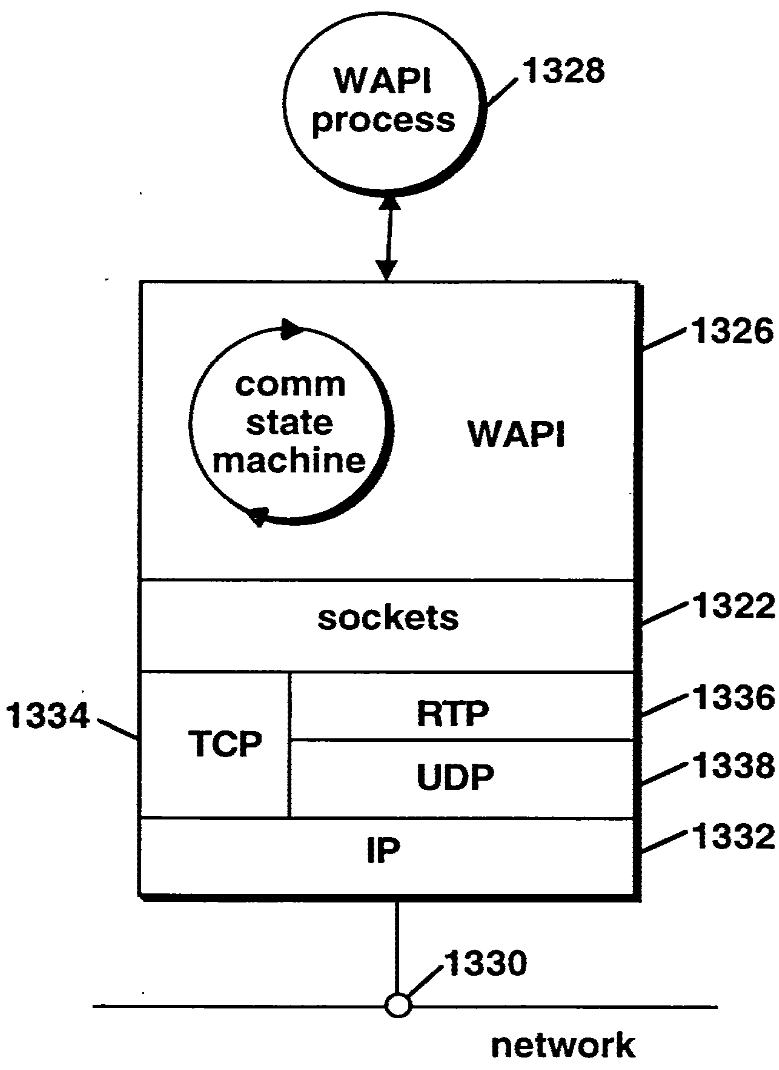
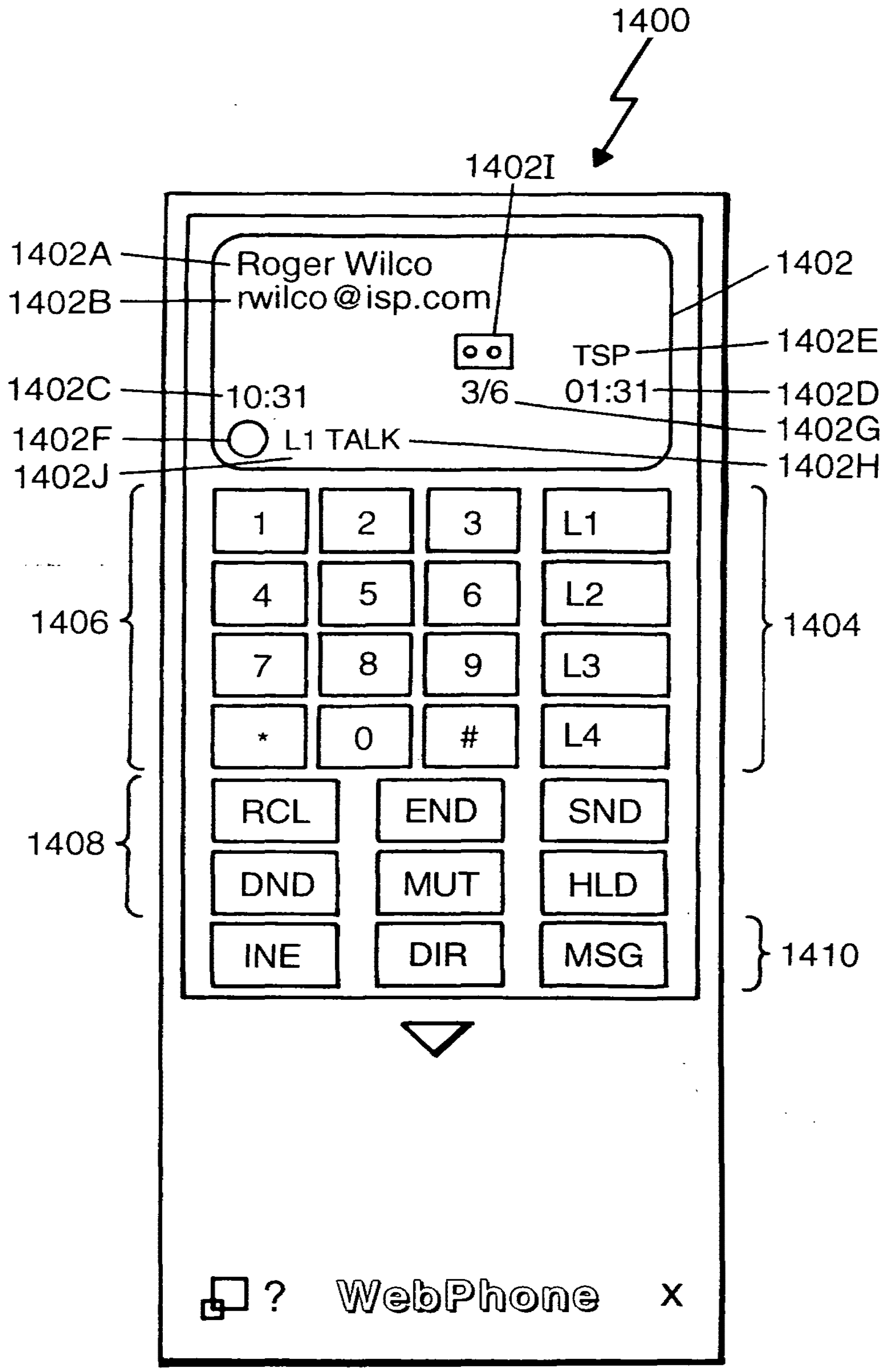

WAPI
process
1328
1326
comm
state
machine
WAPI
sockets
1322
1334
TCP
RTP
1336
UDP
1338
IP
1332
1330
network

FIGURE 13 B



1400
1402I
1402A
Roger Wilco
1402B
rwilco@isp.com
1402
TSP
1402E
1402C
10:31
3/6
01:31
1402D
1402G
1402F
L1 TALK
1402H
1402J
1
2
3
L1
4
5
6
L2
1406
1404
7
8
9
L3
*
0
#
L4
RCL
END
SND
1408
DND
MUT
HLD
INE
DIR
MSG
1410
?
WebPhone
X

Figure 14

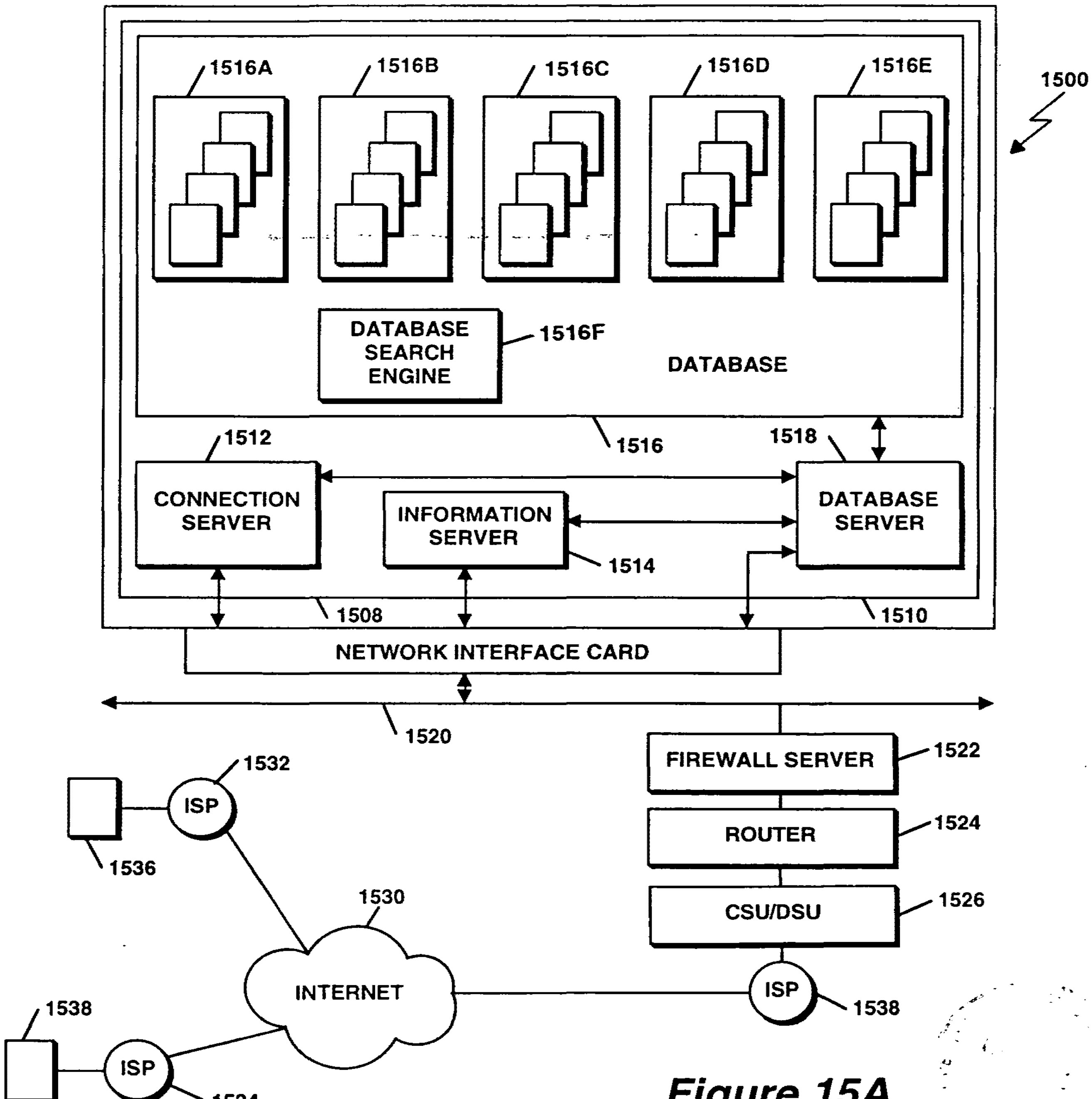

1500
1516A
1516B
1516C
1516D
1516E
DATABASE SEARCH ENGINE
1516F
DATABASE
1512
1516
1518
CONNECTION SERVER
INFORMATION SERVER
DATABASE SERVER
1514
1508
1510
NETWORK INTERFACE CARD
1520
FIREWALL SERVER
1522
ROUTER
1524
CSU/DSU
1526
1532
ISP
1536
1530
INTERNET
ISP
1538
1538
ISP
1534

Figure 15A

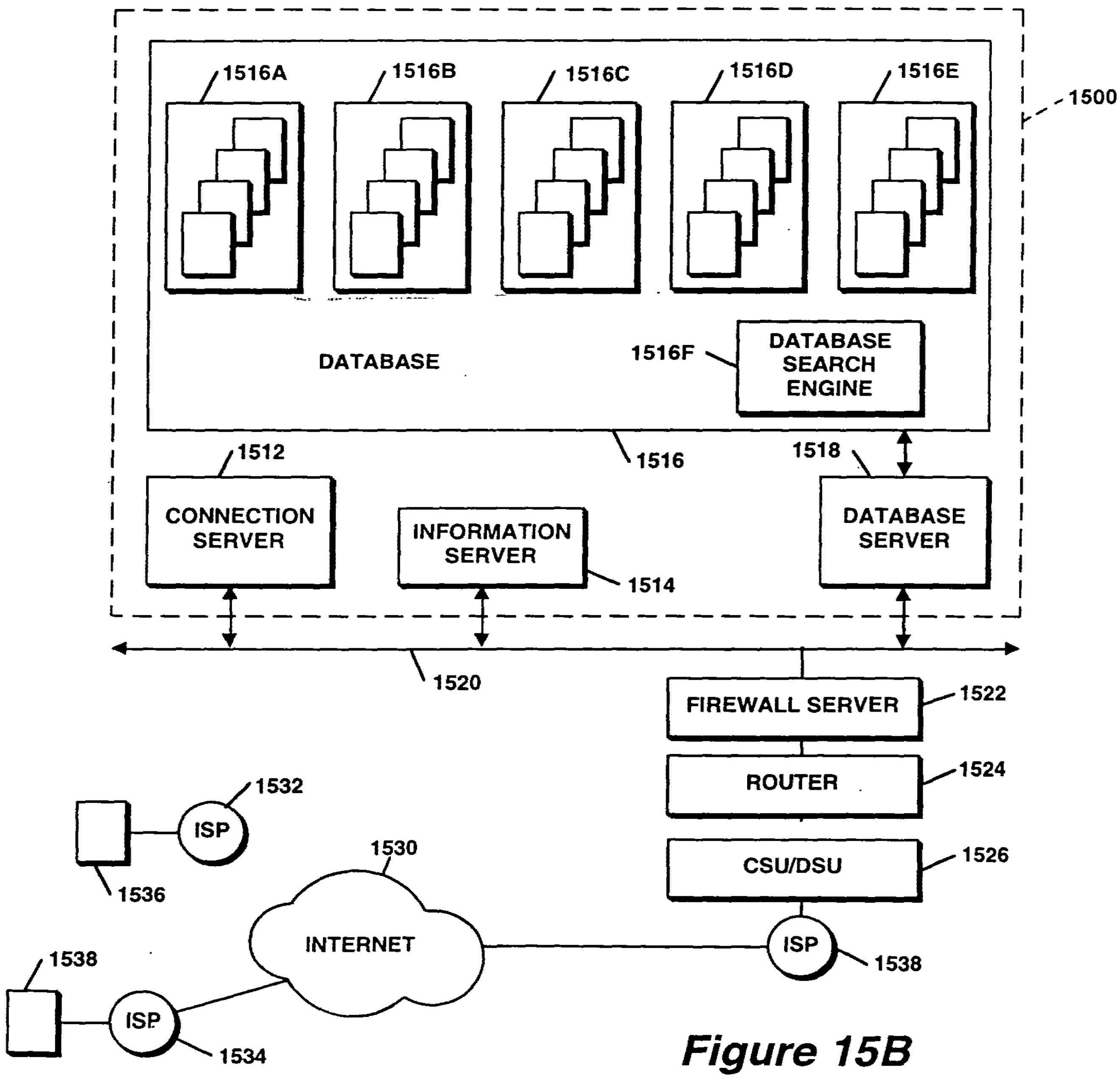

1516A
1516B
1516C
1516D
1516E
1500
DATABASE
1516F
DATABASE SEARCH ENGINE
1512
1516
1518
CONNECTION SERVER
INFORMATION SERVER
1514
DATABASE SERVER
1520
FIREWALL SERVER
1522
ROUTER
1524
CSU/DSU
1526
1532
ISP
1536
1530
INTERNET
ISP
1538
1538
ISP
1534

Figure 15B

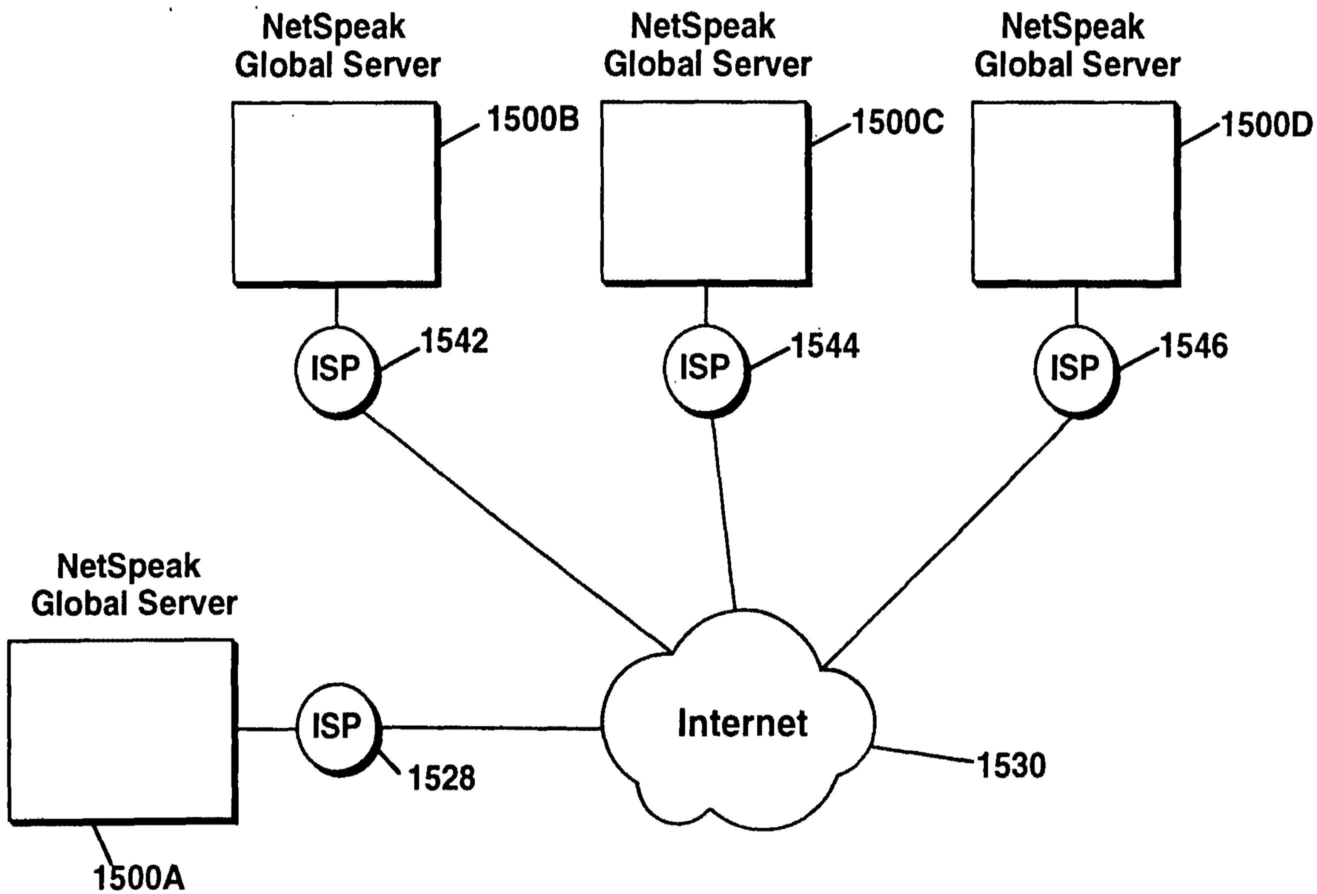


Figure 15C

15/27

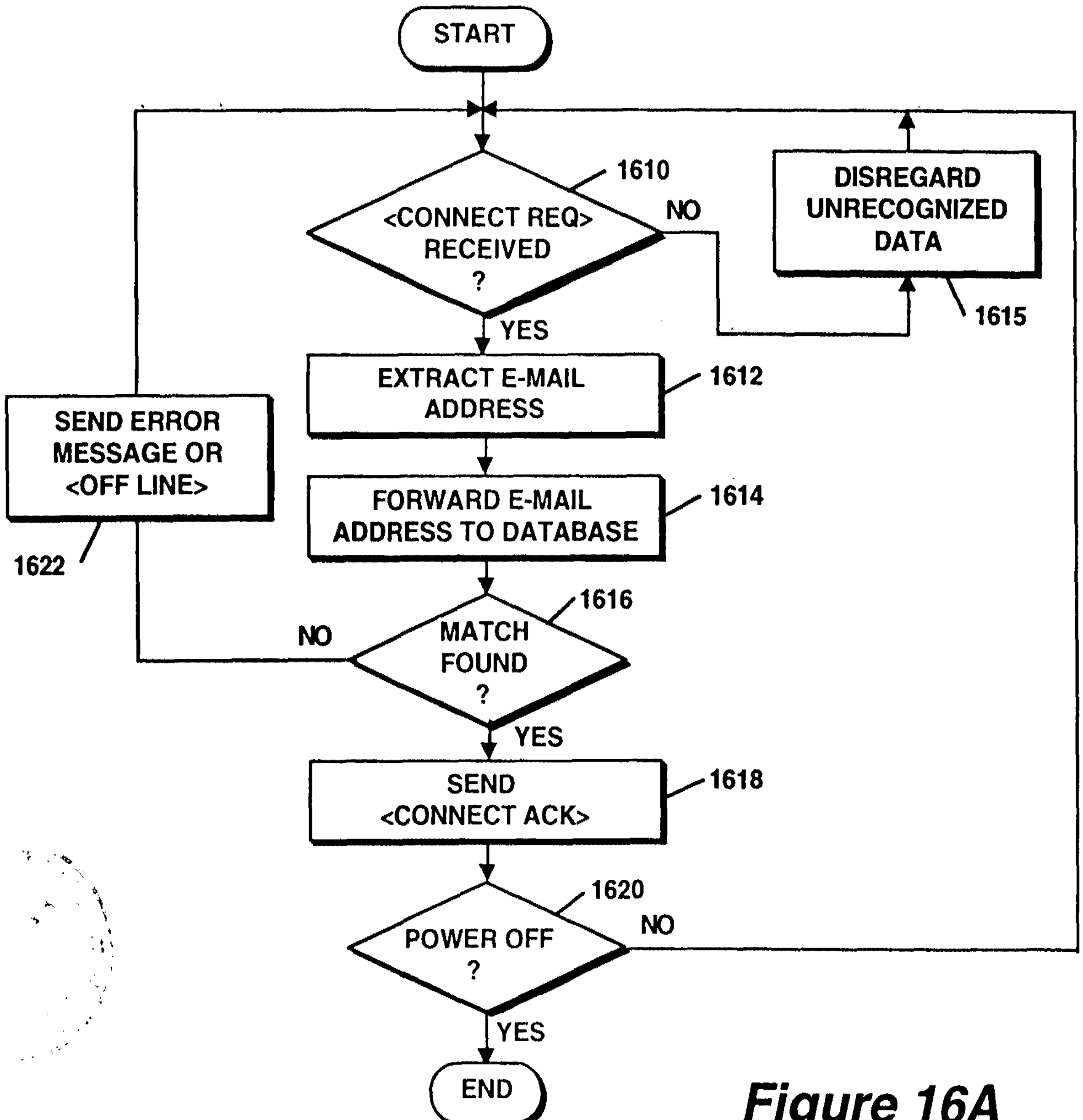


Figure 16A

16/27

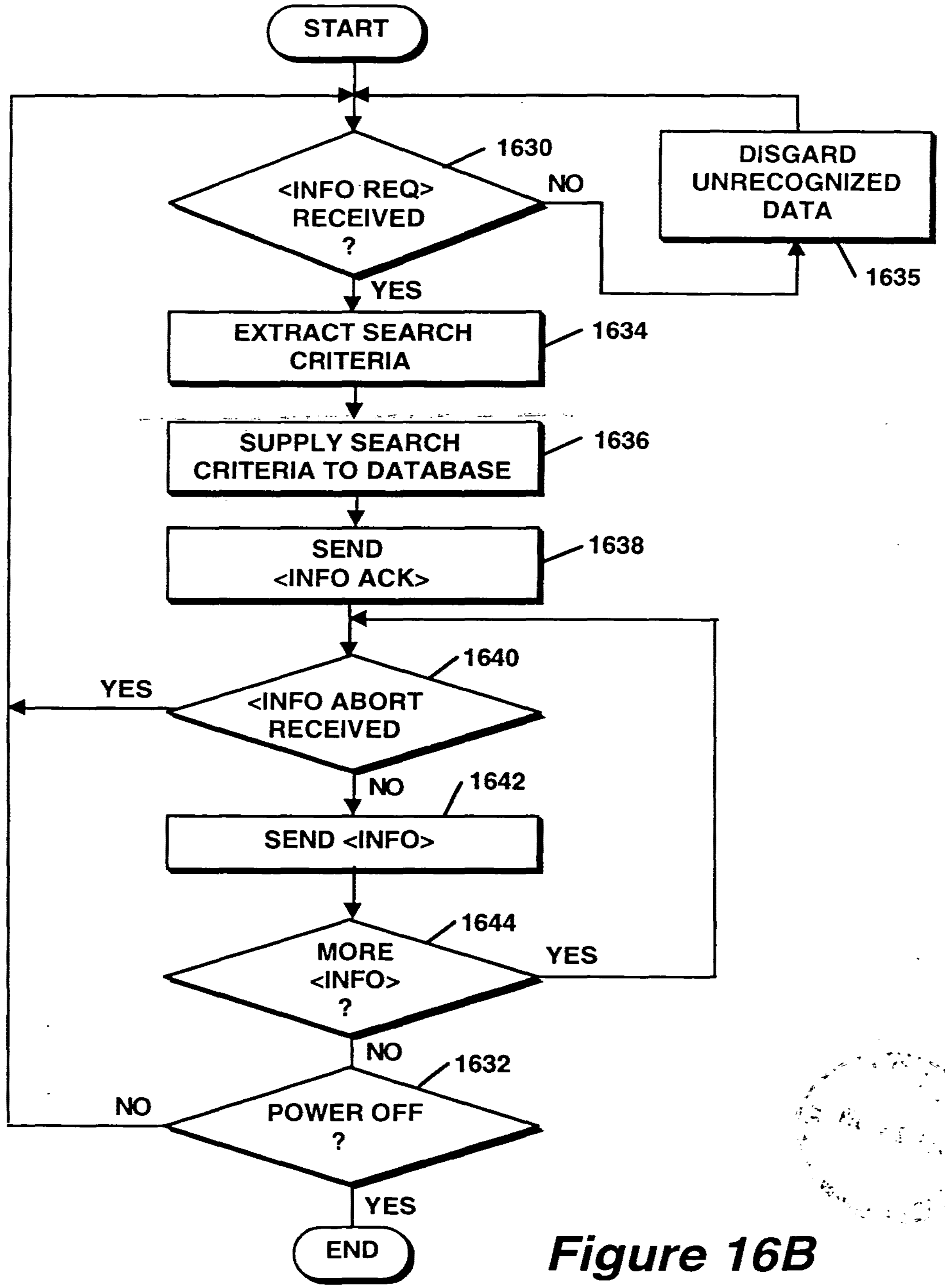
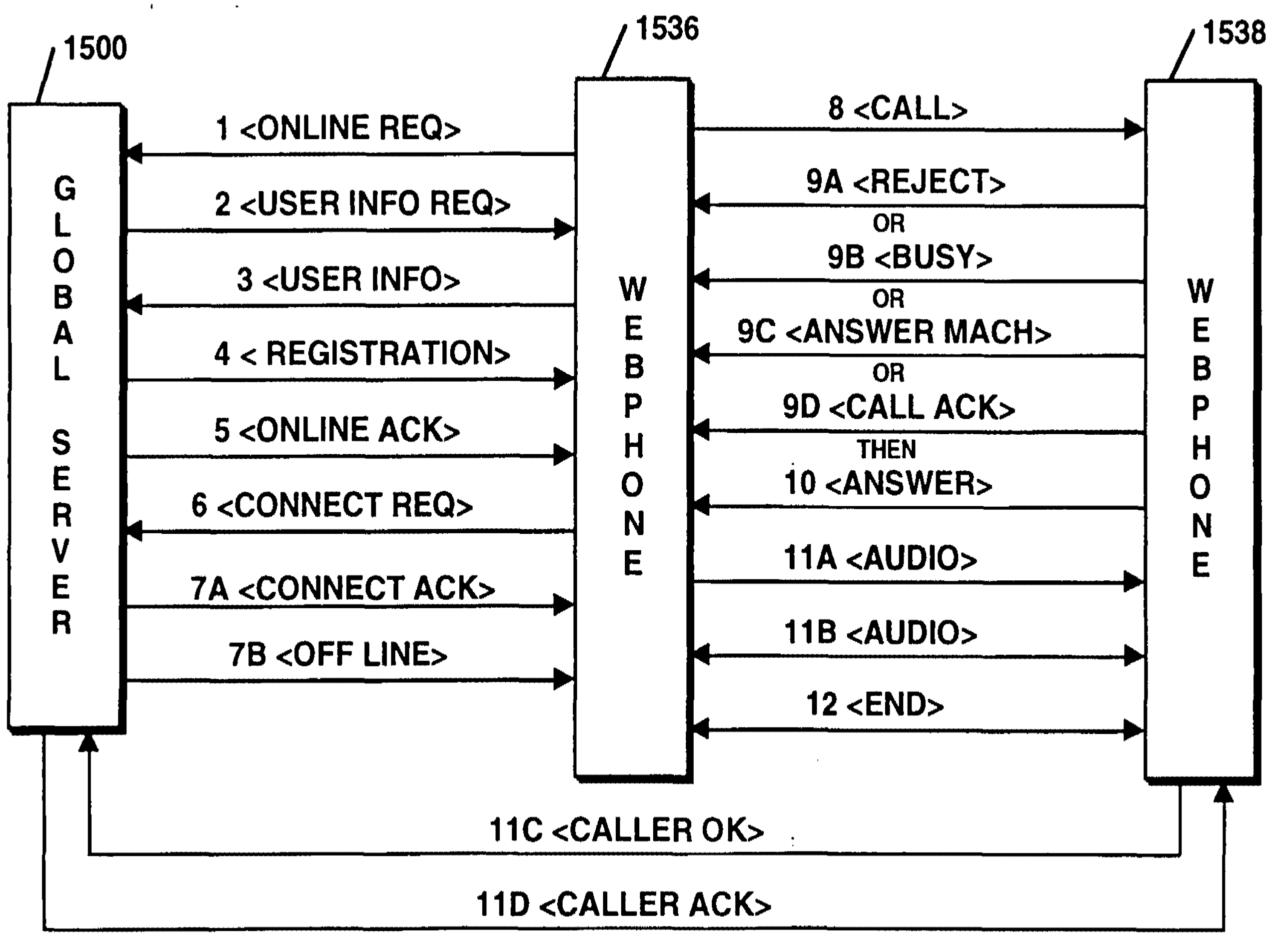

START
1630
<INFO REQ>
RECEIVED
?
NO
DISGARD
UNRECOGNIZED
DATA
1635
YES
EXTRACT SEARCH
CRITERIA
1634
SUPPLY SEARCH
CRITERIA TO DATABASE
1636
SEND
<INFO ACK>
1638
1640
YES
<INFO ABORT
RECEIVED
NO
1642
SEND <INFO>
1644
MORE
<INFO>
?
YES
NO
1632
NO
POWER OFF
?
YES
END

Figure 16B



18/27

Figure 17A

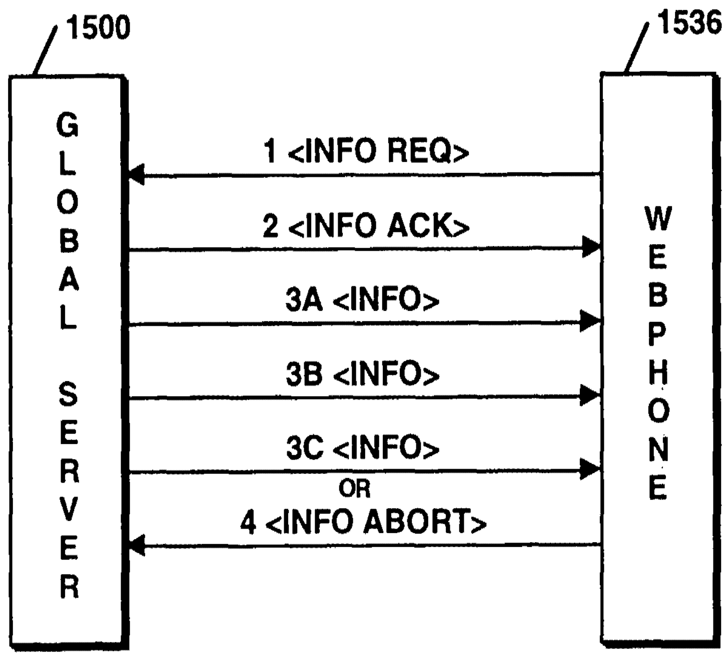

1500
1536
GLOBAL SERVER
WEBPHONE
1 <INFO REQ>
2 <INFO ACK>
3A <INFO>
3B <INFO>
3C <INFO>
OR
4 <INFO ABORT>

Figure 17B

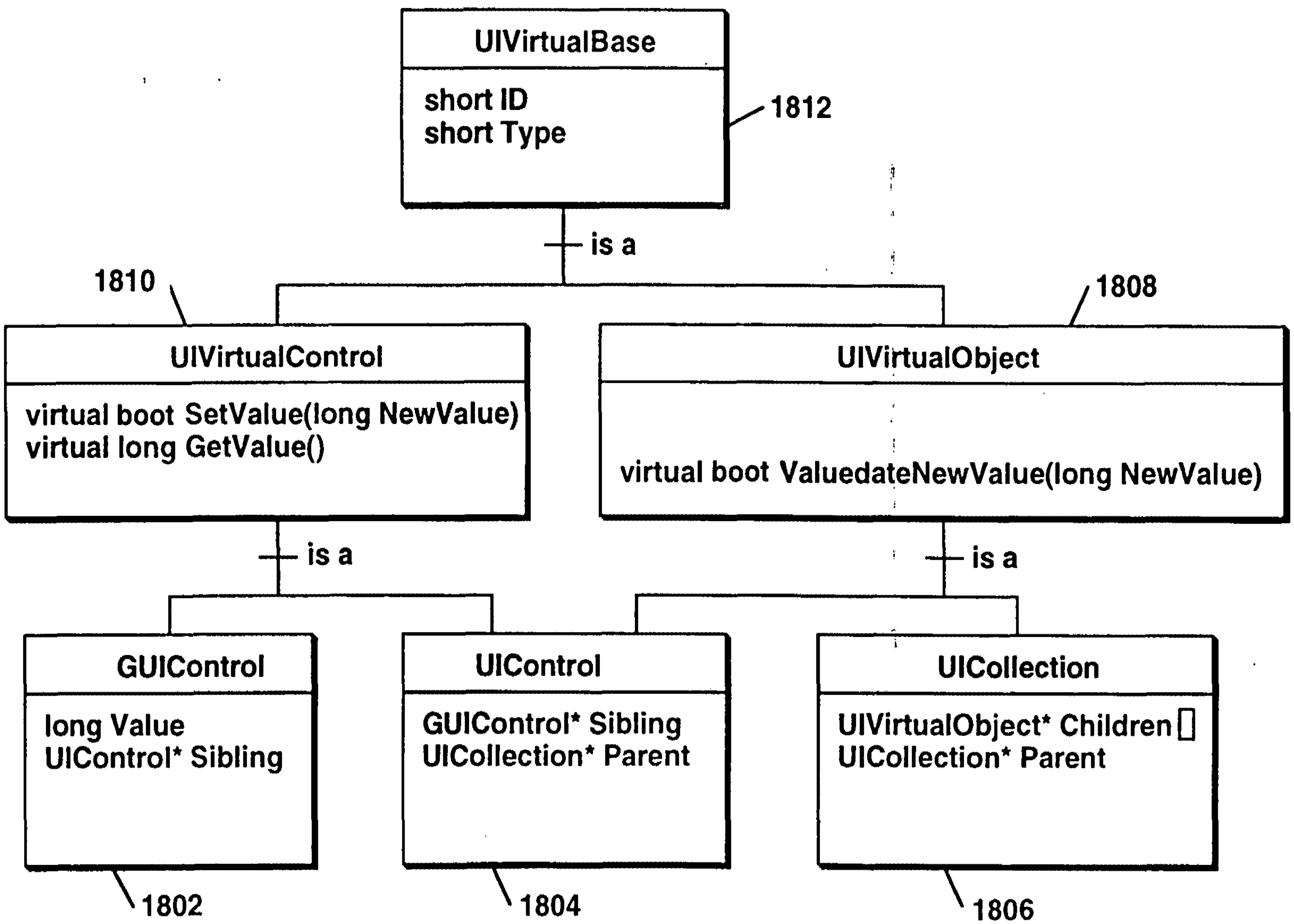


Figure 18A

20/27

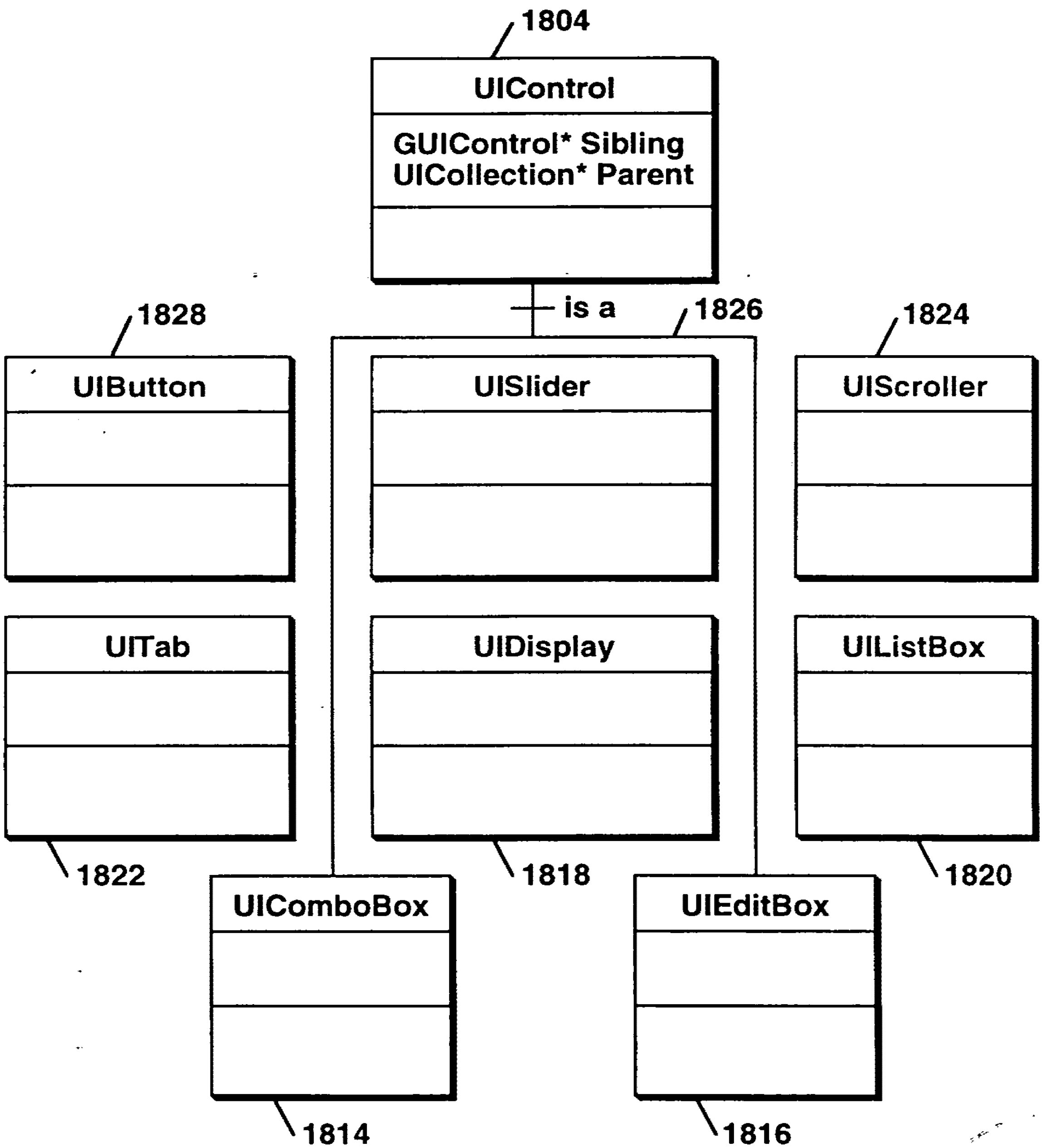

1804
UIControl
GUIControl* Sibling
UICollection* Parent
is a
1826
1828
UIButton
UISlider
1824
UIScroller
UITab
UIDisplay
UIListBox
1822
1818
1820
UIComboBox
UIEditBox
1814
1816

Figure 18B

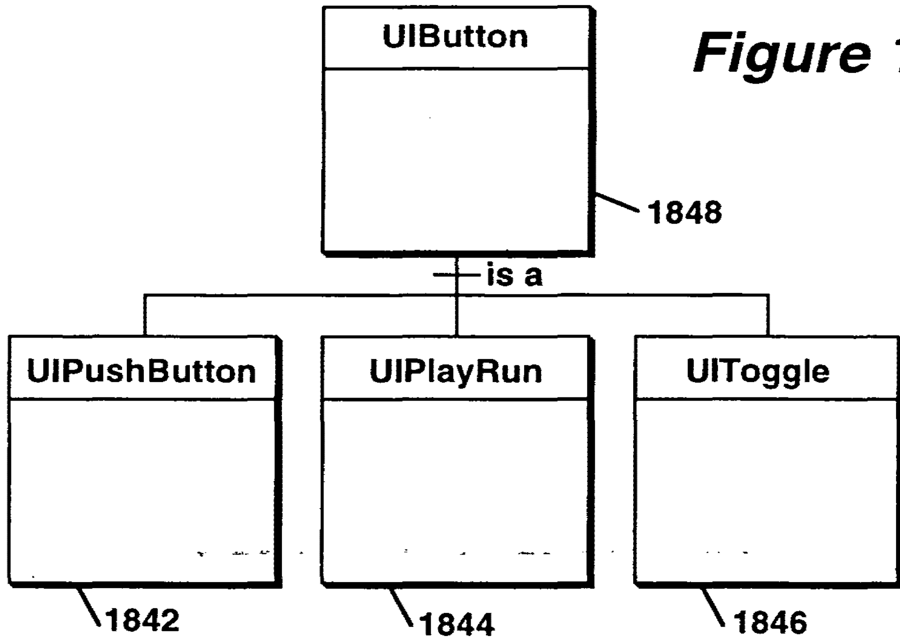


Figure 18C

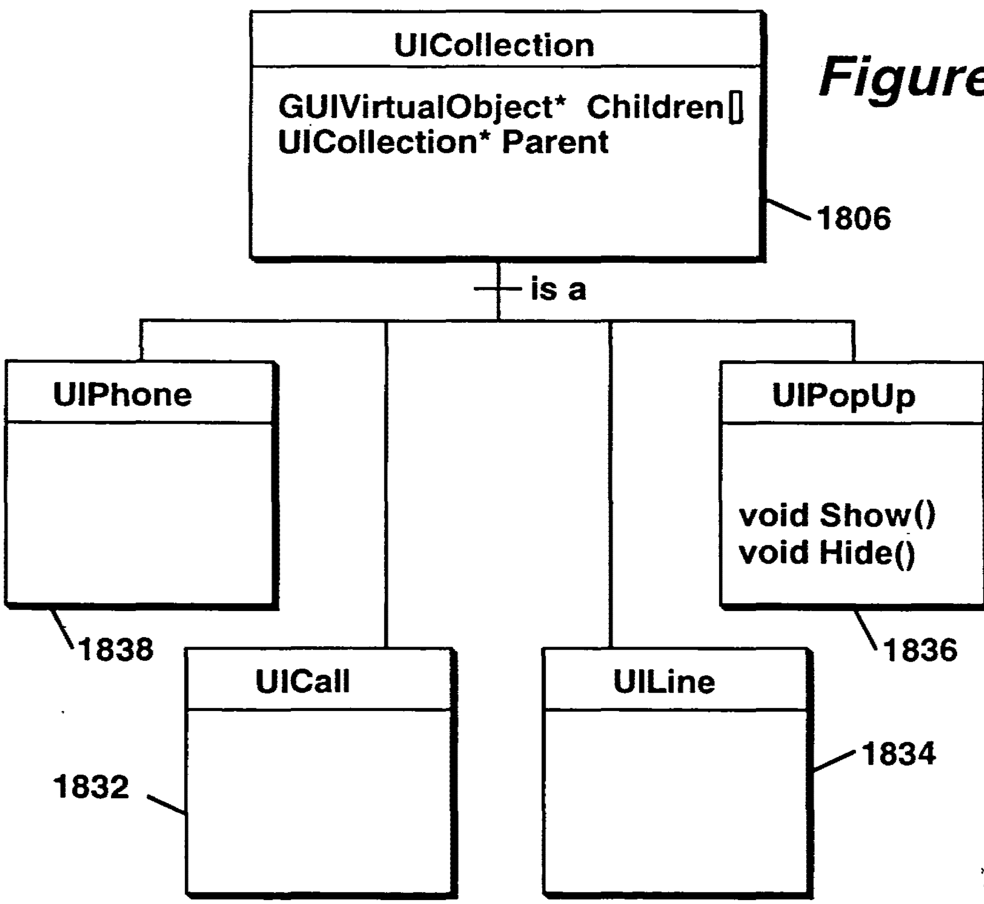


Figure 18D

23/27

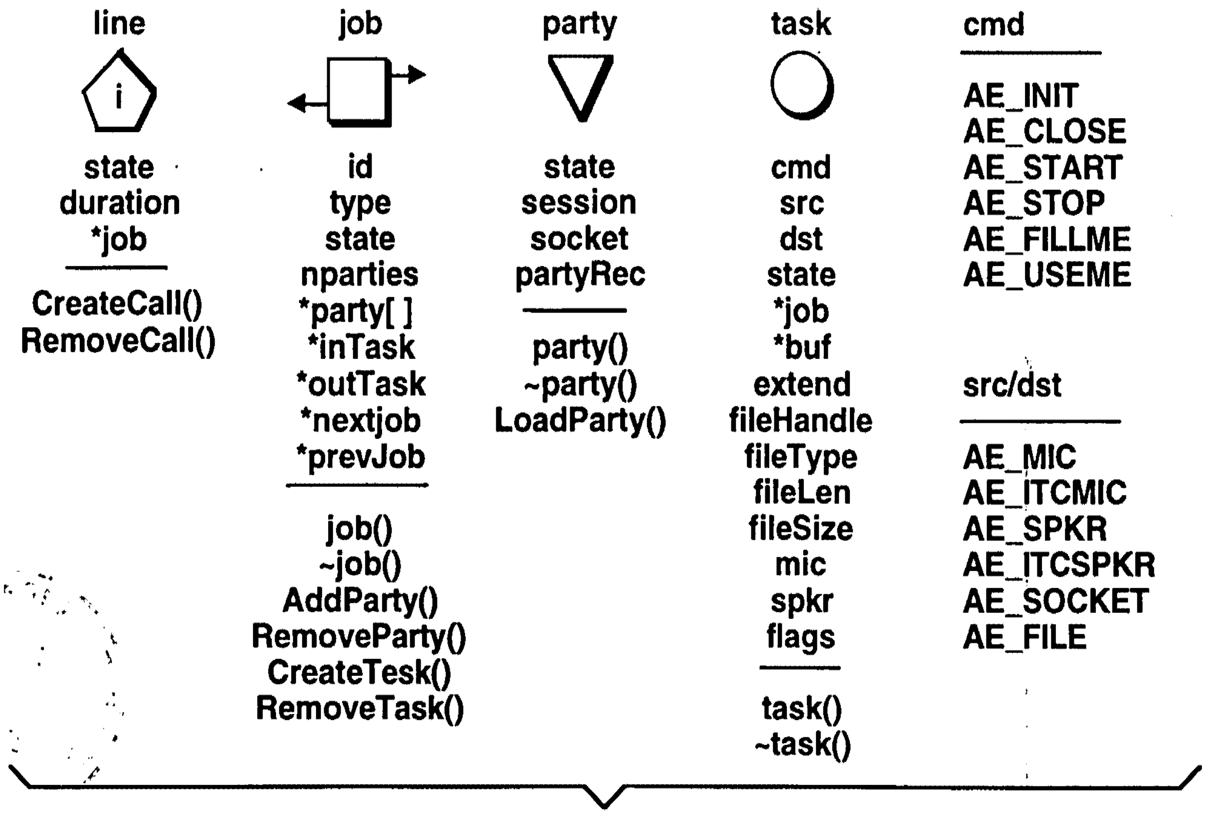


Figure 19A

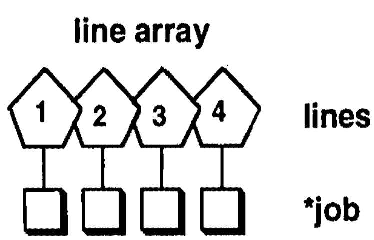


Figure 19B

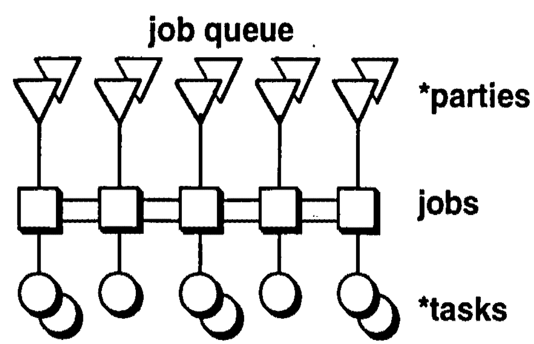


Figure 19C

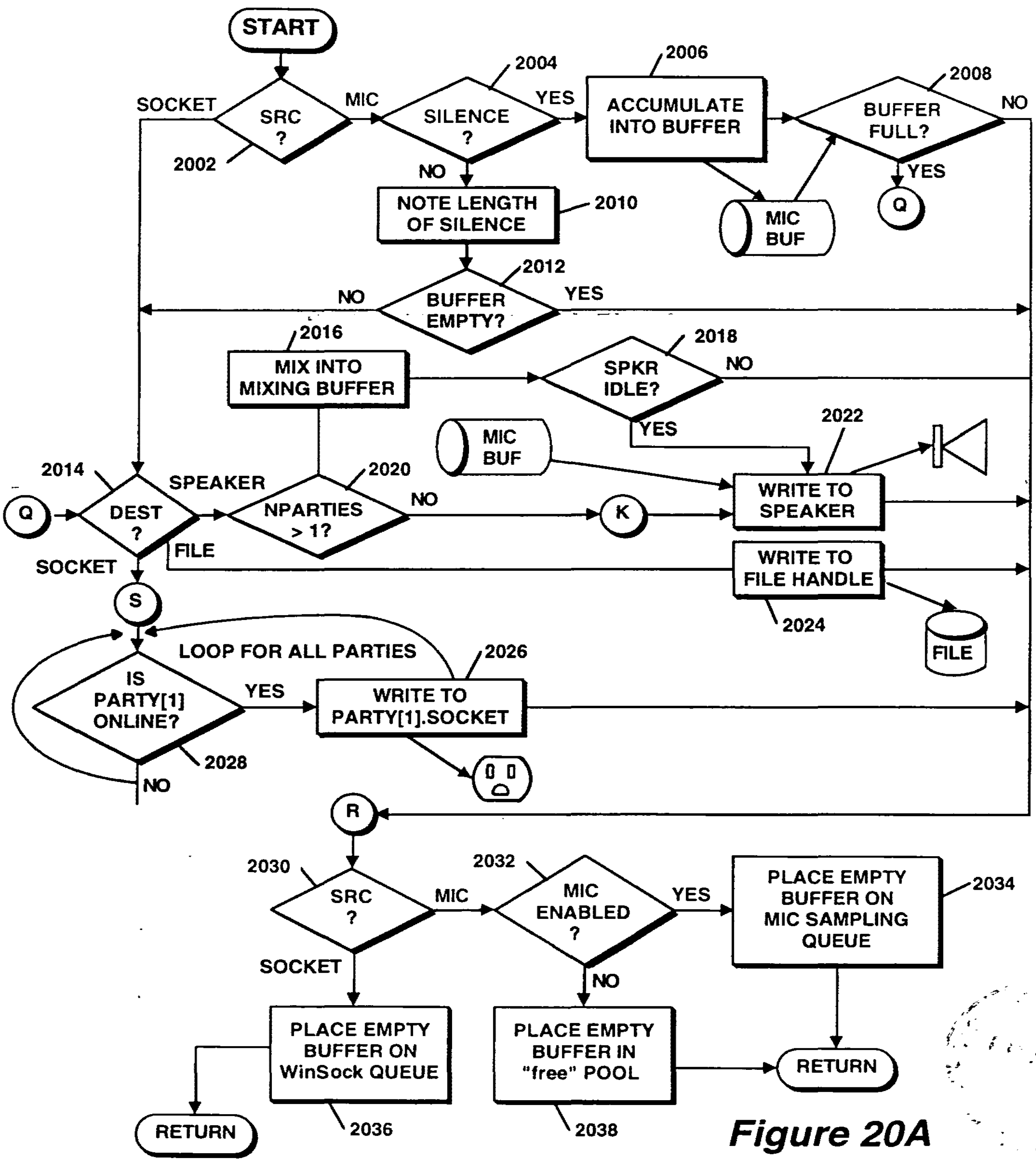

START
SRC ?
2002
SOCKET
MIC
SILENCE ?
2004
YES
NO
ACCUMULATE INTO BUFFER
2006
BUFFER FULL?
2008
NO
YES
Q
MIC BUF
NOTE LENGTH OF SILENCE
2010
BUFFER EMPTY?
2012
NO
YES
MIX INTO MIXING BUFFER
2016
SPKR IDLE?
2018
NO
YES
MIC BUF
2022
WRITE TO SPEAKER
2014
Q
DEST ?
SPEAKER
NPARTIES > 1?
2020
NO
K
FILE
SOCKET
WRITE TO FILE HANDLE
2024
FILE
S
LOOP FOR ALL PARTIES
2026
IS PARTY[1] ONLINE?
YES
WRITE TO PARTY[1].SOCKET
2028
NO
R
2030
SRC ?
MIC
2032
MIC ENABLED ?
YES
PLACE EMPTY BUFFER ON MIC SAMPLING QUEUE
2034
SOCKET
NO
PLACE EMPTY BUFFER ON WinSock QUEUE
PLACE EMPTY BUFFER IN "free" POOL
RETURN
RETURN
2036
2038

Figure 20A

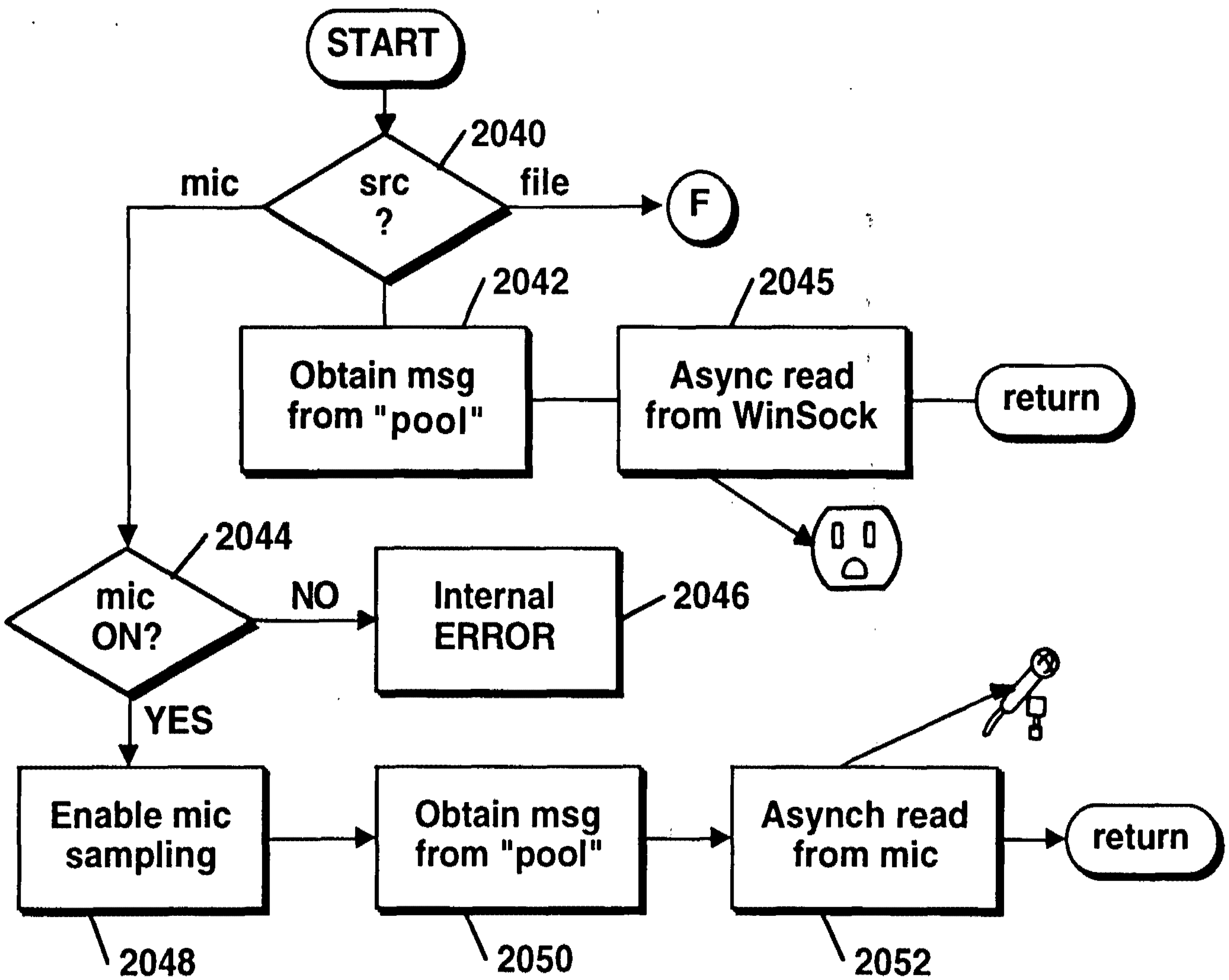

START
2040
mic
src ?
file
F
2042
2045
Obtain msg from "pool"
Async read from WinSock
return
2044
mic ON?
NO
Internal ERROR
2046
YES
Enable mic sampling
Obtain msg from "pool"
Asynch read from mic
return
2048
2050
2052

Figure 20B

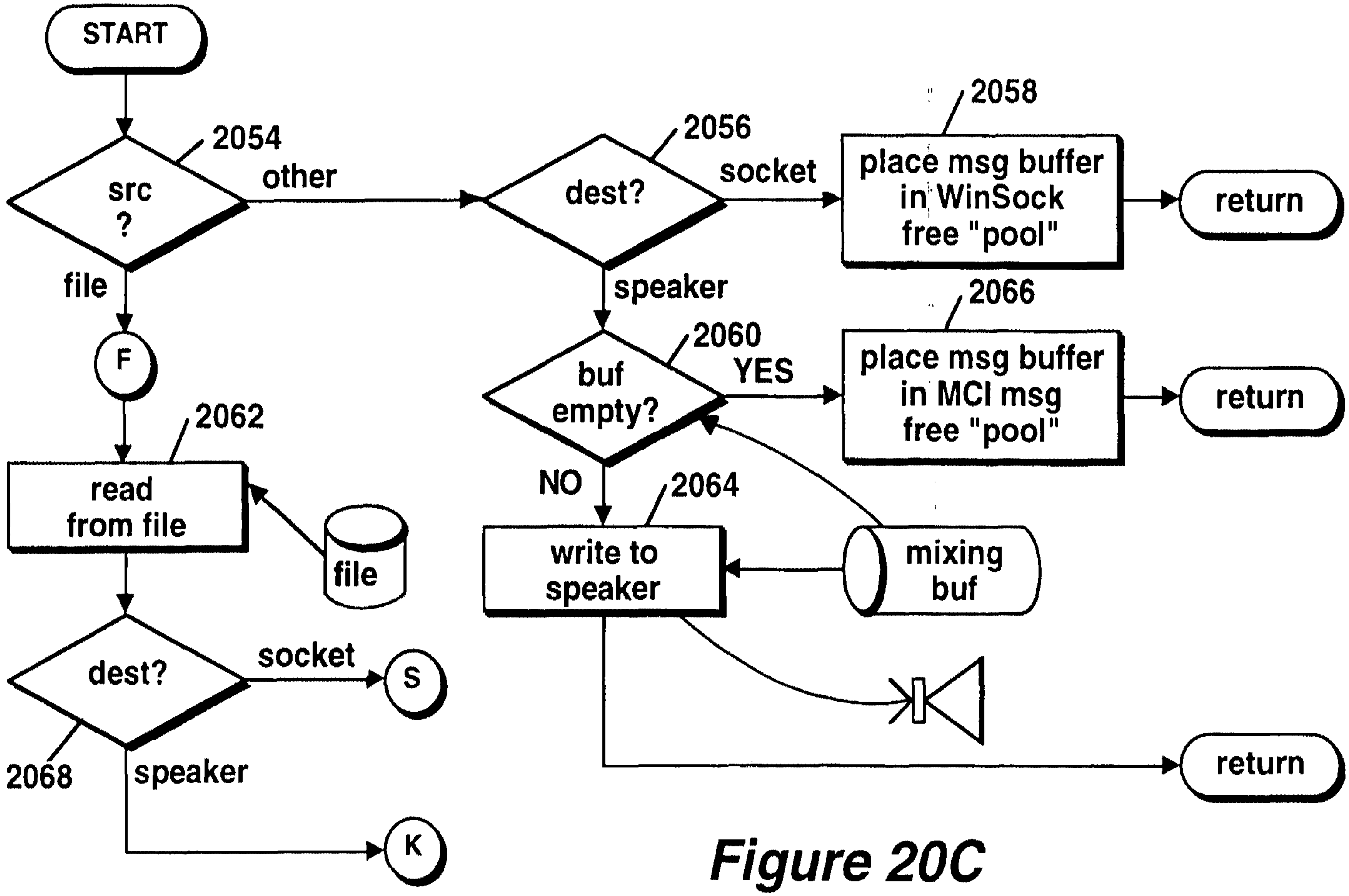

START
src ?
2054
other
file
F
2062
read from file
file
dest?
socket
S
2068
speaker
K
dest?
2056
socket
speaker
2058
place msg buffer in WinSock free "pool"
return
2060
buf empty?
YES
2066
place msg buffer in MCI msg free "pool"
return
NO
2064
write to speaker
mixing buf
return

Figure 20C

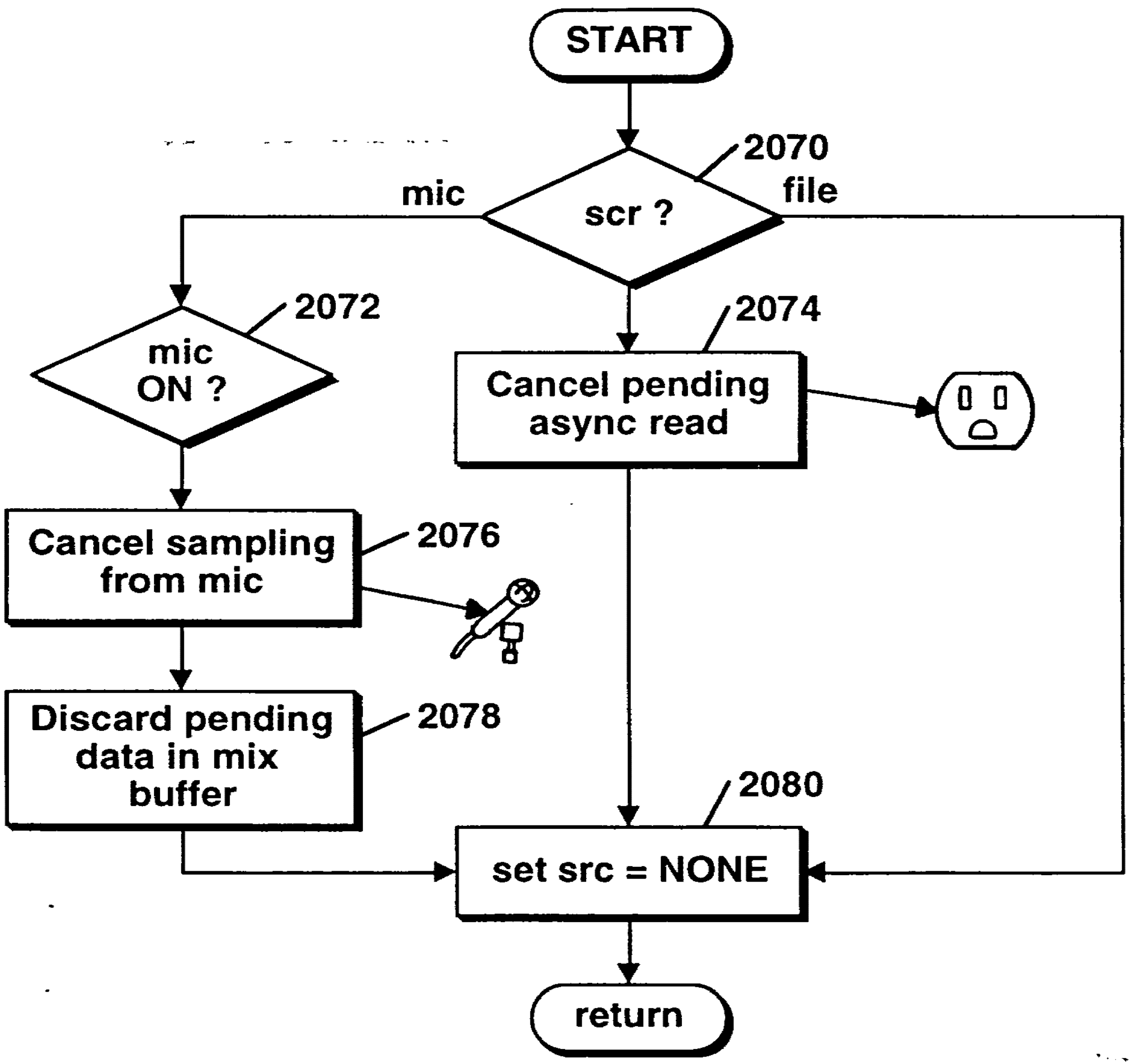

START
2070
mic
scr ?
file
2072
mic
ON ?
2074
Cancel pending
async read
Cancel sampling
from mic
2076
Discard pending
data in mix
buffer
2078
2080
set src = NONE
return

Figure 20D

#11

KUDIRKA & JOBSE, LLP

Two Center Plaza
Boston MA 02108
Tel: (617) 367-4600
Fax: (617) 367-4656

FACSIMILE COVER SHEET

Number of pages being transmitted (including cover sheet): 2

Date: August 31, 1999 **Time:** 1:19 PM

TO:	**Name:**	Ms. Terry Dyson
	Company:	United States Patent & Trademark Office
	Facsimile No:	(703) 308-6642
	Telephone No:	
FROM:	**Name:**	Bruce D. Jobse, Esq.
RE:	**Our File Number:**	N0003/7002
	Your File Number:	

Originals By: ☐ First Class Mail ☐ Overnight ☐ Air Mail ☒ Not Sent

Comments or Instructions

KUDIRKA & JOBSE, LLP
TWO CENTER PLAZA
BOSTON, MASSACHUSETTS 02108
Tel.: (617) 367-4600

PAUL E. KUDIRKA
BRUCE D. JOBSE
PHILIP L. CONRAD
VINCENT J. PROIO+

OF COUNSEL
GARY E. ROSS

SPECIALIZING IN
INTELLECTUAL PROPERTY LAW

FAX: (617) 367-4656
E-MAIL: K-JPAT.COM

+NOT ADMITTED IN ANY JURISDICTION

August 31, 1999

VIA FACSIIMLE

Ms. Terry Dyson
United States Patent & Trademark Office
Washington, DC 20231

Re: U.S. Patent Application Serial No. 08/721,316
GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Our File No.: N0003/7002

Dear Ms. Dyson,

This is to confirm our telephone conversation today that the letters "X" as found on page 4, lines 15-16 and page 15, lines 10-12 of United States Patent Appln. Serial No. 08/721,316 do not require further modification before the application advances to printing and issuance.

Do not hesitate to contact me or have the Examiner contact me if there are any further questions regarding this matter.

Cordially yours,

KUDIRKA & JOBSE, LLP

Bruce D. Jobse, Esq.
Attorney of Record for Applicants

BDJ:fmc

UNITED STAT DEPARTMENT OF COMMERCE
Patent and T. emark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO
08/721,316	09/25/96	MATTAWAY	S

021127
KUDIRKA & JOBSE
TWO CENTER PLAZA
BOSTON MA 02108

LM51/1019

EXAMINER	
RAMIREZ,E	
ART UNIT	PAPER NUMBER
2757	12

DATE MAILED: 10/19/99

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

Sup. NOTICE OF ALLOWABILITY

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to the filling of formal drawings on 8/24/99

☐ The allowed claim(s) is/are ______

☐ The drawings filed on ______ are acceptable.

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) ______

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR REPLY to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

☐ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

☐ because the originally filed drawings were declared by applicant to be informal.

☒ including changes required by the Notice of Draftperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. 12.

☐ including changes required by the proposed drawing correction filed on ______, which has been approved by the examiner.

☐ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftperson.

☐ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any reply to this notice should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

☒ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

☐ Interview Summary, PTO-413

☐ Examiner's Amendment/Comment

☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

☐ Examiner's Statement of Reasons for Allowance

Moustafa Meky
MOUSTAFA M. MEKY
PRIMARY EXAMINER

PTOL-37 (Rev. 8/97)

*U.S. GPO: 1998-433-221/82106

Form PTO 948 (Rev. 8-98) U.S. DEPARTMENT OF COMMERCE - Patent and Trademark Office Application No. 08/721316

NOTICE OF DRAFTSPERSON'S PATENT DRAWING REVIEW

The drawing(s) filed (insert date) 8/24/99 are:

A. ☐ approved by the Draftsperson under 37 CFR 1.84 or 1.152.

B. ☒ objected to by the Draftsperson under 37 CFR 1.84 or 1.152 for the reasons indicated below. The Examiner will require submission of new, corrected drawings when necessary. Corrected drawing must be sumitted according to the instructions on the back of this notice.

1. DRAWINGS. 37 CFR 1.84(a): Acceptable categories of drawings:
   Black ink. Color.
   ____ Color drawings are not acceptable until petiton is granted.
   Fig(s) ________
   ____ Pencil and non black ink not permitted. Fig(s) ________
2. PHOTOGRAPHS. 37 CFR 1.84 (b)
   ____ 1 full-tone set is required. Fig(s) ________
   ____ Photographs not properly mounted (must use brystol board or photographic double-weight paper). Fig(s) ________
   ____ Poor quality (half-tone). Fig(s) ________
3. TYPE OF PAPER. 37 CFR 1.84(e)
   ____ Paper not flexible, strong, white, and durable.
   Fig(s) ________
   ____ Erasures, alterations, overwritings, interlineations, folds, copy machine marks not accepted. Fig(s) ________
   ____ Mylar, velum paper is not acceptable (too thin).
   Fig(s) ________
4. SIZE OF PAPER. 37 CFR 1.84(f): Acceptable sizes:
   ____ 21.0 cm by 29.7 cm (DIN size A4)
   ____ 21.6 cm by 27.9 cm (8 1/2 x 11 inches)
   ____ All drawing sheets not the same size.
   Sheet(s) ________
   ____ Drawings sheets not an acceptable size. Fig(s) ________
5. MARGINS. 37 CFR 1.84(g): Acceptable margins:
   Top 2.5 cm Left 2.5cm Right 1.5 cm Bottom 1.0 cm
   SIZE: A4 Size
   Top 2.5 cm Left 2.5 cm Right 1.5 cm Bottom 1.0 cm
   SIZE: 8 1/2 x 11
   Margins not acceptable. Fig(s) 5-7, 9, 15A, 15B
   X Top (T) X Left (L)
   ____ Right (R) ____ Bottom (B)
6. VIEWS. 37 CFR 1.84(h)
   REMINDER: Specification may require revision to correspond to drawing changes.
   Partial views. 37 CFR 1.84(h)(2)
   ____ Brackets needed to show figure as one entity.
   Fig(s) ________
   ____ Views not labeled separately or properly.
   Fig(s) ________
   ____ Enlarged view not labeled separetely or properly.
   Fig(s) ________
7. SECTIONAL VIEWS. 37 CFR 1.84 (h)(3)
   ____ Hatching not indicated for sectional portions of an object.
   Fig(s) ________
   ____ Sectional designation should be noted with Arabic or Roman numbers. Fig(s) ________
8. ARRANGEMENT OF VIEWS. 37 CFR 1.84(i)
   ____ Words do not appear on a horizontal, left-to-right fashion when page is either upright or turned so that the top becomes the right side, except for graphs. Fig(s) ________
9. SCALE. 37 CFR 1.84(k)
   ____ Scale not large enough to show mechanism without crowding when drawing is reduced in size to two-thirds in reproduction.
   Fig(s) ________
10. CHARACTER OF LINES, NUMBERS, & LETTERS. 37 CFR 1.84(l)
    ____ Lines, numbers & letters not uniformly thick and well defined, clean, durable, and black (poor line quality).
    Fig(s) ________
11. SHADING. 37 CFR 1.84(m)
    ____ Solid black areas pale. Fig(s) ________
    ____ Solid black shading not permitted. Fig(s) ________
    ____ Shade lines, pale, rough and blurred. Fig(s) ________
12. NUMBERS, LETTERS, & REFERENCE CHARACTERS. 37 CFR 1.84(p)
    ____ Numbers and reference characters not plain and legible.
    Fig(s) ________
    ____ Figure legends are poor. Fig(s) ________
    ____ Numbers and reference characters not oriented in the same direction as the view. 37 CFR 1.84(p)(1)
    Fig(s) ________
    ____ English alphabet not used. 37 CFR 1.84(p)(2)
    Figs ________
    ____ Numbers, letters and reference characters must be at least .32 cm (1/8 inch) in height. 37 CFR 1.84(p)(3)
    Fig(s) ________
13. LEAD LINES. 37 CFR 1.84(q)
    ____ Lead lines cross each other. Fig(s) ________
    ____ Lead lines missing. Fig(s) ________
14. NUMBERING OF SHEETS OF DRAWINGS. 37 CFR 1.84(t)
    ____ Sheets not numbered consecutively, and in Arabic numerals beginning with number 1. Sheet(s) ________
15. NUMBERING OF VIEWS. 37 CFR 1.84(u)
    ____ Views not numbered consecutively, and in Arabic numerals, beginning with number 1. Fig(s) ________
16. CORRECTIONS. 37 CFR 1.84(w)
    ____ Corrections not made from prior PTO-948 dated ________
17. DESIGN DRAWINGS. 37 CFR 1.152
    ____ Surface shading shown not appropriate. Fig(s) ________
    ____ Solid black shading not used for color contrast.
    Fig(s) ________

COMMENTS

REVIEWER AD DATE 10/15/99 TELEPHONE NO. ________

ATTACHMENT TO PAPER NO. 12

OIPE JC16
OCT 25 1999
PATENT & TRADEMARK OFFICE

LETTER TO OFFICIAL DRAFTSPERSON	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland
Serial No:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: **EL401821480US**
Date of Deposit: **October 22, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed Assistant Commissioner for Patents, Box Issue Fee, Washington, D.C. 20231.

Jan L. Mellen
Jan L. Mellen

Assistant Commissioner for Patents
Box Issue Fee
Washington, DC 20231

1. Upon approval of the Examiner in charge of the above-identified application, please substitute the enclosed drawing sheets containing formal versions of Figures 5-7, 9, 15A and 15B for the corresponding drawing sheets currently in the application.

2. The Commissioner is hereby authorized to charge any other fees under 37 CFR §1.16 and §1.17 that may be required , or credit any overpayment, to our Deposit Account No. 02-3038.

Respectfully submitted,

Bruce D. Jobse
Date: 10/22/99

Bruce D. Jobse, Esq. /Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

RECEIVED
OCT 26 1999
Publishing Division
10

$B

TRANSMITTAL LETTER	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland
Serial No:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

OIPE
OCT 25 1999
PATENT & TRADEMARK OFFICE

Assistant Commissioner for Patents
Washington, D.C. 20231

Enclosures

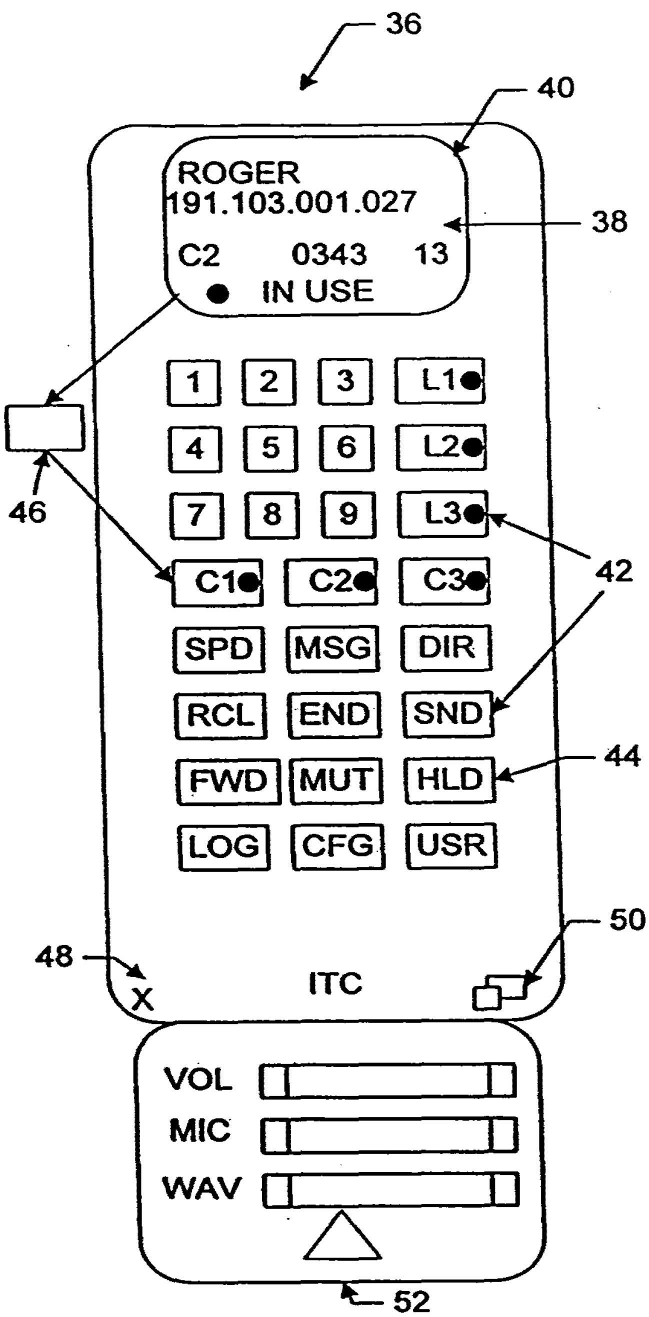
- ☐ Affidavit under 37 C.F.R. 1.131
- ☐ Assignment Papers
- ☐ Change of Correspondence Address
- ☒ Extension of Time Request
- ☐ Declaration/Power of Attorney
- ☐ Fee Transmittal Form
- ☐ Information Disclosure Statement
- ☐ Invention Disclosure Document
- ☐ Notice of Appeal
- ☐ Petition and Petition Routing Slip
- ☐ Power of Attorney Form
- ☐ PTO-1449 Form(s)
- ☐ Request for Certified Copies
- ☐ Request for Corrected Filing Receipt
- ☐ Copy of Original Filing Receipt
- ☐ Request for Reconsideration
- ☐ Request for Refund
- ☐ Response to Missing Parts
- ☐ Return Receipt Postcard
- ☒ 5 Sheets Formal Drawing(s)
- ☐ Small Entity Statement
- ☐ Status Letter
- ☐ Terminal Disclaimer
- ☒ Other: Letter to Official Draftsperson; and Check for $110.00

Bruce D. Jobse

Date: 10/22/99

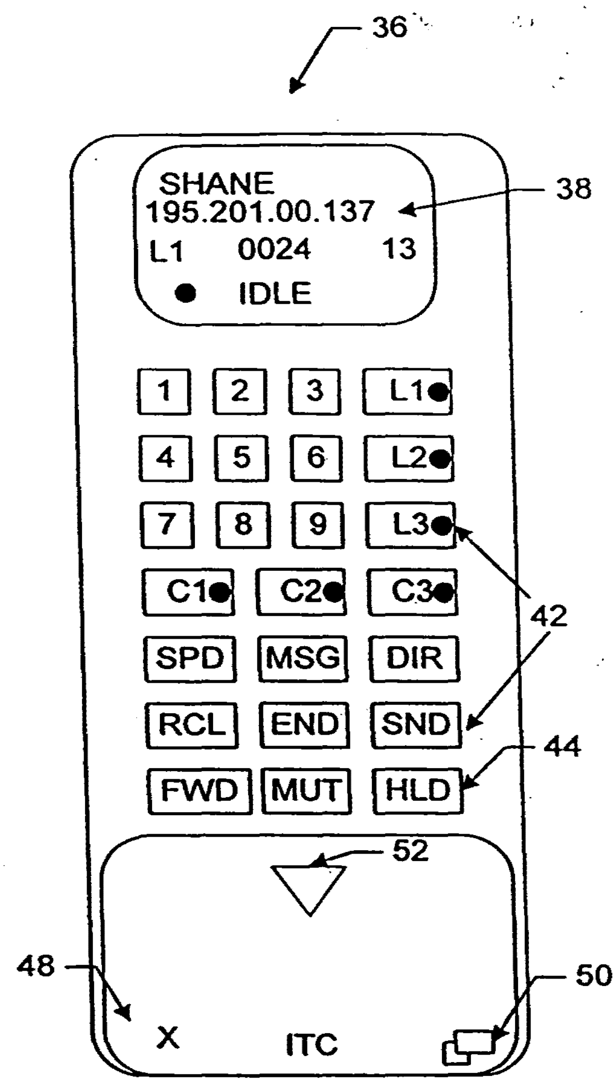
Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

RECEIVED
OCT 26 1999
Publishing Division
10



36
40
ROGER
191.103.001.027
38
C2 0343 13
IN USE
46
1
2
3
L1
4
5
6
L2
7
8
9
L3
C1
C2
C3
42
SPD
MSG
DIR
RCL
END
SND
FWD
MUT
HLD
44
LOG
CFG
USR
48
50
X
ITC
VOL
MIC
WAV
52

FIG. 5



36
SHANE
195.201.00.137
38
L1 0024 13
IDLE
1
2
3
L1
4
5
6
L2
7
8
9
L3
C1
C2
C3
42
SPD
MSG
DIR
RCL
END
SND
44
FWD
MUT
HLD
52
48
50
X
ITC

FIG. 6

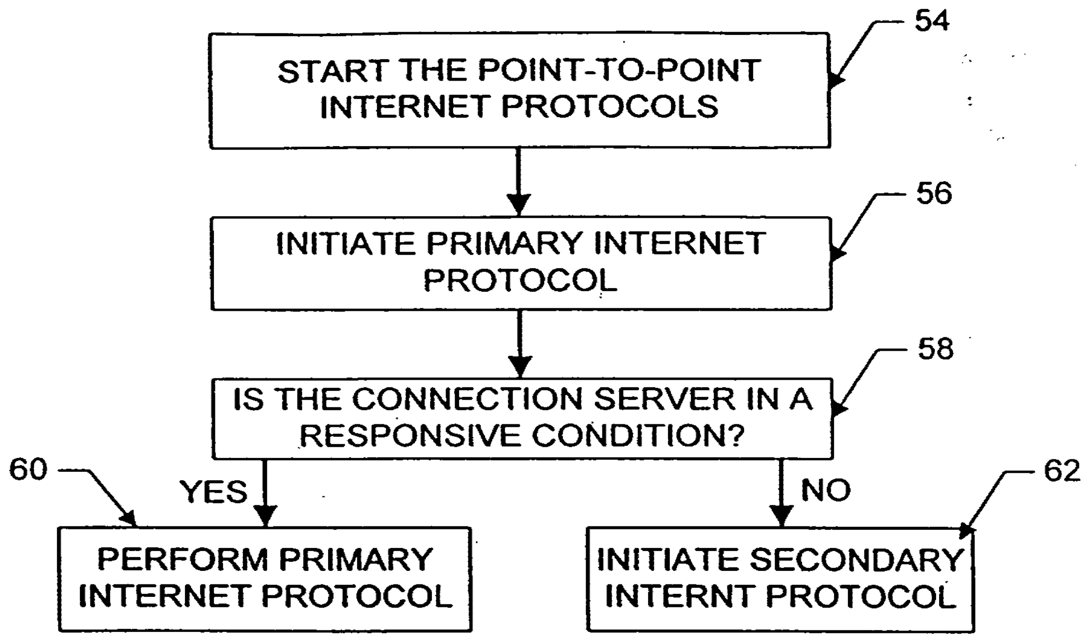

54
START THE POINT-TO-POINT INTERNET PROTOCOLS
56
INITIATE PRIMARY INTERNET PROTOCOL
58
IS THE CONNECTION SERVER IN A RESPONSIVE CONDITION?
60
YES
NO
62
PERFORM PRIMARY INTERNET PROTOCOL
INITIATE SECONDARY INTERNT PROTOCOL

FIG. 7

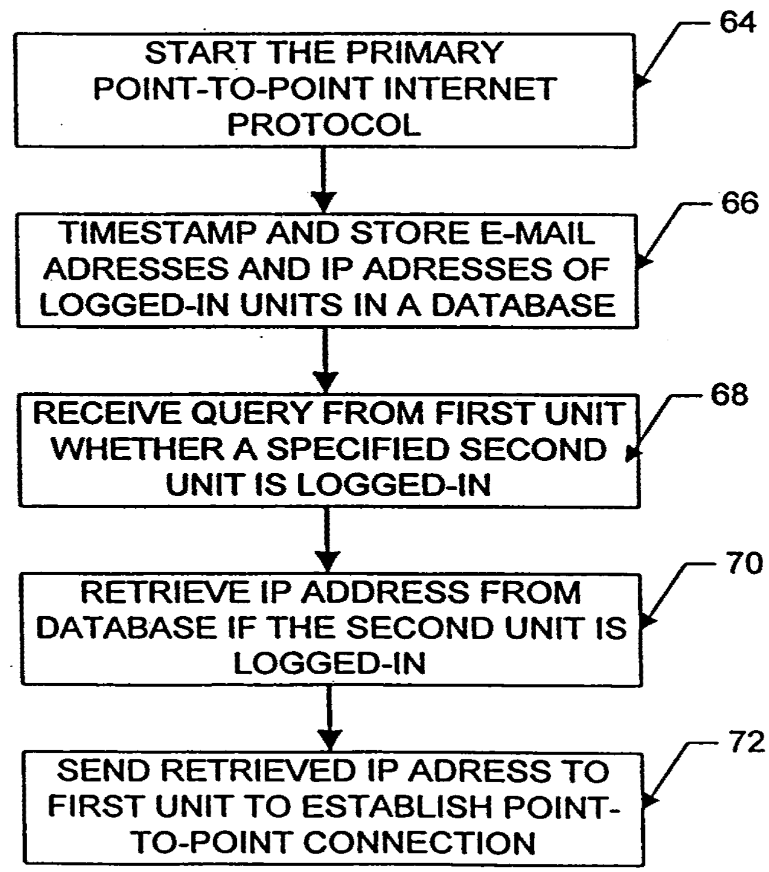

64
START THE PRIMARY POINT-TO-POINT INTERNET PROTOCOL
66
TIMESTAMP AND STORE E-MAIL ADRESSES AND IP ADRESSES OF LOGGED-IN UNITS IN A DATABASE
68
RECEIVE QUERY FROM FIRST UNIT WHETHER A SPECIFIED SECOND UNIT IS LOGGED-IN
70
RETRIEVE IP ADDRESS FROM DATABASE IF THE SECOND UNIT IS LOGGED-IN
72
SEND RETRIEVED IP ADRESS TO FIRST UNIT TO ESTABLISH POINT-TO-POINT CONNECTION

FIG. 8

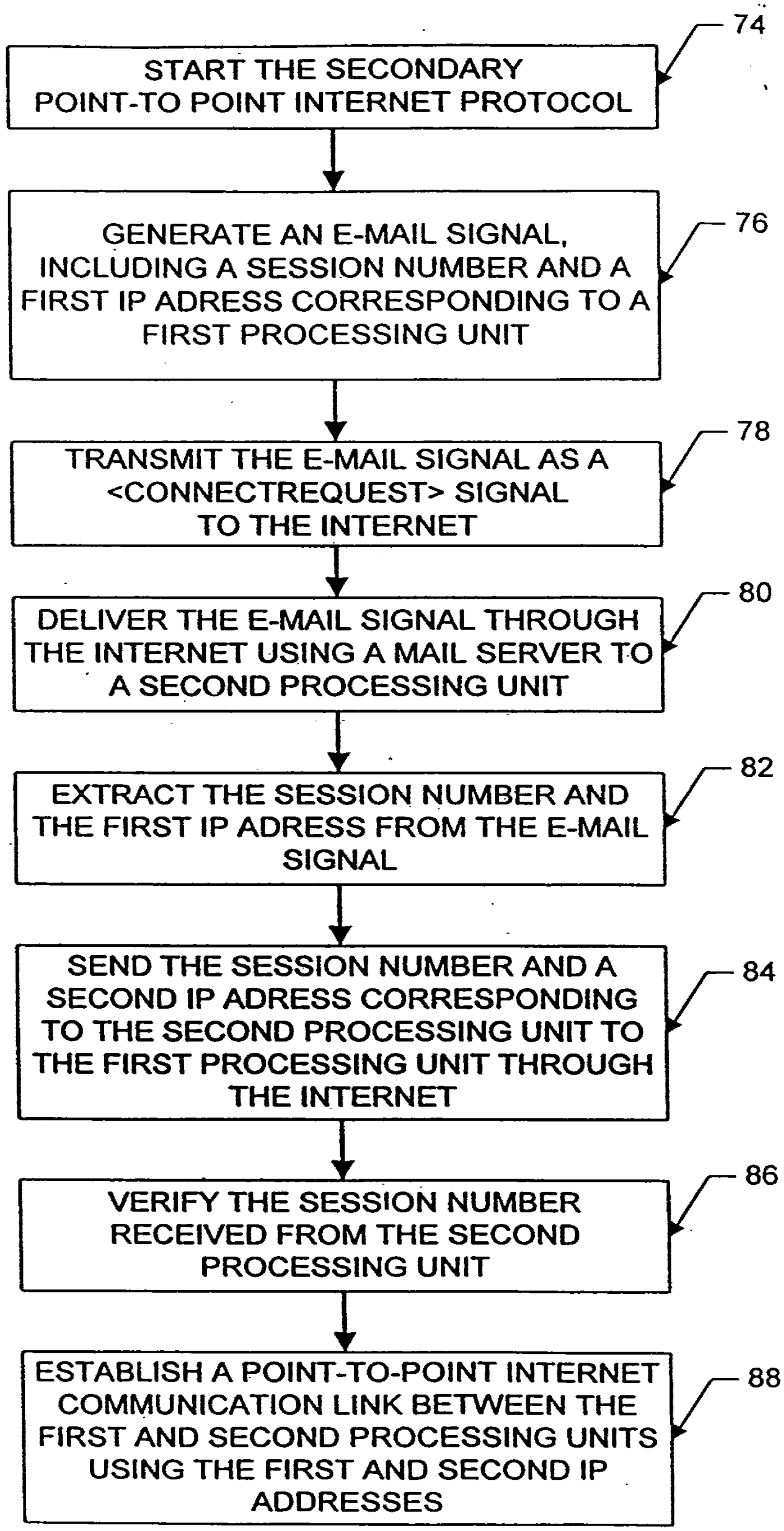

74
START THE SECONDARY POINT-TO POINT INTERNET PROTOCOL
76
GENERATE AN E-MAIL SIGNAL, INCLUDING A SESSION NUMBER AND A FIRST IP ADRESS CORRESPONDING TO A FIRST PROCESSING UNIT
78
TRANSMIT THE E-MAIL SIGNAL AS A <CONNECTREQUEST> SIGNAL TO THE INTERNET
80
DELIVER THE E-MAIL SIGNAL THROUGH THE INTERNET USING A MAIL SERVER TO A SECOND PROCESSING UNIT
82
EXTRACT THE SESSION NUMBER AND THE FIRST IP ADRESS FROM THE E-MAIL SIGNAL
84
SEND THE SESSION NUMBER AND A SECOND IP ADRESS CORRESPONDING TO THE SECOND PROCESSING UNIT TO THE FIRST PROCESSING UNIT THROUGH THE INTERNET
86
VERIFY THE SESSION NUMBER RECEIVED FROM THE SECOND PROCESSING UNIT
88
ESTABLISH A POINT-TO-POINT INTERNET COMMUNICATION LINK BETWEEN THE FIRST AND SECOND PROCESSING UNITS USING THE FIRST AND SECOND IP ADDRESSES

FIG. 9

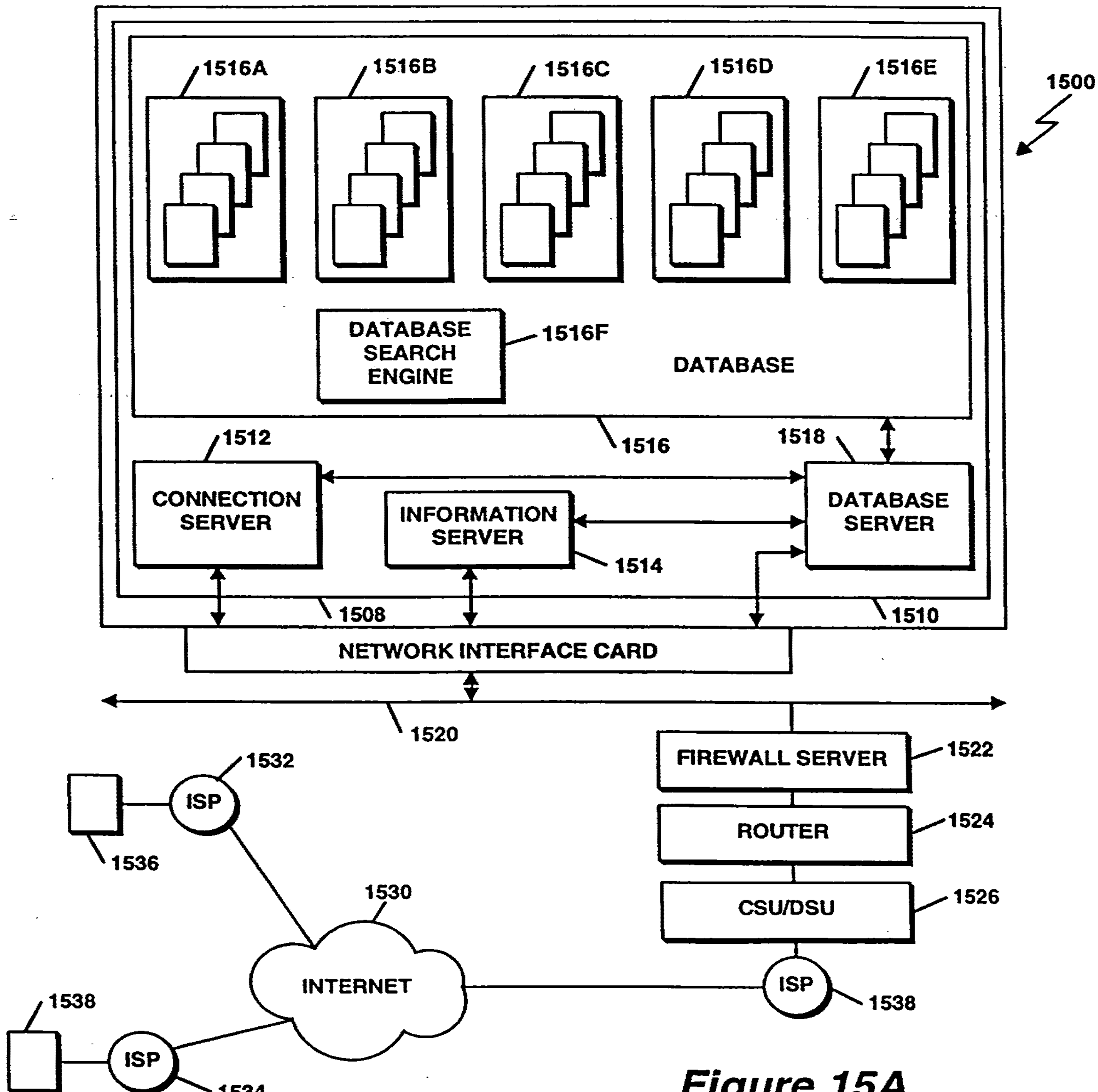

1516A
1516B
1516C
1516D
1516E
1500
DATABASE SEARCH ENGINE
1516F
DATABASE
1512
1516
1518
CONNECTION SERVER
INFORMATION SERVER
DATABASE SERVER
1514
1508
1510
NETWORK INTERFACE CARD
1520
FIREWALL SERVER
1522
1532
ISP
1536
ROUTER
1524
1530
CSU/DSU
1526
INTERNET
ISP
1538
1538
ISP
1534

Figure 15A

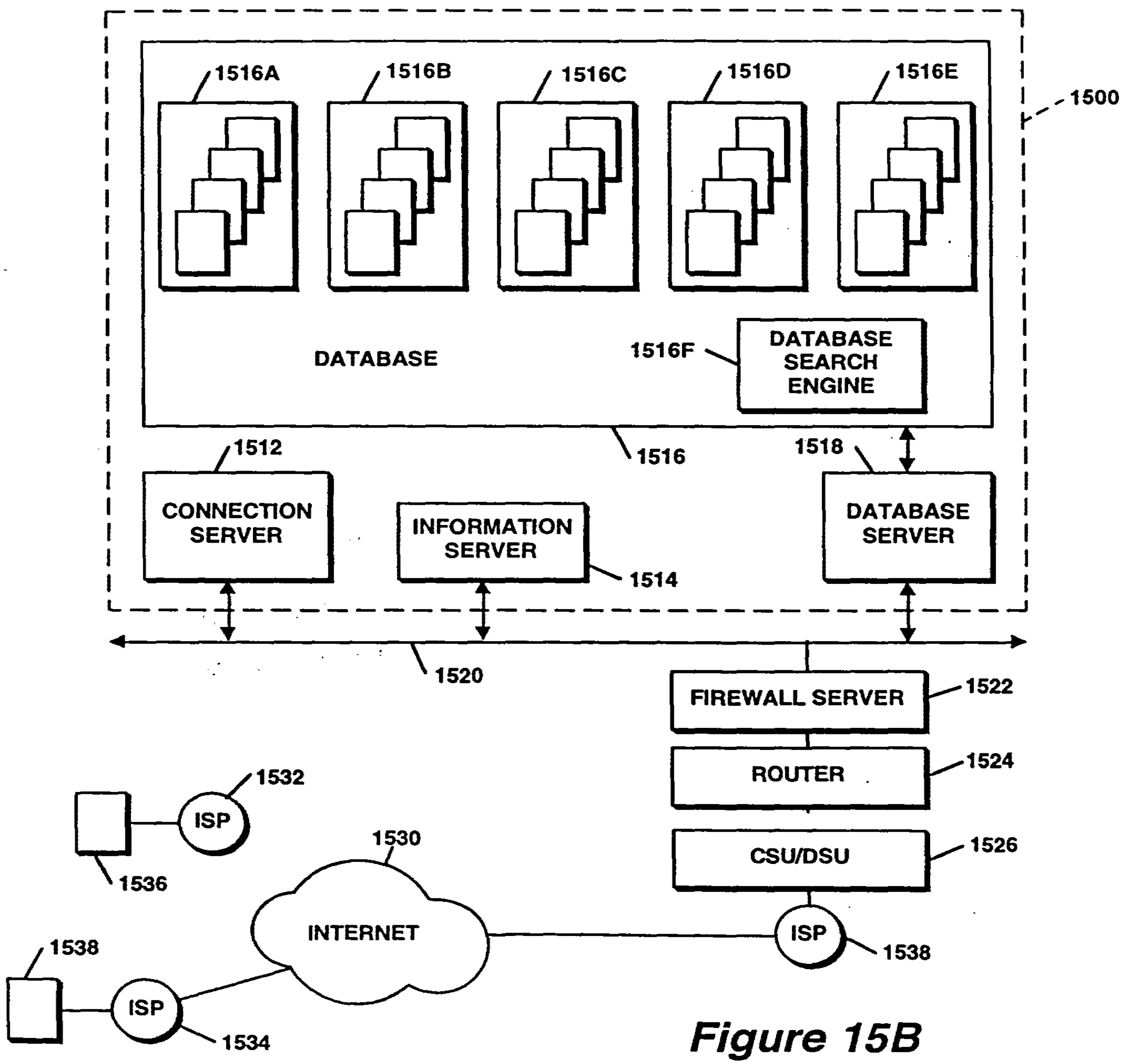

1516A
1516B
1516C
1516D
1516E
1500
DATABASE
1516F
DATABASE SEARCH ENGINE
1512
1516
1518
CONNECTION SERVER
INFORMATION SERVER
1514
DATABASE SERVER
1520
FIREWALL SERVER
1522
ROUTER
1524
1532
ISP
1530
CSU/DSU
1526
1536
INTERNET
ISP
1538
1538
ISP
1534

Figure 15B

PETITION FOR EXTENSION OF TIME UNDER 37 CFR §1.136(a)	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland
Serial No:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: **EL401821480US**
Date of Deposit: **October 22, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed Assistant Commissioner for Patents, Box Issue Fee, Washington, D.C. 20231.

Jan L. Mellen
Jan L. Mellen

Assistant Commissioner for Patents
Box Issue Fee
Washington, D.C. 20231

This is a request under the provisions of 37 C.F.R. §1.136(a) to extend the period for filing a response in the above-identified application up to, and including, October 22, 1999.

Small Entity

- ☐ A small entity statement under 37 C.F.R. §1.27 has already been filed.
- ☐ A small entity statement under 37 C.F.R. §1.27 is attached

Extension

The requested extension and the appropriate fee are as follows:

☒	One month (37 C.F.R. §1.17(a)(1))	$110.00
☐	Two months (37 C.F.R. §1.17(a)(2))	
☐	Three months (37 C.F.R. §1.17(a)(3))	
☐	Four months (37 C.F.R. §1.17(a)(4))	
☐	Five months (37 C.F.R. §1.17(a)(5))	
	Reduction by one-half for request by small entity	
	Total Fee:	$110.00

Payment

- ☒ A check in the amount of the extension fee is enclosed.
- ☐ The extension fee is included in a fee payment made in connection with papers accompanying this petition.

☐ Charge the extension fee to deposit account no. 02-3038. A duplicate of this sheet is attached.

☒ The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §1.16 and §1.17 that may be required, or credit any overpayment, to deposit account no. 02-3038.

Bruce D. Jobse Date: 10/22/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

PETITION FOR EXTENSION OF TIME UNDER 37 CFR §1.136(a)	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland
Serial No:	08/721,316
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: **EL401821480US**
Date of Deposit: **October 22, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed Assistant Commissioner for Patents, Box Issue Fee, Washington, D.C. 20231.

Jan L. Mellen
Jan L. Mellen

Assistant Commissioner for Patents
Box Issue Fee
Washington, D.C. 20231

This is a request under the provisions of 37 C.F.R. §1.136(a) to extend the period for filing a response in the above-identified application up to, and including, October 22, 1999.

Small Entity

- ☐ A small entity statement under 37 C.F.R. §1.27 has already been filed.
- ☐ A small entity statement under 37 C.F.R. §1.27 is attached

Extension

The requested extension and the appropriate fee are as follows:

☒	One month (37 C.F.R. §1.17(a)(1))	$110.00
☐	Two months (37 C.F.R. §1.17(a)(2))	
☐	Three months (37 C.F.R. §1.17(a)(3))	
☐	Four months (37 C.F.R. §1.17(a)(4))	
☐	Five months (37 C.F.R. §1.17(a)(5))	
	Reduction by one-half for request by small entity	
	Total Fee:	$110.00

Payment

- ☒ A check in the amount of the extension fee is enclosed.
- ☐ The extension fee is included in a fee payment made in connection with papers accompanying this petition.

☐ Charge the extension fee to deposit account no. 02-3038. A duplicate of this sheet is attached.

☒ The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §1.16 and §1.17 that may be required, or credit any overpayment, to deposit account no. 02-3038.

Bruce D. Jobse Date: 10/22/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address : COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/721,316	09/25/96	MATTAWAY S	

021127 LM51/1116
KUDIRKA & JOBSE
TWO CENTER PLAZA
BOSTON MA 02108

EXAMINER	
RAMIREZ, E	
ART UNIT	**PAPER NUMBER**
2757	14

DATE MAILED: 11/16/99

The amendment filed 7/20/99 under Rule 312 has been considered, and has been:

1. ☒ entered.
2. ☐ entered as directed to matters of form not affecting the scope of the invention (0.3311).
3. ☐ disapproved. A report appears below.
4. ☐ entered in part. A report appears below.

By Direction of the Commissioner

Report:

Moustafa M. Meky
MOUSTAFA M. MEKY
PRIMARY EXAMINER

PLEASE FURNISH YOUR ZIP CODE IN ALL CORRESPONDENCE

FORM PTOL-271 (REV. 4/81)

COfC
#15
DGO
3-19-01

TRANSMITTAL LETTER	Docket No. N0003/7002

Applicant:	Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland
Serial No:	08/721,316
Patent No:	6,009,469
Filed:	September 25, 1996
For:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner:	E. Ramirez
Art Unit:	2757

OIPE JC104 JAN 0 2 2001 PATENT & TRADEMARK OFFICE

RECEIVED JAN 21 2001 CERTIFICATES OF CORRECTION

Assistant Commissioner for Patents
Washington, D.C. 20231

Enclosures

- ☐ Affidavit under 37 C.F.R. 1.131
- ☐ Assignment Papers
- ☐ Change of Correspondence Address
- ☐ Extension of Time Request
- ☐ Declaration/Power of Attorney
- ☐ Fee Transmittal Form
- ☐ Information Disclosure Statement
- ☐ Invention Disclosure Document
- ☐ Notice of Appeal
- ☐ Petition and Petition Routing Slip
- ☐ Power of Attorney Form
- ☐ PTO-1449 Form(s)
- ☒ Request for Certificate of Correction
- ☐ Request for Corrected Filing Receipt
- ☐ Copy of Original Filing Receipt
- ☐ Request for Reconsideration
- ☐ Request for Refund
- ☐ Response to Missing Parts
- ☒ Return Receipt Postcard
- ☐ Sheets Formal Drawing(s)
- ☐ Small Entity Statement
- ☐ Status Letter
- ☐ Terminal Disclaimer
- ☒ Other: Certificate of Correction; Copy of Amendment After Allowance; Copy of Approval of Amendment After Allowance

OK to issue. DGO 3-19-01

Bruce D. Jobse Date: 12/29/00

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

APPROVED
MAR 2 9 2001 LW
FOR THE DIRECTOR OF USPTO

REQUEST FOR CERTIFICATE OF CORRECTION	Docket No. N0003/7002

Applicant: Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland
Serial No: 08/721,316
Patent No: 6,009,469
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: E. Ramirez
Art Unit: 2757

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Assistant Commissioner for Patents, Washington, DC 20231 on December 29, 2000.

Frances M. Cunningham
Frances M. Cunningham

Assistant Commissioner for Patents
Washington, D.C. 20231

OIPE JC104 JAN 02 2001 PATENT & TRADEMARK OFFICE

ATTENTION: **Decision and Certificate of Correction**
Branch of the Patent Issue Division

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT FOR PTO MISTAKE (37 C.F.R. 1.322(a))

Applicant hereby requests the issuance of a Certificate of Correction for the above-referenced patent, the corrections being shown on the attached Certificate of Correction form. The corrections, as outlined on the Certificate of Correction, were previously submitted by Applicants with an Amendment After Allowance mailed July 20, 1999, a copy of which is attached. Such Amendment After Allowance was entered by the Examiner as indicated by the Office Action, Paper No. 14, dated November 16, 1999, a copy of which is also attached. Unfortunately, the amendments from the approved and entered Amendment after Allowance were not present in the above-identified patent at issuance. Since these errors in the text of the patent is the fault of the PTO, no fees are due for the filing of this request. The Commissioner is hereby authorized to charge any additional fees to Deposit Account No. 02-3038. Any questions regarding this matter may be directed to Attorney Bruce D. Jobse at the below-referenced number.

Respectfully submitted,

Bruce D. Jobse Date: 12/29/00

Bruce D. Jobse, Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO :6,009,469

DATED :December 28, 1999

INVENTOR(S) :Shane D. Mattaway, Glenn W. Hutton and Craig B. Strickland

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

IN THE CLAIMS:

In claim 1, column 41, line 23, after "having a display", please delete "and an audio transducer"; C

In claim 1, column 41, line 43, after "program code", please delete "means"; C

In claim 3, column 41, line 60, after "program code", please delete "means"; C

In claim 4, column 42, line 1, after "program code", please delete "means"; C

In claim 4, column 42, line 5, after "program code", please delete "means"; C

In claim 5, column 42, lines 8 and 9, after "having a display", please delete "and an audio transducer"; C

MAILING ADDRESS OF SENDER: KUDIRKA & JOBSE, LLP
Two Center Plaza
Boston, MA 02108

PATENT NO. 6,009,469

No. of additional copies

⇒ 10

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address : COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/721,316	09/25/96	MATTAWAY	S

1V0003/7002

021127 LM51/1116
KUDIRKA & JOBSE
TWO CENTER PLAZA
BOSTON MA 02108

EXAMINER	
RAMIREZ, E	
ART UNIT	PAPER NUMBER
2757	14

DATE MAILED: 11/16/99

File Folder
Client Info Access
Entry
Other

The amendment filed 7/20/99 under Rule 312 has been considered, and has been:

1. ☒ entered.
2. ☐ entered as directed to matters of form not affecting the scope of the invention (0.3311).
3. ☐ disapproved. A report appears below.
4. ☐ entered in part. A report appears below.

OIPE
JAN 0 2 2001
JC104
PATENT & TRADEMARK OFFICE

By Direction of the Commissioner

Report:

Moustafa M Meky
MOUSTAFA M. MEKY
PRIMARY EXAMINER

AMENDMENT TRANSMITTAL	Docket No. N0003/7002

Applicant: Shane D. Mattaway, et al.
Serial No. 08/721,316
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: E. Ramirez
Art Unit: 2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL445948665US
Date of Deposit: July 20, 1999

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, Box Issue Fee, Washington, D.C. 20231.

Frances M. Cunningham

Frances M. Cunningham

Assistant Commissioner for Patents
BOX ISSUE FEE
Washington, DC 20231

OIPE JC104 JAN 02 2001 PATENT & TRADEMARK OFFICE

Transmitted herewith for filing is the following:

Enclosures

☒ Amendment After Allowance
☐ Petition for a month Extension of Time
☒ Return Receipt Postcard

Small Entity

☐ A small entity statement under 37 C.F.R. §1.27 has already been filed.
☐ A small entity statement under 37 C.F.R. §1.27 is attached

Fees

Claims as Filed					
	Claims Filed	Highest Number Paid for	Number of Extra Claims	Rate	Additional Fees Due
Total Claims (37 CFR §1.16(c))	18	- 20 =	0 X	$18.00 =	$ 0.00
Independent Claims (37 CFR §1.16(b))	3	- 3 =	0 X	$78.00 =	$ 0.00
Extension Fee					$ 0.00
Reduction by 50% for filing by small entity					$ 0.00
Total Filing Fee					$ 0.00

Payment

☐ Check in the amount of the total filing fee.

☐ Charge Account No. 02-3038 in the amount of the total filing fee. A duplicate of this transmittal sheet is attached.

Authorization to Charge Additional Fees

☒ The Commissioner is hereby authorized to charge any additional fees under 37 C.F.R. §1.16 and §1.17 required by the attached papers and during the entire pendency of this application to Account No. 02-3038.

OIPE JC1004 JAN 0 2 2001 PATENT & TRADEMARK OFFICE

Bruce D. Jobse Date: 7/20/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

AMENDMENT AFTER ALLOWANCE UNDER 37 CFR §1.312(a)	Docket No. N0003/7002

Applicant: Shane D. Mattaway, et al.
Serial No. 08/721,316
Filed: September 25, 1996
For: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION
Examiner: E. Ramirez
Art Unit: 2757

CERTIFICATE OF EXPRESS MAILING

"Express Mail" mailing label number: EL445948665US
Date of Deposit: **July 20, 1999**

I hereby certify that the following Correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Commissioner of Patents and Trademarks, BOX ISSUE FEE, Washington, D.C. 20231.

Frances M. Cunningham

Frances M. Cunningham

OIPE JC104 JAN 0 2 2001 PATENT & TRADEMARK OFFICE

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to issuance, Applicants request the above-identified application be amended as follows:

In the Claims

1. (Thrice Amended) A computer program product for use with a computer system having a display [and an audio transducer], the computer system capable of executing a first process and connecting to other processes and a server process over a computer network, the computer program product comprising a computer usable medium having computer readable code means embodied in the medium comprising:

a. program code for generating a user-interface enabling control a first process executing on the computer system;

b. program code for determining the currently assigned network protocol address of the first process upon connection to the computer network;

c. program code responsive to the currently assigned network protocol address of the first process, for establishing a communication connection with the server process and for forwarding the assigned network protocol address of the first process and a unique identifier of the first process to the server process upon establishing a communication connection with the server process; and

d. program code [means], responsive to user input commands, for establishing a point-to-point communications with another process over the computer network.

3. (Thrice Amended) The computer program product of claim 2 wherein the program code for establishing a point-to-point communication link further comprise:

d.2 program code for transmitting, from the first process to the server process, a query as to whether the second process is connected to the computer network; and

d.3 program code [means] for receiving a network protocol address of the second process from the server process, when the second process is connected to the computer network.

4. (Thrice Amended) The computer program product of claim 2 wherein the program code for establishing a point-to-point communication link further comprises:

d.2 program code [means] for transmitting an E-mail message containing a network protocol address from the first process to the server process over the computer network;

d.3 program code [means] for receiving a second network protocol address from the second process over the computer network.

7. (Twice Amended) In a computer system having a display [and an audio transducer], the computer system capable of executing a first process and communicating with other processes and a server process over a computer network, a method for establishing point-to-point communications with other processes comprising:

A. determining the currently assigned network protocol address of the first process upon connection to the computer network;

B. establishing a communication connection with the server process once the assigned network protocol of the first process is known;

C. forwarding the assigned network protocol address of the first process to the server process upon establishing a communication connection with the server process; and

D. establishing a point-to-point communication with another process over the computer network.

Remarks

This application is currently under Allowance. A Notice of Allowance dated June 22, 1999 was mailed indicating that claims 1-4 and 7-20 are allowed. Applicants submit this Amendment to resolve minor informalities in the claim language.

Applicants have amended claims 1 and 7 to eliminate superfluous language. Specifically, the phrase "and an audio transducer" provided a basis for limitations recited in claims 5-6, previously cancelled. This term does not occur elsewhere in claims 1-4 and should be deleted. A similar change has been made to claim 7. The phrase "and an audio transducer" does not occur elsewhere in claims 7-9 and should be deleted. In the previous response mailed March 3,1999, claims 1-4 were amended to eliminate the term “means” from the claim language, however, several occurrences were overlooked. Applicant's submit additional amendments to claims 1, 3 and 4 to eliminate the term "means" from the claim language. These amendments are offered to conform the claims to 35 U.S.C. §112, 2nd paragraph, and are not necessitated or made in response to any rejection by the Examiner, or, in light of any reference cited by the Examiner.

No new matter or substantive issues are believed raised by this amendment. In light of the foregoing amendments and remarks, this application is now believed in condition for issuance and the Examiner is respectfully requested to advance this application to issuance. If the Examiner has any further questions regarding this Amendment, he is invited to call Applicants' attorney at the number listed below.

The Commissioner is hereby authorized to charge any fees or credits under 37 C.F.R. §1.16 and 1.17 to our deposit account No. 02-3038.

Respectfully submitted

Bruce D. Jobse Date: 7/20/99

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

RECEIVED
CENTRAL FAX CENTER
FEB 2 4 2006

FACSIMILE TRANSMISSION

COMPLETED

To: United States Patent and Trademark Office
Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

No. of Pages (including this page): 4

IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US IMMEDIATELY BY TELEPHONE AT (703) 894-6400.

USPTO: PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430

In re Patent Application of:	Attorney Docket No. 2655-0063
Shane D. Mattaway et al.	Group Art Unit: 2757
Patent No. 6,009,469	Confirmation No.: 2693
Issue date: December 28, 1999	Examiner: RAMIREZ, Ellis B.
Application Serial No. 08/721,316	Date: February 24, 2006
Filing date: September 25, 1996	
Title: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION	

Name(s) of paper(s) being transmitted:

- Transmittal
- General Power of Attorney
- Statement under 37 CFR 3.73(b)

CERTIFICATE OF FACSIMILE TRANSMISSION					
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.					
Name:	Amanda Sandusky	Signature: Amanda Sandusky		Date:	02/24/2006

CUSTOMER NUMBER
42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

RECEIVED
CENTRAL FAX CENTE
FEB 2 4 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION OF:

Shane D. Mattaway et al.		Atty. Dkt. No.:	2655-0063
Patent No.:	6,009,469	Art Unit:	2757
Issue Date:	December 28, 1999	Confirmation No.	2693
Appln. No.:	08/721,316	Examiner:	RAMIREZ, Ellis B.
Filing Date:	September 25, 1996	Date:	February 24, 2006
Title:	GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION		

TRANSMITTAL

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached please find the following documents, submitted for filing in connection with the above-identified application:

☒ General Power of Attorney

☒ Statement under 37 C.F.R. § 3.73(b)

Our Deposit Account No.: 501860 Our Order No. (Client-Matter No.): 2655-0063

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official document under Rule 20, or credit any overpayment, to our Account/Order Nos. (or Attorney Docket No.) shown in the heading hereof for which purpose a duplicate copy of this paper is attached.

This Charge Statement does not authorize charge of the issue fee until/unless an issue fee transmittal form is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,

By: Michael R. Casey

Michael R. Casey, Ph.D.
Registration No. 40,294

Davidson Berquist Jackson & Gowdey LLP

PTO/SB/80 (04-05)
Approved for use through 11/30/2005. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

[X] Practitioners associated with the Customer Number: **42624**

OR

[ ] Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

[X] The address associated with Customer Number: **42624**

OR

[ ] Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

Assignee Name and Address:
NET2PHONE, INC.
520 Broad Street, 8th Floor
Newark, New Jersey 07102

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	9/1/2005
Name	Glenn J. Williams	Telephone	(973) 438-6066
Title	Executive Vice President, General Counsel		

RECEIVED
CENTRAL FAX CENTER
FEB 2 4 2006

STATEMENT UNDER 37 CFR 3.73(b)

Applicant / Patent Owner: Net2Phone, Inc. Attorney Docket No.: 2655-0063

Application No. / Patent No. 6,009,469 Filed / Issue Date: December 28, 1999

Entitled: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

Assignee: Net2Phone, Inc. A Delaware Corporation

States that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
   The extent (by percentage) of its ownership interest is % in the patent application / patent identified above by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application / patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application / patent identified above, to the current assignee shown below:

1. From: Shane D. Mattaway, Craig Strickland To: NetSpeak Corporation
   The document was recorded in the United States Patent and Trademark Office at Reel 008311 Frame 0785, or for which a copy thereof is attached.
2. From: Glenn W. Hutton To: NetSpeak Corporation
   The document was recorded in the United States Patent and Trademark Office at Reel 008448 Frame 0779, or for which a copy thereof is attached.
3. From: NetSpeak Corporation To: VoIP Technology Holdings, LLC
   The document was recorded in the United States Patent and Trademark Office at Reel 016522 Frame 0205, or for which a copy thereof is attached.
4. From: VoIP Technology Holdings, LLC To: Net2Phone, Inc.
   The document was recorded in the United States Patent and Trademark Office at Reel 016945 Frame 0858, or for which a copy thereof is attached.

☐ Copies of assignments or other documents in the chain of title are attached.

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

By: Michael R. Casey
Michael R. Casey, Ph.D.
Registration No. 40,294

Date: February 24, 2006

Telephone No.: (703) 894-6406

Title: Attorney

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
08/721,316	09/25/1996	SHANE D. MATTAWAY	

CONFIRMATION NO. 2693

OC000000019645740

JEFFREY S. GINSBERG, ESQ.
KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

Date Mailed: 07/18/2006

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/24/2006.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

DDurham

DESHAWN D DURHAM
OIPE (703) 308-9010

OFFICE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
08/721,316	09/25/1996	SHANE D. MATTAWAY	2655-0063

CONFIRMATION NO. 2693

OC000000019645760

42624
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

Date Mailed: 07/18/2006

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/24/2006.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

D. Durham

DESHAWN D DURHAM
OIPE (703) 308-9010

OFFICE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
Alexandria, Virginia 22313

Patent No. 6,009,469

Paper No. ____

NOTICE OF *EX PARTE* REEXAMINATION

Notice is hereby given that a request for *ex parte* reexamination of U.S. Patent No. 6,009,469 was filed on 2-26-04 under 35 U.S.C. 302 and 37 CFR 1.510(a).

The reexamination proceeding has been assigned Control No. 90/010,422

This Notice incorporates by reference into the patent file, all papers entered into the reexamination file.

Note: This Notice should be entered into the patent file and given a paper number.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

POWER OF ATTORNEY, CORRESPONDENCE ADDRESS AND REVOCATION OF PRIOR POWERS

OIPE
MAR 13 2009
PATENT & TRADEMARK OFFICE

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Revocation: I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

Power of Attorney: I hereby appoint the practitioners associated with customer number **42624**, individually and collectively, as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

I authorize Davidson Berquist Jackson & Gowdey, LLP to delete names/numbers of persons no longer with the Firm and to act and rely on instructions from and communicate directly with the entity who first sent this case to them and by whom I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Davidson Berquist Jackson & Gowdey, LLP in writing to the contrary.

Correspondence Address: Please recognize or change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to the address associated with Customer Number **42624**.

Assignee Name and Address:

Net2Phone, Inc.
520 Broad Street, 8th Floor
Newark, New Jersey 07102

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record The individual whose signature and title is supplied below is authorized to act on behalf of the assignee			
Signature		Date	3/12/09
Name	JAMES RAPANN	Telephone	973 438 3253
Title	EVP & DIRECTOR		

OIPE
MAR 1 3 2009
PATENT & TRADEMARK OFFICE

08721316

IFW

STATEMENT UNDER 37 CFR 3.73(B)

Applicant / Patent Owner: Net2Phone, Inc. Docket No. 2655-0063

Patent No. 6,009,469 Filed / Issued Date: 12/28/1999

Entitled: GRAPHIC USER INTERFACE FOR INTERNET TELEPHONY APPLICATION

Assignee: Net2Phone, Inc. A corporation
(Name of assignee) (Type of Assignee: corporation, partnership, university, government agency, etc.)

States that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
(The extent (by percentage) of its ownership interest is %)

in the patent application / patent identified above by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application / patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel , Frame , or for which a copy thereof is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application / patent identified above, to the current assignee shown below:

1.	From: MATTAWAY, Shane D. et al. To: Netspeak Corporation The document was recorded in the United States Patent and Trademark Office at Reel 008311 Frame 0785, or for which a copy thereof is attached.
2.	From: HUTTON, Gleen W. To: Netspeak Corporation The document was recorded in the United States Patent and Trademark Office at Reel 008448 Frame 0779, or for which a copy thereof is attached.
3.	From: Netspeak Corporation To: VOIP Technology Holdings, LLC The document was recorded in the United States Patent and Trademark Office at Reel 016522 Frame 0205, or for which a copy thereof is attached.

☒ Additional documents in the chain of title are listed on a supplemental sheet.

☒ Copies of assignments or other documents in the chain of title are attached.

As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[Note: A separate copy (*i.e.,* a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Michael R. Casey
Signature

3/13/09
Date

Michael R. Casey, Ph.D
Printed or Typed Name

703-894-6400
Telephone Number

Title: Attorney, Registration No. 40,294

STATEMENT UNDER 37 CFR 3.73(B)
Continued

4.	From: VOIP Technology Holdings, LLC To: Net2Phone, Inc. The document was recorded in the United States Patent and Trademark Office at Reel 016945 Frame 0858, or for which a copy thereof is attached.
5.	From: Netspeak Corporation To: Net2Phone, Inc. The document was recorded in the United States Patent and Trademark Office at Reel 016945 Frame 0890, or for which a copy thereof is attached.
6.	From: VOIP Technology Holdings, LLC To: Net2Phone, Inc. The document was recorded in the United States Patent and Trademark Office at Reel 017105 Frame 0240, or for which a copy thereof is attached.

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Virginia on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:12CV 8	1/11/12	for the Eastern District of Virginia 600 Granby St, Norfolk, VA 23510

PLAINTIFF	DEFENDANT
INNOVATIVE COMMUNICATIONS TECHS., INC.	OOVOO, LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469	12/28/1999	INNOVATIVE COMMUNICATIONS TECHNOLOGIES, INC.
2 6,701,365	3/2/2004	INNOVATIVE COMMUNICATIONS TECHNOLOGIES, INC.
3 6,513,066	1/28/2003	INNOVATIVE COMMUNICATIONS TECHNOLOGIES, INC.
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Fernando Galindo	R. Simmons	1/11/2012

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Virginia on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:12cv8	1/4/2012	Eastern District of Virginia

PLAINTIFF	DEFENDANT
Innovative Communications Technologies, Inc.	ooVoo, LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,513,066	12/28/1999	Innovative Communications Technologies, Inc.
2 6,701,365	3/2/2004	Innovative Communications Technologies, Inc.
3 6,009,469	1/28/2003	Innovative Communications Technologies, Inc.
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
10/11/2012 Stipulation of Dismissal filed

CLERK	(BY) DEPUTY CLERK	DATE
Fernando Galindo	R. Simmons	10/12/2012

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Virginia on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
3:13CV503	8/2/2013	Richmond

PLAINTIFF	DEFENDANT
Straight Path IP Group, Inc.	Toshiba Corporation Toshiba America, Inc. Toshiba America Information Systems, Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469		
2 6,108,704		
3 6,131,121		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Fernando Galindo	Robert L. Walker	8/8/2013

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Virginia on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:13cv934	8/1/2013	Eastern District of Virginia

PLAINTIFF	DEFENDANT
Straight Path IP Group, Inc.	Vizio, Inc., et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469	12/28/1999	NetSpeak Corporation
2 6,108,704	8/22/0200	NetSpeak Corporation
3 6,131,121	10/10/2000	NetSpeak Corporation
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Virginia - Norfolk Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:13cv427	8/1/2013	for the Eastern District of Virginia - Norfolk Division

PLAINTIFF	DEFENDANT
STRAIGHT PATH IP GROUP, INC.	SONY CORPORATION, et al

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469	12/28/1999	Straight Path IP Group, Inc.
2 6,108,704	8/22/2000	Straight Path IP Group, Inc.
3 6,131,121	10/10/2000	Straight Path IP Group, Inc.
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Fernando Galindo	Brad Newell	8/2/2013

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Virginia on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:13cv936	8/1/2013	Eastern District of Virginia

PLAINTIFF	DEFENDANT
Straight Path IP Group, Inc.	Sharp Corp., et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469	12/28/1999	NetSpeak Corporation
2 6,108,704	8/22/2000	NetSpeak Corporation
3 6,131,121	10/10/2000	NetSpeak Corporation
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Virginia - Alexandria on the following

☐ Trademarks or ☒ Patents . (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:13cv935-GBL/TCB	8/1/2013	Eastern District of Virginia - Alexandria Division

PLAINTIFF	DEFENDANT
Straight Path Group, Inc.	Panasonic Corporation of North America, et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469	12/28/1999	NetSpeak Corporation
2 6,108,704	8/22/2000	NetSpeak Corporation
3 6,131,121	10/10/2000	NetSpeak Corporation
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
FERNANDO GALINDO		

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Virginia on the following

☐ Trademarks or ☒ Patents . (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:13cv933	8/1/2013	Eastern District of Virginia

PLAINTIFF	DEFENDANT
Straight Path IP Group, Inc.	LG Electronics, Inc. LG Electronics U.S.A., Inc. LG Electronics MobileComm U.S.A., Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,009,469	12/28/1999	Netspeak Corporation
2 6,108,704	8/22/2000	NetSpeak Corporation
3 6,131,121	10/10/2000	NetSpeak Corporation
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		FILED
3		AUG - 6 2013
4		CLERK, U.S. DISTRICT COURT
5		ALEXANDRIA, VIRGINIA

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Fernando Galindo		8/6/2013

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy