

**PCT**WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau

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

<b>(51) International Patent Classification <sup>6</sup> :</b> <b>H01J 13/00</b>	<b>A2</b>	<b>(11) International Publication Number:</b> <b>WO 99/13486</b> <b>(43) International Publication Date:</b> 18 March 1999 (18.03.99)
<b>(21) International Application Number:</b> PCT/US98/18943 <b>(22) International Filing Date:</b> 11 September 1998 (11.09.98)  <b>(30) Priority Data:</b> 08/929,162                      12 September 1997 (12.09.97)      US  <b>(71) Applicant:</b> SUN MICROSYSTEMS INC. [US/US]; 901 San Antonio Road, MS Pali-521, Palo Alto, CA 94303 (US). <b>(72) Inventor:</b> KALAJAN, Kevin, E.; 2900 Broadway #F, Redwood City, CA 94062 (US). <b>(74) Agent:</b> SOBON, Wayne, P.; Fish & Richardson P.C., Suite 100, 2200 Sand Hill Road, Menlo Park, CA 94025 (US).		<b>(81) Designated States:</b> CA, IL, JP, MX, NO, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Published</b> <i>Without international search report and to be republished upon receipt of that report.</i>
<b>(54) Title:</b> SOURCE ADDRESS DIRECTED MESSAGE DELIVERY  <b>(57) Abstract</b>  A method for delivering a message unit to a destination network resource within a transport communications layer includes the steps of configuring a mapping to the destination network resource based upon a source address of the message unit, and sending the message unit to the destination network resource based upon the mapping.		

**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.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SOURCE ADDRESS DIRECTED MESSAGE DELIVERYBACKGROUND

5 The present invention relates generally to  
electronic communications.

10 Networks provide communication sessions between  
clients and servers where, generally speaking, clients  
request information provided by servers. Some networks  
provide a high degree of security, so that messages  
15 passing between clients and servers are protected from  
unauthorized interception, reading, or tampering. Other  
networks, particularly more public networks such as the  
Internet, do not themselves necessarily protect from  
unauthorized reception of messages. Communications  
20 sessions and messages can be encoded to lend a degree of  
protection.

In addition, servers on public networks are  
vulnerable to discovery by unauthorized users, who can  
try to "hack" into such servers to obtain otherwise  
25 confidential information. Fire walls have been developed  
which help protect against unwanted intruders. Users,  
after logging onto a public network server, can be  
identified by any of a number of schemes (e.g.,  
passwords), and then be transferred to other servers to  
30 access more sensitive information.

Network clients, especially Internet clients, often  
access the Internet through routers, or proxies. For  
example, a network client may be a particular user on a  
local area network (LAN). The network client may not  
35 have a valid Internet address, but may have a valid  
TCP/IP address (certain ranges of IP addresses are called  
"private" or "invalid" addresses and can be used within  
an organization's LAN but do not work over the Internet).  
Nonetheless, the network client can send and receive  
40 messages via the Internet by having those messages  
communicated through a device which does have a valid  
Internet address. For example, e-mail clients can access

e-mails sent and received via the Internet from their e-mail server attached to their LAN, which in turn can attach to an Internet server which has a valid IP address and is attached to the Internet. The Internet has protocols (e.g., IMAP) for constructing and addressing e-mail messages so that e-mail clients properly receive their e-mail.

Computer users may also desire to access information that exists on particular computers attached to a LAN.

One method for doing so requires a direct connection between the computer user and the LAN resource. For example, an employee can directly call (via a modem) a LAN computer that has a dedicated telephone port. A number of remote access applications provide for such connections. Such remote access applications allow the employee to remotely control and view the operations of a work computer, e.g., the employee's desktop computer, or a special computer having access to common LAN files at work.

However, if the employee wishes to have more flexible access to a LAN resource, for example, by using an existing remote access application but over the Internet instead of through a dedicated phone connection, there are some difficulties. Apart from securing the communication session itself (by, e.g., encryption), typical LAN resources do not have their own, Internet-acceptable, IP addresses. For example, an employee's LAN computer might have a LAN address of "10.0.0.3." Should message packets be sent to or from that LAN computer with that address, typical Internet routers will drop them as having improper IP addresses.

One might try using some form of network address translation (NAT), which operates at the IP layer, to translate improper LAN addresses to some other arbitrary proper IP address, and back again. However, such a method would require a translation of each message

packet's address, a recalculation of the checksum of the packet, and then a rewriting of the packet for delivery.

Even if a LAN resource has a proper IP address, it might not be desirable to make it known. For example, a firm might want several clients to have access to subsets of information applicable to each client separately, but not give that client access to other clients' information. The firm might put the information on a common Internet server, behind a firewall, and allocate client access by Uniform Resource Locator (URL): e.g., one client accesses information at `http:// . . . //client A`, another client at `http:// . . . //client B`. However, it can be difficult to develop a sufficiently complex set of different URLs for a variety of clients that is not also susceptible to someone figuring out its organization and accessing protected data.

LAN administrators may not want to give a LAN resource its own IP address, but also may not want to give others (for example, clients) network address translation information, since that information can include sensitive specifics about the LAN configuration. Also, administrators may not want any information about the location of a particular resource sent through the Internet, to lessen the chance others might locate the resource without authorization and try to break into it.

#### SUMMARY

In general, in one aspect, the invention features a method for delivering a message unit to a destination network resource within a transport communications layer including the steps of configuring a mapping to the destination network resource based upon a source address of the message unit, and sending the message unit to the destination network resource based upon the mapping.

Embodiments of the invention may include one or more of the following features. The source address can be the source IP address of the message unit, or the source IP

address and source port number of the message unit. The destination network resource can have a network resource address to which the message unit is sent. The network resource address might not be a valid Internet IP address, or might be a network address on a local area network. Configuring the mapping can include writing a table that maps the source address of the message unit and a network resource address for the destination network resource. The table can map a host address and the host port number for the destination network resource. The mapping can be configured to send message units to destination network resources based upon source addresses of the message units. The source addresses can be source IP addresses, or source IP addresses and source port numbers for the message units. Configuring the mapping can include recording the source IP address of a latest-received connection request. The message unit can be a single message sent during a connection-oriented transport session, and the session can be a TCP session. The message unit can be a datagram sent during a connectionless transport session, and the session can be a UDP session.

In general, in another aspect, the invention features a storage device tangibly storing a control program. The control program, when coupled to a control device, operates the control device to deliver a message unit to a destination network resource within a transport communications layer. The control program is configured to operate the control device to perform the functions of: configuring a mapping to the destination network resource based upon a source address of the message unit, and sending the message unit to the destination network resource based upon the mapping.

Advantages of the invention may include one or more of the following. Clients can access destination network resources through available transport protocols, even if those resources do not have proper network addresses, or

where those addresses remain secret. Employees can access their own desktop computers, ordinarily not having proper IP addresses, over the Internet using existing remote access applications. By conducting remote access sessions through Internet transport protocols, existing Internet encryption protocols (e.g., SSL as part of HTTPS) can be added to such sessions without any modification of the underlying remote access applications. Clients can be allocated access to resources based solely upon their source IP address information. This can lessen the risk that others, not having that address information, will become aware of such resources or try to break into them. A client can be authorized access dynamically, so that a traveling employee can access his or her desktop computer from anywhere. The client does not require detailed information about the network location of the LAN resource: no translation details need to be given to the client, either in advance, or through the Internet, to allow access. The client can simply be told the address of a proxy server, but not the IP address of the destination network resource.

These and other features and advantages of the present invention will become more apparent from the following description, drawings, and claims.

#### DRAWINGS

Figure 1 is a schematic of a network having a server allowing access to LAN resources.

Figure 2 is a schematic of a message routing application on the server for routing messages.

Figure 3 is a diagram of a address mapping table.

Figure 4 is a schematic of multiple instances of a message routing application.

Figure 5 is a flow chart for message routing between a client and a destination network resource.

Figure 6 is a block diagram of a machine-readable device encoded with software for generating a message routing application.

5

#### DESCRIPTION

Referring to Figure 1, client 10 connects through network 16 to server 18. Client 10 typically has source port number 12 (which can vary by message and by communication session) and source address 14, while server 18 has server port number 20 and server address 22. Client 10 can be, e.g., a traveling employee seeking direct access to his or her desktop computer at work, through an Internet connection. Network 16 can be the Internet (or, e.g., any Internet protocol (IP) network). The employee can access server 18 using a web browser, or other Internet communication software, using a computer (not shown) connected to the Internet via an Internet Service Provider (ISP). In this case, the ISP's source address is, for purposes of establishing a network connection, client source address 14. Where network 16 is an IP network, source address 14 is an IP address.

Local area network (LAN) 26 has one or more hosts 28a, 28b, and 28c that can represent various LAN resources. For example, host 28a can be the employee's desktop computer, having host destination address 30a with respect to LAN 26. Even though host 28a may not have a proper IP address for directly receiving and transmitting over the Internet, message routing application 24 within server 18 can route messages received from client 10 having source address 14 to the appropriate LAN resource (e.g., host 28a).

Referring also to Figure 2, message routing application 24 includes port monitor 32, message delivery module 34 and dynamic table update module 36. Port monitor 32 monitors one or more selected ports 20a (20b, 20c, etc.) of server 18 for incoming messages. When a client 10 having source address 14 makes a request for a

connection, port monitor 32 retrieves an entry in address mapping table 38 for that client's source address 14.

Referring also to Figure 3, address mapping table 38 is structured with fields (shown in header 46) representing respectively: first field 48a--source IP address (or source host name) 14 of requesting client 10; second field 48b--destination IP address (or destination host name) 30; and third field 48c--destination port number (or service name) 31. Destination IP address 30 and destination port number 31 are of a particular LAN resource 28 (or other destination or host IP address), the host being the resource to which client 10 wishes to be connected. For example, entry 50a of address mapping table 38 maps source address 14a to address 30a and port 31a, of host 1 (item 28a). Port monitor 32 retrieves the mapping information corresponding to a particular source address 14 from address mapping table 38 and passes it to message delivery module 34.

Message delivery module 34 handles all further communications between client 10 and host destination address 30a, in a manner transparent to client 10. Operating system (OS) 44 of server 18 receives messages having particular source address 14 and source port number 12, and passes those messages to their corresponding message delivery module 34, which, because of the mapping information received from address mapping table 38, then delivers those messages via LAN 26 to host 28a at host destination address 30a.

Depending upon the particular OS of server 18, message delivery module 34 may be configured as a single program that keeps track of all incoming messages mapped from a number of external clients 10 to a number of internal resources 28 having respective host destination addresses 30. Or, for example in the case of UNIX, message delivery module 34 may fork itself into a new instance for each new mapping, as shown in Figure 4. Each forked instance 34a, 34b, and 34c of message

delivery module 34 receives (from OS 44) only messages arriving respectively from clients 10a, 10b, 10c (having respective source addresses and port numbers). Each instance 34a, 34b, and 34c then delivers its respective  
5 messages to respective hosts 28a, 28b, and 28c. Another alternative, for a different type of OS (such as Windows), provides the message delivery module as a subroutine within message routing application 24, so that a new thread of the message delivery module subroutine is  
10 replicated for each mapping.

Regardless of method, message routing application 34 maintains separate communication sessions between particular clients 10 and particular hosts 28, based upon the source address 14 of clients 10. These sessions can  
15 be connection-oriented sessions (such as transport connection protocol (TCP) sessions) or can be connectionless sessions (such as unigram data protocol (UDP) sessions).

Address mapping table 38 can be updated  
20 periodically, e.g., by a LAN administrator using table maintenance module 40 (or the like) to add, edit, or delete individual mapping entries of address mapping table 38 so as to allow individual users to access particular hosts from external source addresses. For  
25 example, employees working from home through static source addresses could have those addresses entered into table 38, well in advance of any communication session between home and work. Or, address mapping table 38 can be updated dynamically, for example, at the start of a  
30 connection request, by, e.g., an employee seeking access to his or her desktop computer 28 while traveling, from a remote location having a previously unknown source address 14.

To dynamically route messages from a user from a new  
35 source address 14, the user can first access web application 42 provided by server 18 on the world wide web (WWW) of the Internet. Web application 42 can

authenticate the user using any of a number of authentication methods. For examples of such methods, see co-pending application serial number 08/928,360, filed on even date, entitled "Remote Access-Controlled Communications", incorporated herein by reference. Once the identity and authority of the user have been verified by web application 42, the user's information, including his or her source address 14, are passed to table maintenance module 40, which then passes that information directly into address mapping table 38. Or the information is passed to dynamic table update module 36 of message routing application 24. Dynamic table update module 36 then enters the new client mapping information into address mapping table 38, and passes the connection request onto port monitor 32 and message delivery module 34.

Where the first portion of the connection session is mediated over the world wide web of the Internet, using some variant of the HTTP protocol, Java application, ActiveX control, or another form of program or executable content sent over the public network, web application 42 may typically receive only a requesting client's source address 14, and possibly certain other identifying information sent during the session (such as an employee's name and one-time password, for example). The initial HTTP session is stateless, so the requesting client 10, while having a persistent source address 14, will not necessarily have a persistent source port number 12. Therefore, address mapping table 38 contains only one entry for each source address. The entry represents the latest received connection request from that source address, since any previous entry for that address (from, for example, another employee calling into server 18 from the same proxy server as another employee) is first deleted. The deletion poses no difficulties, though, for proper message delivery, even if a number of clients (employees) are calling in from the same source address.

Once message routing application 24 either looks up or modifies the users' information in address mapping table 38, retrieves the latest mapping for the source address, and causes message delivery module 34 to initiate a  
5 connection session between client 10 and host 28, client 10 typically starts using a persistent source port number 12, unique for that communication session from that source address 14. OS 44 automatically uses both the client's source address 14 and port number 12 to uniquely  
10 route messages received by server 18 to the appropriate forked instance, subroutine, or thread of message delivery module 34, which then uniquely handles that client's messages alone for that communication session. Another client, having the same source IP address 14 but  
15 a necessarily different port number 12, will be serviced by a different appropriate forked instance, subroutine, or thread of message delivery module 34.

Message routing application 24 transparently handles messages during a communication session and provides  
20 those messages to a particular destination network resource, based upon the origin (source address) of the messages. A user can simply connect to a web application 42, request a connection with a particular host 28, and the system can transparently handle the transport of  
25 messages to and from client 10 and host 28. In the case of remote access programs, after connection set-up, the remote access application will act as if it is simply remote accessing server 18, but will instead actually access host 28, via message routing application 24.  
30 Therefore, existing remote access programs can be used to access particular LAN resources without difficult alterations or reprogramming, and LAN administrators can securely limit who has access to particular resources, without passing any sensitive LAN address information  
35 over the public network.

Referring to Figure 5, a message delivery method 100 begins when client 10 having source address 14 requests a

connection to a destination network resource, e.g., host 28a (step 102). The initial configuration step can be managed by web application 42 (operating on server 18 or another web (HTTP) server 19, not shown). The initial  
5 configuration can be mediated through HTTP messages between client 10 and server 18 or 19. If the connection request is a dynamic destination request (step 104), in the sense that address mapping table 38 has not already been filled with a particular mapping for the particular  
10 source address 14 of client 10, then client 10 specifies the destination network resource it wishes to connect with (step 106), and that mapping is added to address mapping table 38 (step 108) (by, e.g., web application 42, table maintenance module 40, or dynamic table update  
15 module 36). Next, any old (duplicate) mapping existing between that source address 14 and any other destination network resource is deleted (step 110). Finally, server 18 and message routing application 24 are notified that the mapping has been updated (step 112).

20 If the connection request is not a dynamic destination request, or after the dynamic configuration has been completed, then address mapping table is accessed to find an appropriate mapping for source address 14 (step 114). If a mapping exists (e.g., in  
25 address mapping table 38) (step 116), then an instance of message delivery module 34 is forked (step 118), and a communication session between client 10 and destination network resource 28 is initiated (step 120). During the communication session, message delivery module 34  
30 properly routes any incoming messages from client 10 having source address 14 to destination network resource 28 based upon the source addresses of the messages (step 122). Similarly, any messages returned by destination network resource 28 are properly addressed and returned  
35 by message delivery module 34 to client 10 via network 16. At the end of all message exchanges, the communication session is closed (step 124).

If a mapping does not exist (step 116), then a default mapping between the client's source address 14 and a default destination network resource is used (step 126) to address mapping table 38, and thereafter, steps 118 through 124 are executed as above. Steps 118 through 124 also are executed after notifying the server that the mapping has been updated (step 112).

Referring to Figure 6, software 210 for providing a message routing application can be placed upon any machine-readable device 210, such as a floppy disk, CD-ROM, removable hard drive, or other memory device, and can then be loaded into a server 18. Software 200 can include code which, when loaded into a server 18 (and/or a server's HTTP server 19), provides the application software needed to generate an appropriate message routing application 24, including as needed, a web application 42 for performing an initial configuration with a client 10 seeking to establish communications, an address mapping table 38, and table maintenance module 40.

Other embodiments are within the scope of the claims. For example, other methods for requesting a connection between a client and a host can be used, including other authentication applications. Connection requests can be sent to the message routing application in a number of ways, including passing semaphores, piping, or setting a file or a stored flag. Each client or host can be a computer, or any machine having a network address. The message routing application can be configured in a number of different ways to pass messages between client and host based upon the client's source address.

What is claimed is:

1. A method for delivering a message unit to a destination network resource within a transport communications layer comprising the steps of:
  - 5 configuring a mapping to the destination network resource based upon a source address of the message unit; and
  - 10 sending the message unit to the destination network resource based upon the mapping.
2. The method of claim 1 wherein the source address comprises a source IP address of the message unit.
3. The method of claim 1 wherein the source address comprises a source IP address and source port number of the message unit.
4. The method of claim 1 wherein the destination network resource has a network resource address to which the message unit is sent.
5. The method of claim 4 wherein the network resource address comprises a not valid Internet IP address.
6. The method of claim 4 wherein the network resource address comprises a network address on a local area network.
7. The method of claim 1 wherein configuring the mapping comprises writing a table that maps the source address of the message unit and a network resource address for the destination network resource.

8. The method of claim 7 wherein the table maps a host IP address and a host port number for the destination network resource.

5 9. The method of claim 1 further comprising configuring the mapping to send message units to destination network resources based upon source addresses of the message units.

10 10. The method of claim 9 wherein the source addresses comprise source IP addresses for the message units.

15 11. The method of claim 9 wherein the source addresses comprise source IP addresses and source port numbers for the message units.

20 12. The method of claim 9 wherein configuring the mapping comprises recording the source IP address of a latest-received connection request.

25 13. The method of claim 1 wherein the message unit comprises a single message sent during a connection-oriented transport session.

14. The method of claim 13 wherein the connection-oriented transport session comprises a TCP session.

30 15. The method of claim 1 wherein the message unit comprises a datagram sent during a connectionless transport session.

16. The method of claim 15 wherein the connectionless transport session comprises a UDP session.

35 17. A storage device tangibly storing a control program, the control program, when coupled to a control

device, operating the control device to deliver a message unit to a destination network resource within a transport communications layer, the control program being configured to operate the control device to perform the function:

configuring a mapping to the destination network resource based upon a source address of the message unit; and

sending the message unit to the destination network resource based upon the mapping.

18. The storage device of claim 17 wherein the source address comprises a source IP address of the message unit.

19. The storage device of claim 17 wherein the source address comprises the source IP address and source port number of the message unit.

20. The storage device of claim 17 wherein the destination network resource has a network resource address to which the message unit is sent.

21. The storage device of claim 20 wherein the network resource address comprises a not valid Internet IP address.

22. The storage device of claim 20 wherein the network resource address comprises a network address on a local area network.

23. The storage device of claim 17 wherein configuring the mapping comprises writing a table that maps the source address of the message unit and a network resource address for the destination network resource.

24. The storage device of claim 23 wherein the table maps a host IP address and a host port number for the destination network resource.

5        25. The storage device of claim 17 further comprising configuring the mapping to send message units to destination network resources based upon source addresses of the message units.

10       26. The storage device of claim 25 wherein the source addresses comprise source IP addresses for the message units.

15       27. The storage device of claim 25 wherein the source addresses comprise source IP addresses and source port numbers for the message units.

20       28. The storage device of claim 25 wherein configuring the mapping comprises recording the source IP address of a latest-received connection request.

25       29. The storage device of claim 17 wherein the message unit comprises a single message sent during a connection-oriented communication session.

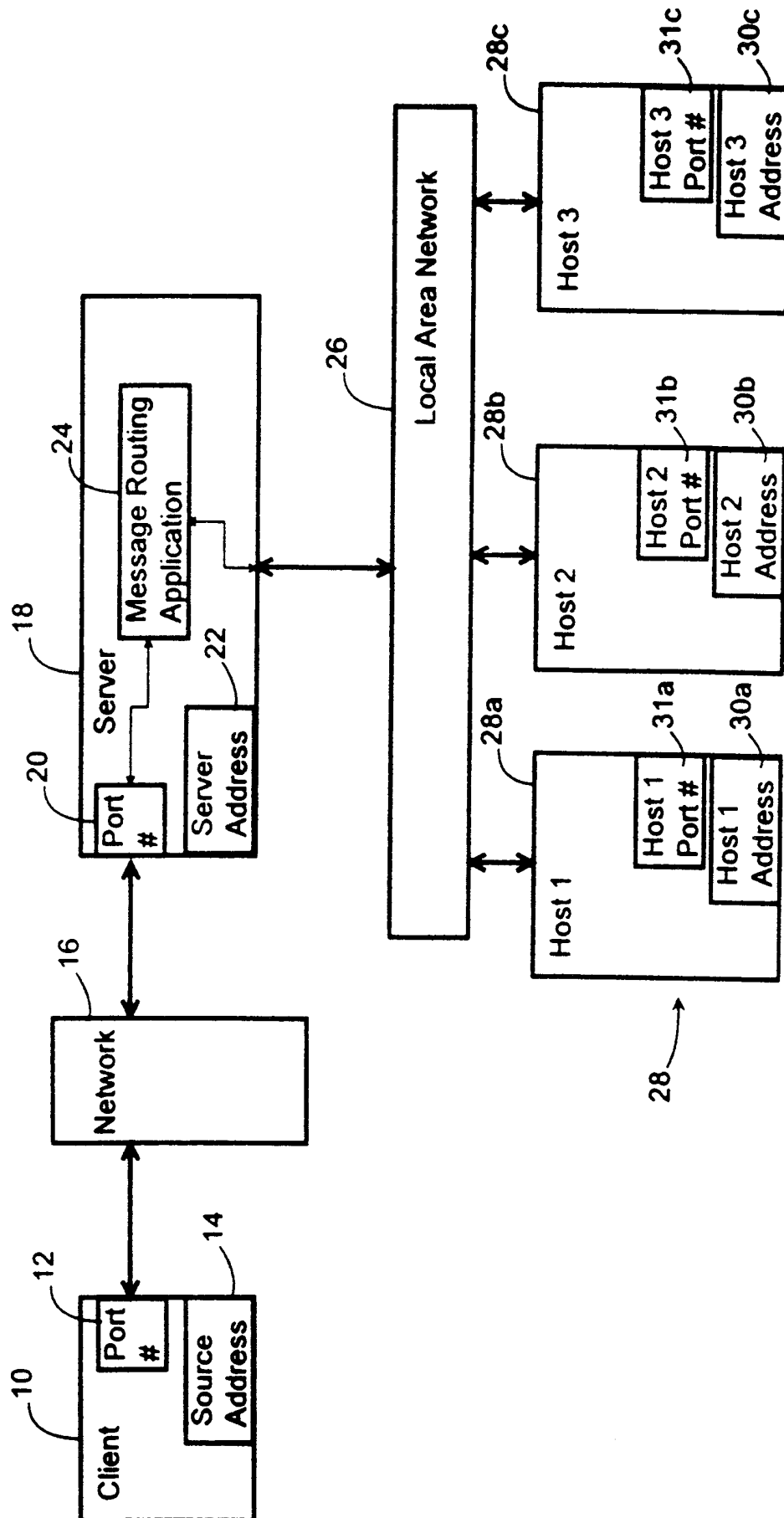
30       30. The storage device of claim 29 wherein the connection-oriented communication session comprises a TCP session.

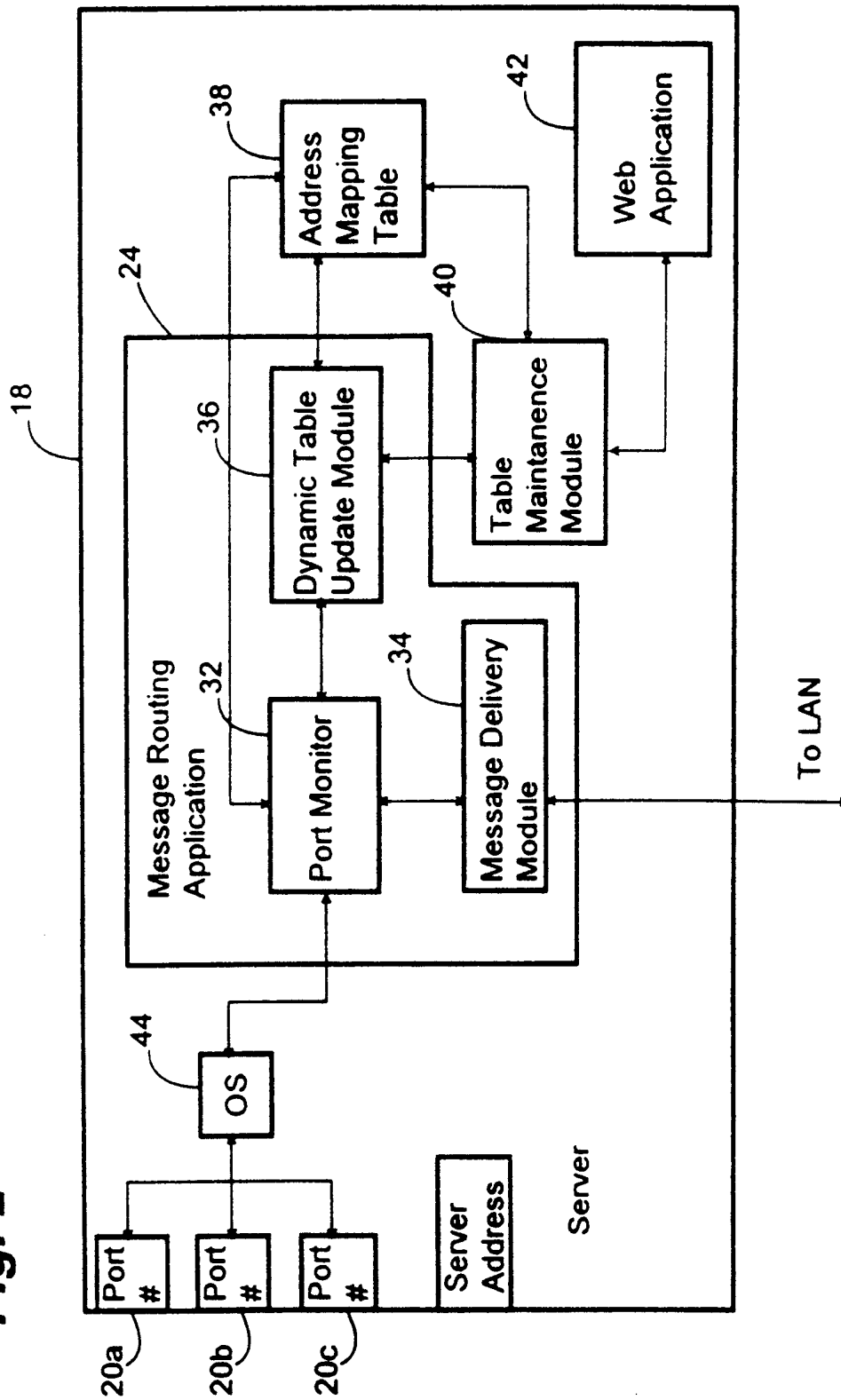
35       31. The storage device of claim 17 wherein the message unit comprises a datagram sent during a connectionless transport session.

35       32. The storage device of claim 31 wherein the connectionless transport session comprises a UDP session.

1/6

**Fig. 1**



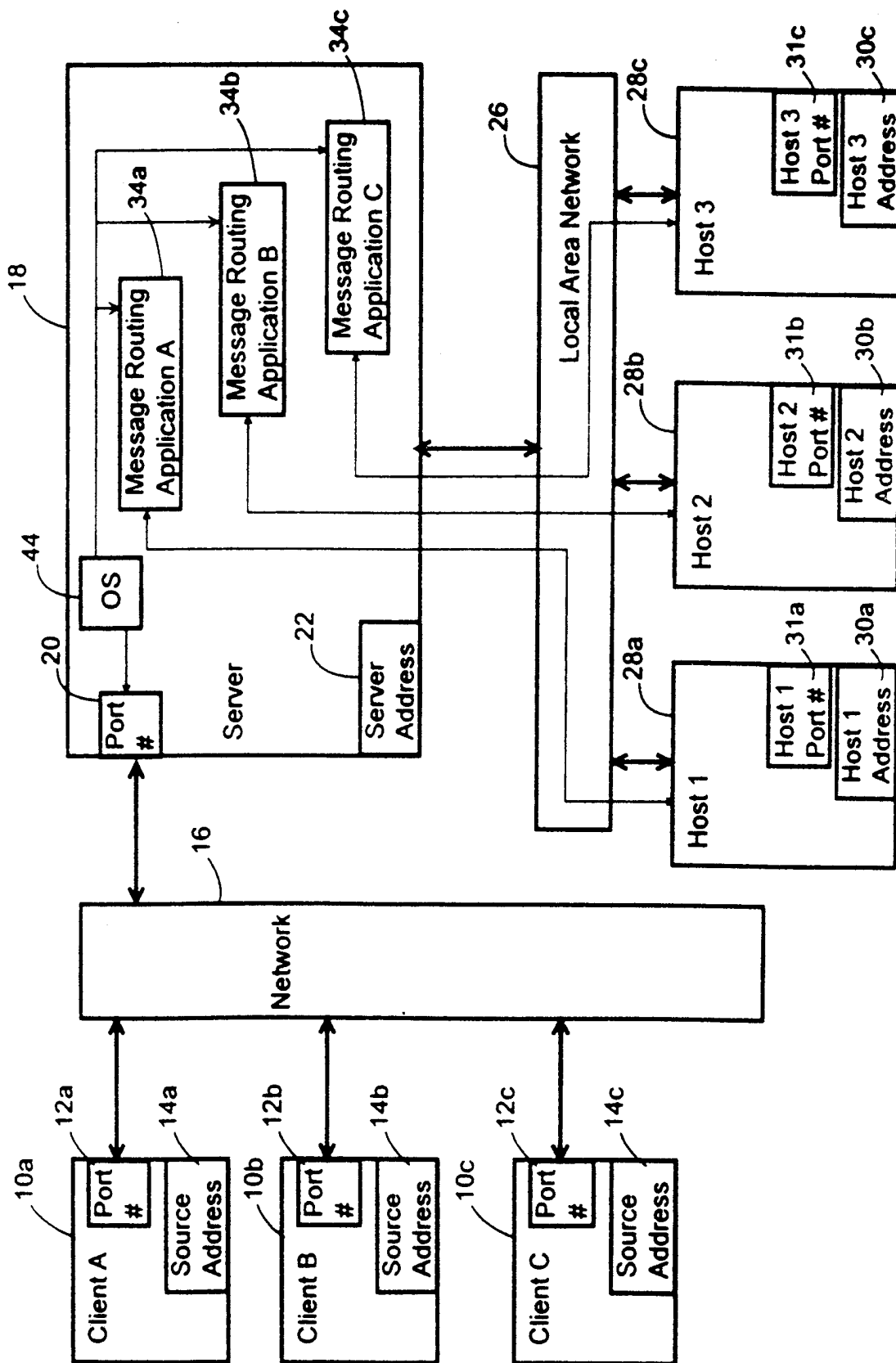
**Fig. 2**

38

Source IP Address (or Source Host Name)	Destination IP Address (or Destination Host Name)	Destination Port # (or Service Name)
Client A (14a)	Host 1 (30a)	Host Port (31a)
Client B (14b)	Host 2 (30b)	Host Port (31b)
Client C (14c)	Host 3 (30c)	Host Port (31c)

Fig. 3

**Fig. 4**



5/6

**Fig. 5**