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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 July 2008 (03.07.2008)

PCT

(10) International Publication Number
WO 2008/079686 A2

(51) International Patent Classification:
H04L 12/26 (2006.01)

(21) International Application Number:
PCT/US2007/087174

(22) International Filing Date:
12 December 2007 (12.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/614,843 21 December 2006 (21.12.2006) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, SJC/10/2/1, San Jose, California 95134-1706 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **WING, Daniel, G.** [US/US]; 222 Coffeeberry Drive, San Jose, CA 95123 (US). **ANDREASEN, Flemming, Stig** [DK/US]; 32 Burlington Drive, Marlboro, New Jersey 07746 (US). **ORAN, David, R.** [US/US]; 7 Ladyslipper Lane, Acton, Massachusetts 01720 (US).

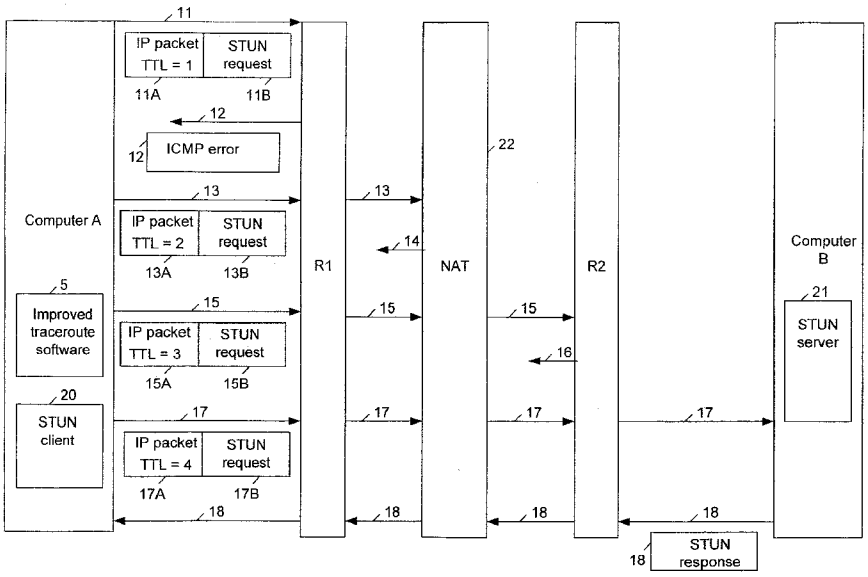
(74) Agents: **LAFFERTY, Wm., Brook** et al.; Scientific-Atlanta, Inc., Intellectual Property Dept., 5030 Sugarloaf Parkway, Lawrenceville, GA 30044 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

(54) **Title:** IMPROVED TRACEROUTE USING ADDRESS REQUEST MESSAGES



(57) **Abstract:** In one embodiment, an endpoint sends messages containing Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) requests to traceroute a path to the remote endpoint. The traceroute may be completed through security devices such as NATs and firewalls. Receipt of a STUN response from the remote endpoint signals that one of the traceroute packets reached the remote endpoint whereas the other traceroute packets have elicited error responses from intermediary, on-path routers, allowing these routers to be identified.

WO 2008/079686 A2

IMPROVED TRACEROUTE USING ADDRESS REQUEST MESSAGES

TECHNICAL FIELD

The present disclosure relates generally to the field of networking.

BACKGROUND

A traceroute is a technique for determining a path used by packets traveling through the network from one endpoint to a remote endpoint. Determination of this path is useful when diagnosing connectivity issues between the two endpoints.

Traceroute involves first sending an Internet Protocol (IP) packet with a Time-To-Live (TTL) value equal to one to a remote host on an unused UDP port. When a first on-path router receives the IP packet and decrements the TTL value to zero, the first on-path router drops the entire message and sends back an Internet Control Message Protocol (ICMP) packet indicating that the IP packet's lifetime has been exceeded. This ICMP error packet contains the IP header and first eight bytes of the payload from the IP packet that exceeded it's lifetime. When the payload is UDP, this information will include the packets source IP-address and port as well as its length. Next, the endpoint sends another IP packet with a TTL value equal to two, which reaches a second on-path router before eliciting the ICMP communication. This process continues until an IP packet has a sufficient TTL value to reach the remote endpoint. When an IP packet reaches the remote endpoint, the receipt of a UDP packet on an unused UDP port elicits an invalid port ICMP error signaling packet from the remote endpoint, which indicates completion of the traceroute.

On-path security devices can interfere with traceroutes by observing the addressing of the packets to the unused UDP port, and blocking those packets from reaching the remote endpoint. When the packets are blocked, the invalid port ICMP error is not elicited and the traceroute does not complete. The disclosure that follows solves these and other problems.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an example computer for sending Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) requests to traceroute a path to a remote endpoint.

FIG. 2 illustrates an example of the computer illustrated in FIG. 1 for conducting both an Real-Time Protocol (RTP) path traceroute and an Real-Time Control Protocol (RTCP) path traceroute.

FIG. 3 illustrates an example of the computer illustrated in FIG. 1 for associating traceroute messages with traceroute responses by observing total length fields.

FIG. 4 illustrates an example method for using the computer illustrated in FIGS. 1-3.

DESCRIPTION OF EXAMPLE EMBODIMENTS

Overview

In one embodiment, an endpoint sends messages containing Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) requests to traceroute a path to the remote endpoint. The traceroute may be completed through security devices such as NATs and firewalls. Receipt of a STUN response from the remote endpoint signals that one of the traceroute packets reached the remote endpoint whereas the

other traceroute packets have elicited error responses from intermediary, on-path routers, allowing these routers to be identified.

Description

Several preferred examples of the present application will now be described with reference to the accompanying drawings. Various other examples of the invention are also possible and practical. This application may be exemplified in many different forms and should not be construed as being limited to the examples set forth herein.

The figures listed above illustrate preferred examples of the application and the operation of such examples. In the figures, the size of the boxes is not intended to represent the size of the various physical components. Where the same element appears in multiple figures, the same reference numeral is used to denote the element in all of the figures where it appears. When two elements operate differently, different reference numerals are used regardless of whether the two elements are the same class of network device.

Only those parts of the various units are shown and described which are necessary to convey an understanding of the examples to those skilled in the art. Those parts and elements not shown are conventional and known in the art.

FIG. 1 illustrates an example computer for sending STUN requests to traceroute a path to a remote endpoint.

Referring to FIG. 1, a call for media exchange between computers A and B is established using Session Initiation Protocol (SIP) or a similar protocol. The SIP signaling message includes a Session Description Protocol (SDP) attachment describing the media streams to be established and for each media stream, it includes instructions to use Interactive Connectivity Establishment (ICE) to establish connectivity.

The computers A and B are generally unaware of the path that the call and its associated media take through the network. In this example, the media path extends through the router R1, through a NAT 22 providing address translation for computer B, and through router R2. To identify the path that the media takes through the network, as well as for diagnostic reasons, computer A traceroutes the media path. The following traceroute process may occur after ICE, or during ICE by leveraging one of the STUN messages sent during ICE.

The improved traceroute software 5 generates a traceroute communication 11 including IP packet 11A containing a STUN request 11B generated by a local STUN client 20. The TTL field in the IP packet 11A is set to one to elicit an ICMP error message 12 from a first on-path router.

The communication 11 is addressed to the same IP address and port number used for sending media to computer B. This is in contrast to other traceroutes that are addressed to an invalid port on a remote endpoint. Addressing the traceroute messages with the port used for the media path (instead of a different, invalid port) advantageously can prevent on-path routers from processing the traceroute messages with a different priority or forwarding them along a different path than the media packets themselves, and also prevent interference from firewalls and NATs. When the traceroute messages are processed using the same priority and destination address as the media flow, the traceroute messages and the media flow packets are given the same treatment by the network. As a result, the traceroute messages will flow on the same path as the media flow, experience the same delays, etc., which produces more accurate diagnostic information.

Router R1 receives the communication 11 and decrements the TTL value by one. Upon observing a TTL equal to zero, router R1 drops the communication 11 and generates an ICMP error 12.

Next, or in parallel with sending communication 11, computer A sends communication 13 including IP packet 13A with TTL equal to two and containing STUN request 13B. This communication 13 is forwarded by router R1 because the TTL value is not decremented to zero. The communication 13 is received by the NAT 13, which decrements the TTL value to zero and sends an ICMP error 14.

Next, or in parallel with sending communications 11 and 13, computer A sends communication 15 including IP packet 15A with TTL equal to three and STUN request 15B. This communication 15 is forwarded by router R1 because the TTL value is not decremented to zero.

Next, the NAT 22 receives the forwarded communication 15. Since the communication 15 is addressed to the same port number as the established media flow, and has a TTL value greater than zero, the NAT forwards the communication 15. This is in contrast to other traceroute techniques that require addressing using an invalid port to elicit an error response from the remote endpoint. Such undeliverable messages are dropped by intermediary NATs when address translation identifies an invalid port. Although there are no intermediary firewalls in this example, the communication 15 is able to pass through a firewall or other security device for similar reasons that the communication 15 is forwarded by NAT 22. Router R2 receives the communication 15, decrements the TTL value to zero and generates an ICMP error message 16.

Next, or in parallel with sending communications 11, 13 and 15, computer A sends communication 17 including IP packet 17A with TTL equal to four and STUN request 17B.

Communication 17 reaches router R2 just as communication 15 did. Since router R2 does not decrement the TTL to zero, the communication 17 also reaches computer B.

When the communication 17 is received at the computer B, in contrast to other traceroute methods, no error message is generated. Instead, the STUN request 11B is received at STUN server 21, which generates a STUN response 18 addressed to computer A. The STUN server 21 includes an address and UDP port observed by the STUN server 21 in the STUN request 17B, which includes either an address for computer A or an address of an intermediary on-path network address translating device (which in turn will forward the message to computer A after performing the necessary network address and port translation).

The STUN response 18 is able to pass through on-path security devices in a similar fashion as communications 15 and 17. Accordingly, computer A receives the STUN response 18 and observes that the traceroute is complete. For example, since the communication 17 having TTL equal to four elicited the STUN response 18, both routers R1 and R2 and the NAT 22 on the media path have been identified because of the earlier STUN traceroute messages with TTL values equal to one, two, and three.

The information gained from the completed traceroute is a valuable diagnostic tool for computer A. In one example, computer A can pinpoint a portion of a path that causes an overall communication delay by comparing timing information associated with the received responses. For example, when computer A receives a first response from a first router in ten milliseconds and a second response from a second router in two hundred milliseconds, computer A can pinpoint an overall delay to the portion of the network that couples the first and second routers. Computer A can make numerous other conclusions using information from the completed traceroute, e.g. determining where connectivity problems occur, as would be recognized by one of ordinary skill in the art.

FIG. 2 illustrates an example of the computer illustrated in FIG. 1 for conducting both an RTP path traceroute and an RTCP path traceroute.

Computer A may conduct different traceroutes to determine whether an RTP path uses the same or a different path through the network than an RTCP path. The RTP protocol is used to transfer audio and video data between to endpoints, while the RTCP protocol is used to send out of band control information associated with an RTP flow. Since the RTP flow and the RTCP flows carry different types of information, they are addressed to different ports, and typically have different Differentiated Services CodePoint (DSCP) values, these flows can have different priorities and may take different paths through the network. When the RTP path and the RTCP path flow through different routers, computer A can traceroute each of the different flow paths to diagnose issues with either of the paths. Tracerouting the separate paths is not possible using conventional traceroute techniques.

To traceroute the RTP path, computer A sends several communications to computer B using IP address X and RTP port Y. For brevity, only the communication 31 that has a TTL sufficient to reach the computer B is illustrated. It is understood from the previous example, that computer A sends other communications with lower TTL values in parallel with communication 31 or before sending communication 31.

Communication 31 includes IP and UDP headers 31A having a TTL equal to four and containing a STUN request 31B. The IP and UDP headers 31A indicate RTP port Y on IP address X as a destination address. Due to the use of a valid port, intervening security devices allow the communication 31 to pass. Also, due to the similar addressing the communication 31 follows the path of the RTP flow, which in this example passes through routers R1 and R2. The communication 31 may also include a priority indicator such as a Differential Services Code Point (DSCP) value equal to a DSCP value for the RTP flow,

which indicates that communication 31 is the same priority as the RTP flow. The use of the DSCP value in communication 31 equal to the DSCP value of the media flow furthermore helps ensure the path taken by the STUN traceroute packet is the same as that of the RTP flow. Computer B receives the communication 31 and responds with a STUN response 32 in a similar manner as explained with reference to FIG. 1.

Still referring to FIG. 2, in this example the RTCP flow takes a different path and flows through routers R3, R4 and R5. To traceroute the RTCP flow, computer A sends communication 33 including IP and UDP headers 33A and a STUN request 33B. It is understood from the previous example, that computer A sends other communications (not shown) with lower TTL values in parallel with communication 33 or before sending communication 33. The IP and UDP headers 33A include a TTL value equal to five, which allows the communication 33 to be forwarded by each of the intermediary routers R3, R4 and R5 located on the RTCP path. The IP and UDP headers 33A include a destination address of RTCP port Z on IP address X, which is the same addressing used for an RTCP flow between the computers A and B. The communication 33 may also include a DSCP value of the RTCP flow, which may be different than the DSCP value included in communication 31. Computer B receives the communication 33 and responds with a STUN response 34 in a similar manner as explained with reference to FIG. 1.

FIG. 3 illustrates an example of the computer illustrated in FIG. 1 for associating traceroute messages with traceroute responses by observing total length fields.

In the previous examples, computer A optionally sent the different traceroute communications having different TTLs in parallel, which means that a second message is sent before a response to the first message has been received. Sending more than one traceroute communication in parallel is advantageous, because doing so reduces the total time

required to complete the traceroute as compared to a sequential process. The software 5 includes a technique for correlating a received ICMP error or STUN response with a sent traceroute communication independently of an order of arrival of the responses. As will be explained, this technique leverages the fact that routers are configured to send ICMP errors that include the IP header and first eight bytes of the IP payload from the original packet. In the case of a STUN request, the IP payload is a UDP packet (containing the STUN request), and the first eight bytes will be the UDP header, which includes the source and destination port number.

The computer A generates a traceroute communication 41 that includes an IP header 41A having a TTL of one, a UDP header 41B and a STUN request 41C. The computer A includes padding data 41D inside the STUN request 41C. In the present example, the padding data 41D includes one or more STUN attributes each being four bytes in size. The padding data 41D affects a total UDP length field included in the UDP header 41B, such that the UDP header 41B indicates a total UDP packet length of Q (the IP header includes a total IP packet length field as well which can be used as an alternative, e.g. if the RTP/RTCP flow is sent over IPsec). In other examples, the padding data 41D may be added to any other practical portion of the communication 41 to manipulate total length.

Router R3 receives the communication 41 and decrements the TTL by one. Upon observing a TTL value equal to zero, the router R3 generates an ICMP error 42. Inside the ICMP payload 42A, the router R3 includes the IP header 41A and the first eight bytes of the IP payload (UDP header 41B or a portion thereof) of the communication 41, which indicates the total length of received packet 41 as well as the source and destination address and port. Next, the router R3 sends the ICMP error 42 back to computer A.

Computer A receives the ICMP error 42 and observes the payload 42A having the portion of the UDP header 41B showing a total length value of Q (alternatively, computer A could examine the length value of the IP header included in the payload in the ICMP response). The computer A then correlates the communication 41 having the UDP header 41B having the source and destination address (from 41A) and port (from 41B) and having a total length field of Q with the response 42 having a payload also showing a total length value of Q. Accordingly, the computer A observes that communications 41 and 42 are associated due to the matching total length field values.

In parallel with sending communication 41, computer A also sends communication 43. The communication 43 includes an IP header 43A having a TTL equal to two, a UDP header 43B and a STUN request 43C. The STUN request 43C may be the same as STUN request 41C, except that a different amount of padding data 43D is included. The padding data 43D may be two STUN attributes, which is equal to eight bytes. The different amount of padding data 43D causes the UDP header 43B to indicate a different total length R for the communication 43.

After router R3 forwards the communication 43, the router R4 receives the communication 43 and decrements the TTL by one. Upon observing a TTL value equal to zero, the router R4 generates an ICMP error 44. Inside the ICMP payload 44A, the router R4 includes the IP header 43A and first eight bytes of the IP payload (at least a portion of UDP header 43B) of the communication 43, which indicates the total length of received packet 43. Next, the router R4 sends the ICMP error 44 back to computer A.

Computer A receives the ICMP error 44 and observes the payload 44A having a portion of the UDP header 43B showing a total length value of R (computer A may examine the source and destination address and port in the ICMP payload as well). The computer A

then correlates the communication 43 having the UDP header 43B with the total length field of R with the response 44 also having the payload 44A containing a total length value of R. Accordingly, regardless of the order that responses 42 and 44 arrive, computer A is able to correlate traceroute communications and responses.

Using the total length field to associate traceroute communications with responses can also be used to distinguish responses for an RTP path traceroute from responses for an RTCP path traceroute independently of the arrival order of responses when the RTP and RTCP streams are multiplexed on a single port. Otherwise, differing port numbers may be used to distinguish responses for an RTP path from responses for an RTCP path.

FIG. 4 illustrates an example method for using the computer illustrated in FIGS. 1-3.

In block 401, the computer A generates traceroute communications with varying lifetime values for sending sequentially or in parallel to traceroute a path to a remote endpoint. The computer A determines whether the traceroute communications are to be sent in parallel in block 402. Such a determination may be made by accessing local configuration settings. When the communications are to be sent in parallel, in block 403 the computer A includes different amounts of padding data inside each of the traceroute communications to manipulate values of packet length fields in attached headers.

In block 404, the computer A addresses the traceroute communications to one or more valid, deliverable ports on the remote endpoint. In block 405, the computer A sends the addressed traceroute communications to the remote endpoint.

The computer A receives back one or more error responses and one or more non-error STUN responses in block 406. When the communications were not sent sequentially, in block 407 the computer A observes total length values included in payloads of the responses. Although correlation by, for example using total length, is optional when using a serial

transfer of the traceroute, correlation is still preferred even in the serial transfer case. In block 408, the computer then correlates responses to traceroute communications by comparing the observed total length values from the payloads to the total length values included in the headers of the traceroute communications. In block 409, the computer A identifies information including network topology and network delays using the responses.

The above examples describe a computer generating traceroutes. In other examples, other endpoints such as a personal computer, an IP phone, a Personal Digital Assistant (PDA), a cell phone, a smart phone, a Publicly Switched Telephone Network (PSTN) gateway, etc., may generate traceroutes using the methods described above.

Several preferred examples have been described above with reference to the accompanying drawings. Various other examples of the invention are also possible and practical. The system may be exemplified in many different forms and should not be construed as being limited to the examples set forth above.

The figures listed above illustrate preferred examples of the application and the operation of such examples. In the figures, the size of the boxes is not intended to represent the size of the various physical components. Where the same element appears in multiple figures, the same reference numeral is used to denote the element in all of the figures where it appears.

Only those parts of the various units are shown and described which are necessary to convey an understanding of the examples to those skilled in the art. Those parts and elements not shown are conventional and known in the art.

The system described above can use dedicated processor systems, micro controllers, programmable logic devices, or microprocessors that perform some or all of the operations.

Some of the operations described above may be implemented in software and other operations may be implemented in hardware.

For the sake of convenience, the operations are described as various interconnected functional blocks or distinct software modules. This is not necessary, however, and there may be cases where these functional blocks or modules are equivalently aggregated into a single logic device, program or operation with unclear boundaries. In any event, the functional blocks and software modules or features of the flexible interface can be implemented by themselves, or in combination with other operations in either hardware or software.

Having described and illustrated the principles of the invention in a preferred embodiment thereof, it should be apparent that the invention may be modified in arrangement and detail without departing from such principles. I claim all modifications and variation coming within the spirit and scope of the following claims.

CLAIMS

1. An apparatus, comprising:

one or more processors; and

a memory coupled to the one or more processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

send a plurality of messages to a remote endpoint, each of the messages including a different lifetime value;

receive back a plurality of error responses identifying the presence of one or more routers located between an originating endpoint of the messages and the remote endpoint; and

receive back a non-error response message indicating completion of a traceroute to the remote endpoint.

2. The apparatus of claim 1 wherein the messages include address requests and the non-error response message includes an address of an intermediary network address translation device that is located remotely with respect to both endpoints.

3. The apparatus of claim 1 wherein at least one of the messages is configured to elicit the non-error response message from a Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) server located on the remote endpoint.

4. The apparatus of claim 1 wherein the processors are further operable to insert padding data into the messages for length manipulation.

5. The apparatus of claim 4 wherein all of the messages include different amounts of padding data.

6. The apparatus of claim 1 wherein the processors are further operable to:

send audio or video data to a Real Time Protocol (RTP) port on the remote endpoint;

wherein the plurality of messages are addressed to the same RTP port on the remote endpoint.

7. A method comprising:

establishing a session with a remote endpoint, the session associated with a first network path for transferring media to the remote endpoint and a second network path that is separate from the first network path, the second network path for transferring out of band control information associated with the media to the remote endpoint;

sending first traceroute communications over the first network path;

sending second traceroute communications over the second network path; and

receiving back error responses and non-error responses, the non-error responses corresponding to the first and second traceroute communications and generated by the remote endpoint.

8. The method of claim 7 wherein the first traceroute communications are addressed to a different valid port on the remote endpoint than the second traceroute communications.

9. The method of claim 7 wherein the traceroute communications include address request messages.

10. The method of claim 9 wherein at least one of the received non-error responses includes a payload identifying an Internet Protocol (IP) address for an intermediary on-path security device that provides network address translation.

11. The method of claim 7 further comprising including different amounts of padding data in the first and second traceroute communications.

12. The method of claim 11 wherein the padding data is one or more Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) attributes for increasing packet length.

13. The method of claim 7 wherein the first traceroute communications are addressed to an IP address and port that corresponds to a same IP address and port used for sending media.

14. An apparatus, comprising:

means for sending a plurality of address request messages having different lifetime values to a valid port on a remote endpoint;

means for receiving back one or more lifetime exceeded error messages, each of the lifetime exceeded messages indicating the presence of a router located between the remote endpoint and a local endpoint; and

means for receiving back a response message identifying traceroute completion.

15. The apparatus of claim 14 wherein the address request messages include Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) requests.

16. The apparatus of claim 14 further comprising means for inserting padding data into the address request messages to manipulate lengths of the address request messages.

17. The apparatus of claim 16 wherein the padding data is inserted into STUN payloads of the address request messages.

18. The apparatus of claim 14 further comprising:

means for sending audio or video data to a port on the remote endpoint; and

means for addressing the address request messages to the same port on the remote endpoint.

19. The apparatus of claim 14 further comprising:

means for tracerouting a Real-Time Protocol (RTP) path to the remote endpoint; and

means for tracerouting a Real-Time Control Protocol (RTCP) path to the remote endpoint;

wherein the RTP path and the RTCP path extend through different groups of routers.

20. The apparatus of claim 14 further comprising means for correlating each received lifetime exceeded error message to one of the address request messages by observing length fields included in the received lifetime exceeded error message.

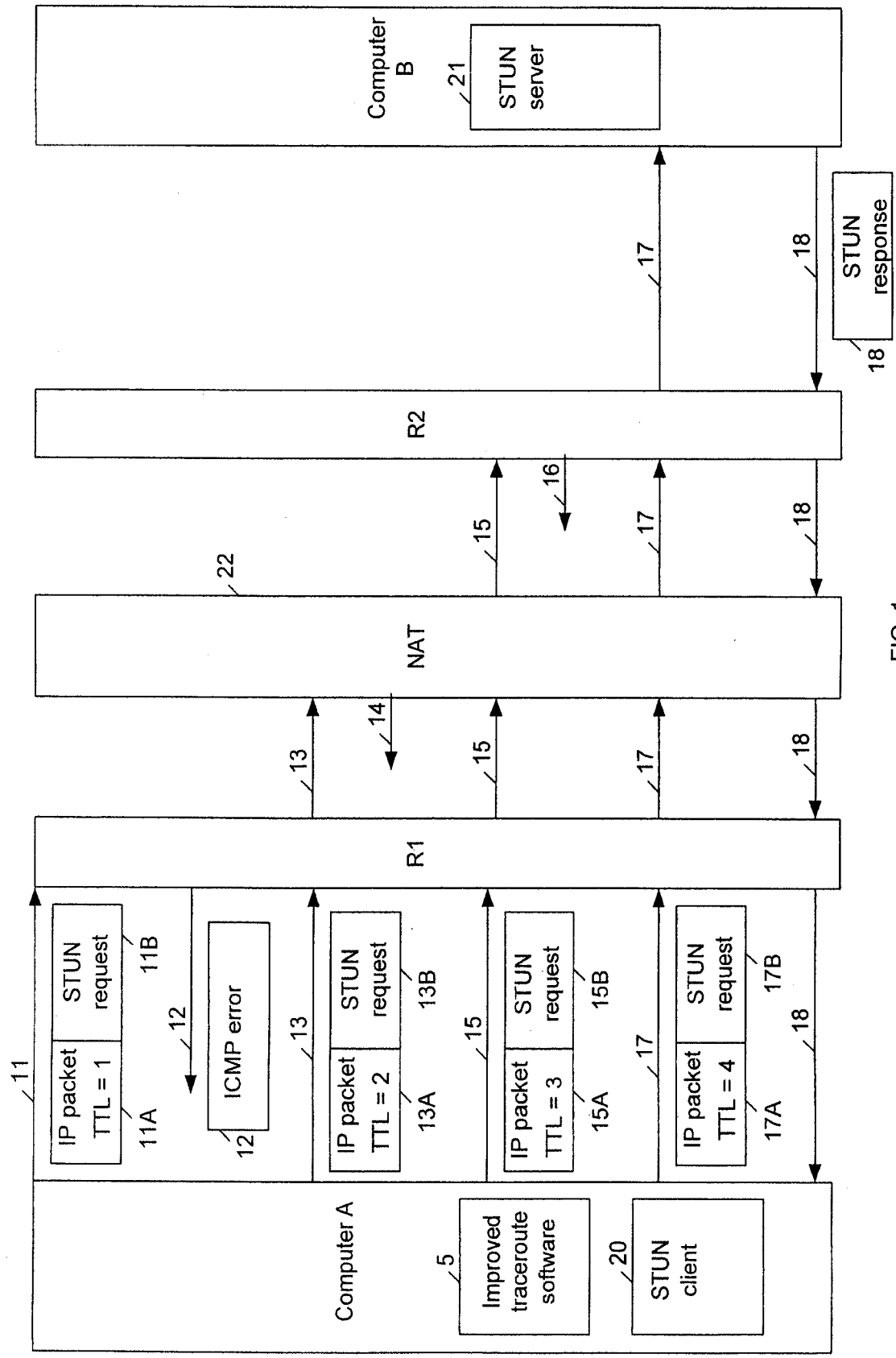

Computer B
21
STUN server
17
18
STUN response
18
R2
16
15
17
18
22
NAT
14
13
15
17
18
R1
11
IP packet TTL = 1
STUN request
11A
11B
12
ICMP error
12
13
IP packet TTL = 2
STUN request
13A
13B
15
IP packet TTL = 3
STUN request
15A
15B
17
IP packet TTL = 4
STUN request
17A
17B
18
Computer A
5
Improved traceroute software
20
STUN client

FIG. 1

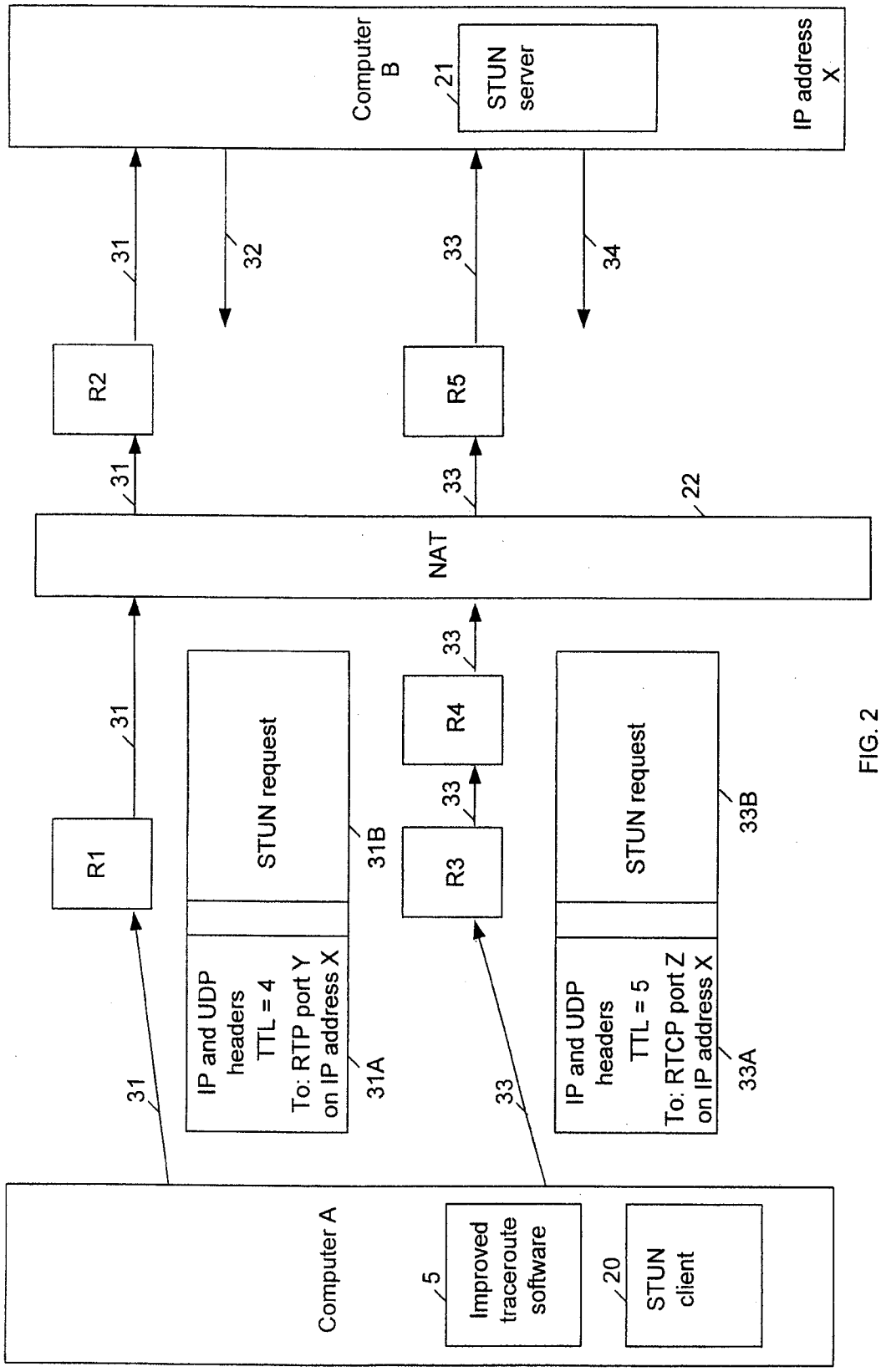

Computer A
5
Improved traceroute software
20
STUN client
IP and UDP headers
TTL = 4
To: RTP port Y
on IP address X
31A
STUN request
31B
IP and UDP headers
TTL = 5
To: RTCP port Z
on IP address X
33A
STUN request
33B
R1
R2
R3
R4
R5
NAT
22
31
32
33
34
Computer B
21
STUN server
IP address X

FIG. 2

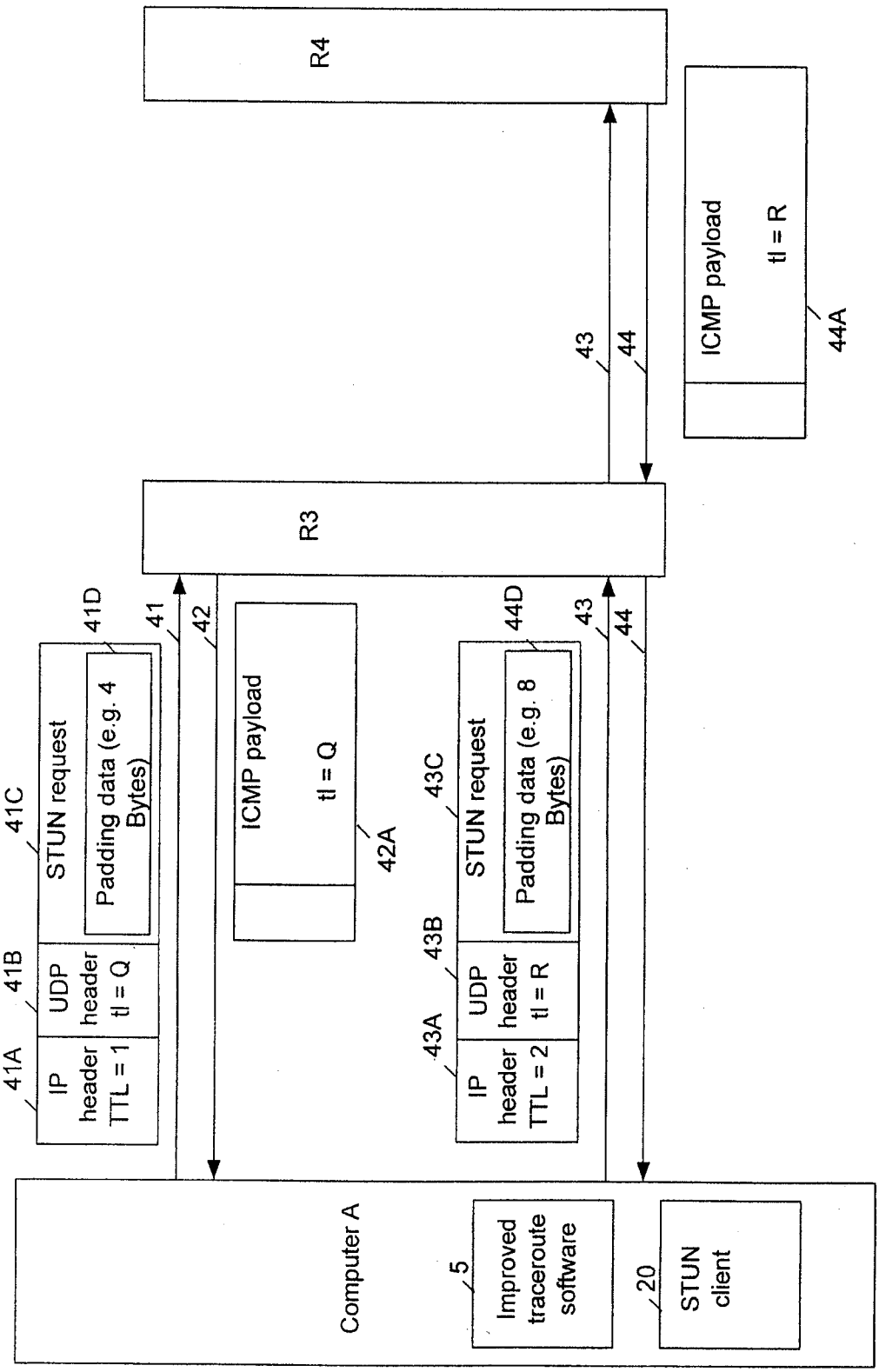

R4
ICMP payload
tl = R
44A
43
44
R3
41
42
41D
Padding data (e.g. 4 Bytes)
41C
STUN request
41B
UDP header tl = Q
41A
IP header TTL = 1
ICMP payload
tl = Q
42A
44D
Padding data (e.g. 8 Bytes)
43C
STUN request
43B
UDP header tl = R
43A
IP header TTL = 2
Computer A
5
Improved traceroute software
20
STUN client

FIG. 3

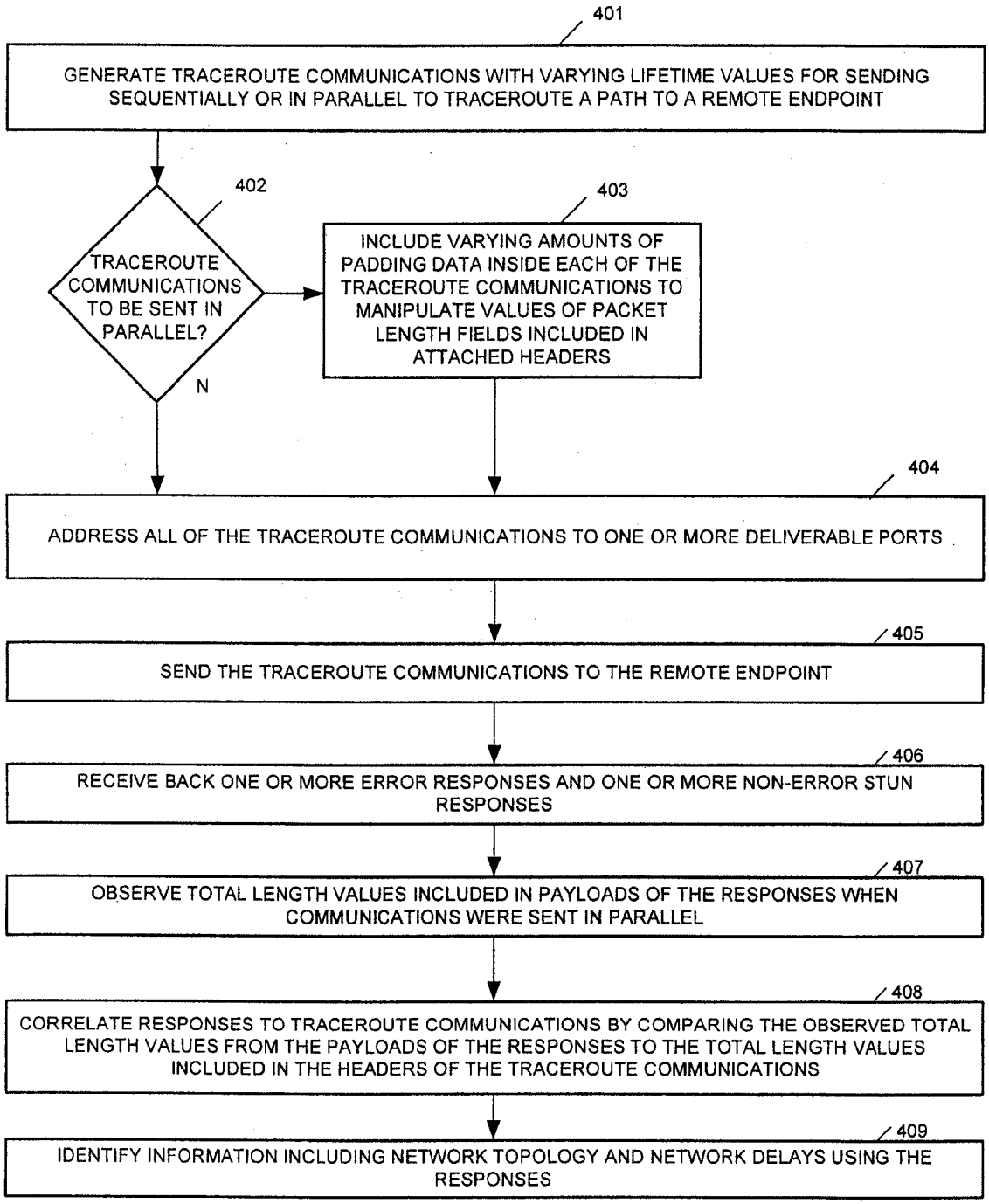

401
GENERATE TRACEROUTE COMMUNICATIONS WITH VARYING LIFETIME VALUES FOR SENDING SEQUENTIALLY OR IN PARALLEL TO TRACEROUTE A PATH TO A REMOTE ENDPOINT
402
TRACEROUTE COMMUNICATIONS TO BE SENT IN PARALLEL?
N
403
INCLUDE VARYING AMOUNTS OF PADDING DATA INSIDE EACH OF THE TRACEROUTE COMMUNICATIONS TO MANIPULATE VALUES OF PACKET LENGTH FIELDS INCLUDED IN ATTACHED HEADERS
404
ADDRESS ALL OF THE TRACEROUTE COMMUNICATIONS TO ONE OR MORE DELIVERABLE PORTS
405
SEND THE TRACEROUTE COMMUNICATIONS TO THE REMOTE ENDPOINT
406
RECEIVE BACK ONE OR MORE ERROR RESPONSES AND ONE OR MORE NON-ERROR STUN RESPONSES
407
OBSERVE TOTAL LENGTH VALUES INCLUDED IN PAYLOADS OF THE RESPONSES WHEN COMMUNICATIONS WERE SENT IN PARALLEL
408
CORRELATE RESPONSES TO TRACEROUTE COMMUNICATIONS BY COMPARING THE OBSERVED TOTAL LENGTH VALUES FROM THE PAYLOADS OF THE RESPONSES TO THE TOTAL LENGTH VALUES INCLUDED IN THE HEADERS OF THE TRACEROUTE COMMUNICATIONS
409
IDENTIFY INFORMATION INCLUDING NETWORK TOPOLOGY AND NETWORK DELAYS USING THE RESPONSES

FIG. 4