



- (51) **International Patent Classification:**
H04L 29/12 (2006.01)
- (21) **International Application Number:**
PCT/IB20 12/002922
- (22) **International Filing Date:**
14 December 2012 (14.12.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
CN201 1/084542 23 December 2011 (23.12.2011) CN
- (71) **Applicant:** FRANCE TELECOM [FR/FR]; 78, rue Olivier de Serres, F-75015 Paris (FR).
- (72) **Inventors:** DENG, Xiaohong; 10/f, South Tower Raycom Info Park C, 2 Sience Institute South Rd, Haidian District, Beijing 100190 (CN). WANG, Lan; 10/f, South Tower Raycom Info Park C, 2 Science Institute South Rd., Haidian District, Beijing 100190 (CN). GU, Daqing; Raycom Tower C, No 2, Kexueyuan South Road, Haidian District, Beijing 100080 (CN).
- (74) **Agent:** FRANCE TELECOM/OLNC/OLPS/IPL; CODA, Sandrine, 38-40, rue du General Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) **Title:** METHOD, GATEWAY AND SYSTEM FOR MANAGING ALG FUNCTIONALITY

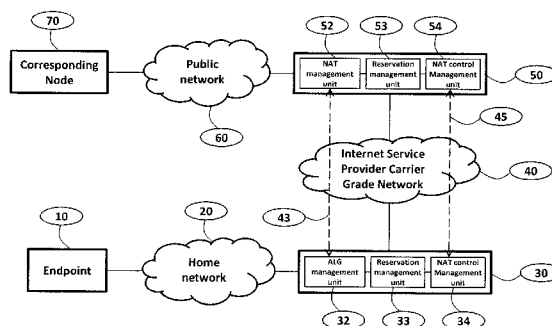


Figure 1

(57) **Abstract:** A system for managing an Application Layer Gateway functionality comprising a telecommunication network comprising at least one endpoint (10), a Customer Premises Equipment gateway (30) and a Network Address Translation Carrier Grade Network device (50), said at least one endpoint (10) being configured for communicating packets with said Network Address Translation Carrier Grade Network device (50) through said Customer Premises Equipment gateway (30), the Network Address Translation Carrier Grade Network device (50) being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint (10), the Customer Premises Equipment gateway (30).

Method, gateway and system for managing ALG functionality

Field of the Invention

5 The present invention relates in general to telecommunications and more specifically to telecommunication networks.

Background of the Invention

10 A known telecommunication network comprises at least an endpoint or host, a host network, an Internet Service Provider Carrier Grade Network (ISP CGN), and a public network, such as e.g. the internet, the Internet Service Provider Carrier Grade Network being interconnected, on one side, to the host network and, on another side, to the public network, for exchanging packets of data using different addresses, ports and protocols. The host network allows the endpoint(s) to connect to the public network through the Internet Service Provider Carrier Grade Network. The host network may be a private network, such as e.g. a home network. The endpoint may be a terminal operated by a customer of the Internet Service Provider.

15 Such a telecommunication network comprises a device configured for performing Network Address Translation (NAT) called NAT device. NAT is performed in a variety of situations in a telecommunication network. Often NAT involves translating addresses from public addresses to private addresses, and vice versa. More particularly, address translation may involve source address translation and/or destination address translation. NAT that involves port mapping may be referred to as network address port translation (NAPT). Thus, NAT may involve address translation, as well as port mapping.

20 Generally, NAT functionality is typically performed on the header of a packet by a gateway called Customer Premises Equipment (CPE) gateway as it is located between the host network and the Internet Service Provider Carrier Grade Network, in the customer's premises, such as e.g. a Digital Subscriber Line router, or by a device located between the Internet Service Provider Carrier Grade Network and the public network and called NAT CGN device.

25 However, some higher-layer protocols, such as File Transfer Protocol (FTP) and Session Initiation Protocol (SIP), provide addresses and/or port numbers inside the body (i.e. payload) of the packet. Consequently, the translation of the IP address(es) and/ or port number(s) by the NAT device makes the information in the body of the packet invalid.

In this case, an Application Layer Gateway (ALG) software module running on a NAT CGN device may be used to update any payload data made invalid by address translation.

However, a drawback exists when an endpoint of the host network uses a specific protocol, such as e.g. Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) or Interactive Connectivity Establishment (ICE), which requires the endpoint to perform its own ALG functionality on the body of packets it transmits. Since the telecommunication network may include endpoints and devices supporting various protocols or versions of such protocols, the result of the application of ALG functionality to packets transmitted by such endpoints or devices is unpredictable.

A solution, described in US2010/0172359, implies that a NAT CGN device should perform ALG functionality on the body of a packet it received from an endpoint only if the endpoint has not performed ALG functionality on the body of the packet prior to sending it to the NAT CGN device. To that end, the NAT CGN device analyses the body of each packet received from the endpoint in order to decide whether it should performed or not ALG functionality.

There is a plurality of drawbacks to such a solution. First of all, a new application based on an application-layer protocol, like e.g. SIP or FTP, can only be developed and used on an endpoint if knowing the specific protocol, the specifications of which being often complex and lengthy. For example, the ICE specifications RFC5245 have more than a hundred pages. Moreover, this solution does not address the ALG issues for the widely deployed and used applications such as e.g. FTP-based and some SIP-based applications when the NAT functionality is performed by a NAT CGN device and not by a CPE gateway device. Furthermore, when the NAT functionality is performed by a NAT CGN device, a drawback is that such a centralized operation of the associated ALG functionality consumes huge resources of the NAT CGN device and may dramatically slow down or block the NAT CGN device and, consequently, the telecommunication network operation. Consecutively, implementing the method described in US2010/0172359 on a NAT CGN device would therefore consume even more resources of the NAT CGN device.

Today there is no solution to efficiently perform ALG functionality when NAT functionality is performed by a NAT CGN device that allows improving efficiency of such a telecommunication network.

Today there is a need for an ALG functionality solution that can be easily implemented on the existing communication infrastructures.

Summary of Invention

It is an object of the present system to overcome disadvantages and/or make improvement over the prior art.

5 To that extend, the invention concerns a method of managing an Application Layer Gateway functionality in a telecommunication network comprising at least one endpoint, a Customer Premises Equipment gateway and a Network Address Translation Carrier Grade Network device, said at least one endpoint being configured for communicating packets with said Network Address Translation Carrier Grade
10 Network device through said Customer Premises Equipment gateway, the Network Address Translation Carrier Grade Network device being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint, said method comprising, for the Customer Premises Equipment gateway, the act of performing an Application Layer Gateway functionality on a
15 communicated packet.

The communicated packet may be received from an endpoint or from the Network Address Translation Carrier Grade Network (NAT CGN) device. Therefore, the Customer Premises Equipment gateway may perform the Application Layer Gateway (ALG) functionality on a packet received from an endpoint then sends it to
20 the NAT CGN device, or on a packet received from the NAT CGN device then sends it to an endpoint.

In an embodiment according to the invention, an ALG functionality is performed by the Customer Premises Equipment gateway whereas a NAT functionality is performed by the NAT CGN device. ALG and NAT functionalities are therefore split between two
25 distinct devices in the telecommunication network, which allows offloading the NAT CGN device of the ALG functionality. This is particularly advantageous in telecommunication networks wherein the NAT functionality needs to be performed centrally on a NAT CGN device as it may be the case, for example, in a Dual-Stack Lite (DS Lite)-based telecommunication network. Dual-Stack Lite is a network architecture solution for
30 addressing Internet Protocol v4 (IPv4) address shortage while migrating to Internet Protocol v6 (IPv6)-based networks, wherein IPv4 is the current Internet Protocol used in most networks and IPv6 is an evolution replacing IPv4 nowadays. Indeed, telecommunication network evolution for migrating from IPv4 to IPv6 may involve using solutions like e.g. DS Lite, NAT444, NAT64 or AplusP. For example, DS Lite implies
35 moving the NAT functionality from the Customer Premises Equipment gateway, located between the host network and the Internet Service Provider Carrier Grade Network, onto

a NATCGN device, located between the Internet Service Provider Carrier Grade Network and the public network. By offloading a NATCGN device of the ALG functionality, fewer resources of the NATCGN device are utilized. This means that more processing ability and memory are left for the NATCGN device for performing NAT functionality, and packet routing and forwarding, thereby increasing packet Input/Output efficiency. Furthermore, performing ALG functionality on the Customer Premises Equipment gateway allows the operator of the Internet Service Provider Carrier Grade Network to manage and upgrade said ALG functionality easily, for example, through CPE device software upgrading, whereas managing and updating ALG functionality in a NATCGN device is complex and put the whole network at risk.

By performing ALG functionality on a packet, it is meant applying the ALG functionality on the body, i.e. payload of the packet, or, in other words, updating any payload data of the packet made invalid by address translation. By performing Network Address Translation functionality on a packet, it is meant performing Network Address Translation on the header of the packet.

In an embodiment according to the invention, the method further comprises an act of managing an application control session of the communicated packet.

In an embodiment according to the invention, the method further comprises an act of managing NAT pinholes reservation.

In an embodiment according to the invention, the method further comprises an act of managing Network Address Translation control, like e.g. managing a Network Address Translation control session and exchanging Network Address Translation control messages.

In an embodiment according to the invention, the method further comprises, prior to performing the Application Layer Gateway functionality, an act of analyzing a communicated packet received from an endpoint.

In an embodiment according to the invention, the method further comprises, subsequently to analyzing a communicated packet received from an endpoint and prior to performing the Application Layer Gateway functionality, an act of sending, to the Network Address Translation Carrier Grade Network device, a request for a Network Address Translation pinhole. In this case, the method may further comprise, subsequently to sending the request and prior to performing the Application Layer Gateway functionality, an act of receiving, from the Network Address Translation Carrier Grade Network device, an allocated Network Address Translation pinhole. A NAT pinhole allows opening a port for a particular application either permanently, e.g. for a webcam session, or temporarily, e.g. while playing a game.

In an embodiment according to the invention, the method further comprises, subsequently to performing the Application Layer Gateway functionality, an act of transmitting the communicated packet received from the endpoint to the Network Address Translation Carrier Grade Network device using the Network Address Translation pinhole.

In an embodiment according to the invention, the method further comprises, subsequently to transmitting, an act of receiving a packet on which a Network Address Translation functionality has been previously performed by the Network Address Translation Carrier Grade Network device and an act of routing said received packet to the corresponding endpoint.

In an embodiment according to the invention, the method according further comprises, subsequently to receiving, from the Network Address Translation Carrier Grade Network device, an allocated Network Address Translation pinhole and prior to performing an Application Layer Gateway functionality, an act of performing a Network Address Translation mapping on the packet received from the endpoint. In this embodiment, the method may comprise, subsequently to performing a Network Address Translation mapping and prior to transmitting the communicated packet received from the endpoint to the Network Address Translation Carrier Grade Network device using the Network Address Translation pinhole, an act of performing a Network Address Translation functionality. Still in this embodiment, the method may further comprise an act of receiving a packet on which a Network Address Translation functionality has not yet been performed, an act of performing a Network Address Translation functionality on the received packet and an act of routing said received packet to the corresponding endpoint.

In an embodiment according to the invention, the method according to the invention is performed using a Port Control Protocol (PCP) between the Customer Premises Equipment gateway and the Network Address Translation Carrier Grade Network device. Such a protocol is simple and easy to implement and easy to use, especially for directly controlling a NAT pinhole, in comparison to STUN or ICE that were designed for NAT discovery.

The invention also concerns a Customer Premises Equipment gateway for managing an Application Layer Gateway functionality in a telecommunication network comprising at least one endpoint, said Customer Premises Equipment gateway and a Network Address Translation Carrier Grade Network device, said at least one endpoint being configured for communicating packets with said Network

Address Translation Carrier Grade Network device through the Customer Premises Equipment gateway, the Network Address Translation Carrier Grade Network device being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint, said Customer Premises Equipment gateway being configured for performing an Application Layer Gateway functionality on a communicated packet.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for managing application control sessions.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for managing pinholes reservation.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for managing Network Address Translation control, like e.g. managing a Network Address Translation control session and exchanging Network Address Translation control messages.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for analyzing a communicated packet received from an endpoint.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for sending, to the Network Address Translation Carrier Grade Network device, a request for a Network Address Translation pinhole and for receiving, from the Network Address Translation Carrier Grade Network device, a Network Address Translation pinhole allocation.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for transmitting the communicated packet received from the endpoint to the Network Address Translation Carrier Grade Network device using a Network Address Translation pinhole.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for receiving a packet on which a Network Address Translation functionality has been previously performed by the Network Address Translation Carrier Grade Network device and for routing said received packet to the corresponding endpoint.

In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for performing a Network Address Translation mapping on the packet received from the endpoint, for performing a Network Address Translation functionality, for receiving a packet on which a Network Address Translation functionality has not yet been performed, for performing a

Network Address Translation functionality on the received packet and for routing said received packet to the corresponding endpoint.

In an embodiment according to the invention, the Application Layer Gateway management unit is further configured for performing NAT functionality.

5 In an embodiment according to the invention, the Customer Premises Equipment gateway is further configured for communicating with the Network Address Translation Carrier Grade Network device using a Port Control Protocol (PCP)

10 In an embodiment according to the invention, the Network Address Translation control management unit of the Customer Premises Equipment gateway comprises a Port Control Protocol client configured for managing Port Control Protocol sessions and exchanging Port Control Protocol messages.

15 In an embodiment according to the invention, the Network Address Translation Carrier Grade Network device is configured for managing application control sessions, for determining if a packet needs applying Network Address Translation functionality, for managing pinholes reservation and for managing Network Address Translation control, like e.g. managing a Network Address Translation control session and exchanging Network Address Translation control messages.

20 In an embodiment according to the invention, the Network Address Translation control management unit of the Network Address Translation Carrier Grade Network device comprises a Port Control Protocol server configured for managing Port Control Protocol sessions and exchanging Port Control Protocol messages.

25 The invention also concerns a system for managing an Application Layer Gateway functionality comprising a telecommunication network comprising at least one endpoint, a Customer Premises Equipment gateway and a Network Address Translation Carrier Grade Network device, said at least one endpoint being configured
30 for communicating packets with said Network Address Translation Carrier Grade Network device through said Customer Premises Equipment gateway, the Network Address Translation Carrier Grade Network device being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint, the Customer Premises Equipment gateway being configured for
35 performing an Application Layer Gateway functionality on a communicated packet.

The invention also concerns a readable computer program for managing an Application Layer Gateway functionality comprising instructions, which, when executed by a processor, perform the method as described here above.

5 **Brief Description of the Drawings**

Embodiments of the present invention will now be described solely by way of example and only with reference to the accompanying drawings, where like parts are provided with corresponding reference numerals, and in which:

Figure 1 schematically illustrates the system according to the invention.

10 Figure 2 illustrates a first embodiment of the method according to the invention.

Figure 3 illustrates a second embodiment of the method according to the invention.

15 **Description of Preferred Embodiments**

The following are descriptions of exemplary embodiments that when taken in conjunction with the drawings will demonstrate the above noted features and advantages, and introduce further ones.

20 In the following description, for purposes of explanation rather than limitation, specific details are set forth such as architecture, interfaces, techniques, and devices etc., for illustration. However, it will be apparent to those of ordinary skill in the art that other embodiments that depart from these details would still be understood to be within the scope of the appended claims.

25 Moreover, for the purpose of clarity, detailed descriptions of well-known devices, systems, and methods are omitted so as not to obscure the description of the present system. Furthermore, routers, servers, nodes, gateways or other entities in a telecommunication network are not detailed as their implementation is beyond the scope of the present system and method.

30 Unless specified otherwise, the exemplary embodiment will be described hereafter in its application to a gateway of a telecommunication network.

In addition, it should be expressly understood that the drawings are included for illustrative purposes and do not represent the scope of the present system.

35 The system according to the invention, illustrated by figure 1, comprises an endpoint or host to, a host network 20, a Customer Premises Equipment (CPE) gateway 30, an Internet Service Provider Carrier Grade Network (ISP CGN) 40, a

Network Address Translation (NAT) Carrier Grade Network (CGN) device 50, a public network 60, like e.g. the internet, and a corresponding node 70. The system according to the invention may comprise a plurality of each of the cited networks and devices.

5 The endpoint 10 is configured for communicating with the corresponding node 70 through the host network 20, the CPE gateway 30, the ISP CGN 40, the NAT CGN device and the public network 60. By communicating, it is meant sending and/or receiving packets of data through a network and/or a device.

10 The endpoint 10 may be, for example, a terminal such as a Personal Computer, a tablet PC, a laptop, a phone, like e.g. a smartphone etc. Endpoints are connected to the CPE gateway through the host network.

The host network 20 may be a home network and is configured for connecting the endpoint 10 to the CPE gateway 30.

15 The CPE gateway 30 is configured for communicating, on one side, with the endpoint 10 through the host network 20, and, on another side, with the NAT CGN device 50 through the ISP CGN 40. The CPE gateway 30 comprises an Application Layer Gateway (ALG) management unit 32 configured for performing ALG functionality and for managing application control sessions, a reservation management unit 33 configured for managing pinholes reservation and a NAT control management unit 34 configured for managing NAT control like e.g. managing a NAT control session and exchanging NAT control messages. The ALG management unit 32 may be further configured to perform NAT functionality. The NAT control management unit 34 may comprise, for example, a PCP client configured for managing PCP sessions and exchanging PCP messages. The CPE gateway 30 may be a Digital Subscriber Line (DSL) router.

25 The ISP CGN 40 may be a private network managed by a telecommunication operator for providing endpoints 10 of the host network 20 with access, through the NAT CGN device 50, to the public network 60, and therefore to a corresponding node 70, for communicating using packets of data.

30 The NAT CGN device 50 is configured for performing NAT functionality, or, in other words, for performing Network Address Translation on the header of the packet. The NAT CGN device 50 comprises a NAT management unit 52 configured for managing application control sessions, for determining if a packet needs applying NAT functionality and for performing NAT functionality, a reservation management unit 53 configured for managing pinholes reservation and a NAT control management unit 54 configured for managing NAT control like e.g. managing a NAT control session and exchanging NAT control messages. The NAT control management unit 54

may comprise, for example, a PCP server configured for managing PCP sessions and exchanging PCP messages.

5 The ALG management unit 32 is configured for communicating, in an application control session on a communication link 43 through the ISP CGN 40, with the NAT management unit 52. For example, such an application control session may be used to exchange FTP control commands, SIP signaling messages or any application control messages.

10 The NAT control management unit 34 is configured for communicating, in a NAT control protocol session on a communication link 45 through the ISP CGN 40, with the NAT control management unit 54. For example, such a NAT control protocol session may be used to exchange PCP messages.

The public network 60 may be, for example, the internet.

The corresponding node 70 may be a terminal or a server connected to the public network 60.

15 Several communication protocols may be used to communicate in the system according to the invention. For example, an Internet Protocol may be used at the network layer level, FTP or SIP protocols may be used to communicate at the application layer level.

20 In an embodiment described here under in reference to figure 3, the telecommunication network is based on the known Dual-Stack Lite (DS Lite) network architecture.

As described here above, Dual-Stack Lite is one technology or network architecture solution used to address IPv4 address shortage in IPv4-based telecommunication networks while migrating to IPv6-based telecommunication networks. DS Lite involves moving a NAT functionality performed by a Customer Premises Equipment gateway to a NAT CGN device, i.e. a device for performing NAT located between the ISP CGN and the public network. DS Lite also involves communicating IPv4-type packets over IPv6 using known IPv4-in-IPv6 Softwires, which is an IP in IP tunnel defined in the Request For Comments (RFC) 5571. In DS Lite, the CPE gateway 30 implements a Basic Bridging Broad Band (B4) element or function and the NAT CGN device 50 implements an Address Family Transition Router (AFTR) element or function. The B4 element allows creating an IP tunnel to the AFTR element while the AFTR element is a combination of an IPv4-in-IPv6 tunnel end-point and an IPv4-IPv4 NAT functionality implemented on the same NAT CGN device 50. In a telecommunication network comprising a plurality of CPE gateways

25
30
35

30, each CPE gateway 30 is assigned a global IPv6 prefix and dynamically allocates private IPv4 addresses, which are in a format in compliance with e.g. RFC1918, to the endpoints 10 located in the associated host network 20. The packets communicated by endpoints 10 are encapsulated and tunneled to the NAT CGN device 50 by the CPE gateway 30 using a IPv4-in-IPv6 Softwire, where the B4 element acts as a Softwire Initiator (SI) and the AFTR element acts as a Softwire Concentrator (SC). The AFTR performs IPv4-IPv4 NAT functionality to multiplex a plurality of communications with a plurality of endpoints 10 through a pool of global IPv4 addresses. Overlapping address spaces used by endpoints are disambiguated through identification of tunnels endpoints.

In the embodiment of the method according to the invention described here above in reference to figure 3 using the DS Lite solution, a Port Control Protocol (PCP) is used to control how incoming packets are transmitted by NAT devices. PCP may be used in DS Lite context, but also with other IPv4-IPv6 migration solutions like NAT64 or Large-Scale NAT444. PCP allows an endpoint 10 to operate a communication permanently, e.g. a webcam communication, or temporarily, e.g. while playing a game in a communication, by creating pinholes from an external IP address to an internal IP address and port. PCP works on a client/server model. A PCP client is a PCP software instance responsible for issuing PCP requests to a PCP server. PCP clients may either be located on the endpoint 10 or on the CPE gateway 30. PCP server may either be separated or embedded within a NAT device.

The method according to the invention will now be described in reference to figures 2 and 3.

In a first embodiment of the method according to the invention, described on figure 2, an endpoint 10 sends, in act Eo, a packet in order to initialize a communication with the corresponding node 70. The packet comprises here, in its payload, an internal IP address and an internal port to inform the corresponding node 70 to connect to the endpoint 10 on said internal IP address and an internal port. The packet comprises also an ID to identify the endpoint.

The packet is received by the CPE gateway 30 and the ALG management unit 32 analyzes, in act E1, whether the received packet needs applying ALG functionality. The received packet may need applying ALG, for example, if the IP header of the received packet comprises a 5-tuple (internal IP address, internal port, corresponding node 70 IP address, corresponding node port, protocol) and the payload of the received packet comprises internal IP address and internal port.

When the ALG management unit 32 determine that the received packet needs applying ALG functionality, the reservation management unit 33 of the CPE gateway 30 sends, in act E2, via the NAT control management unit 34, a NAT control message, using e.g. PCP, on the communication link 45, to the NAT control management unit 54 of the NATCGN device 50 for requesting an NAT pinhole.

The NAT control management unit 54 of the NAT CGN device 50 receives the NAT control message and the reservation management unit 53, in act E3, assigns, for the communication of the packet to the corresponding node 70 through the NATCGN device 50, a pair of external IP address and external port, and then creates a NAT mapping relating external IP address and external port to endpoint ID, internal IP address and internal port, e.g. a NAT mapping (subscriber ID, internal IP address, internal port) <-> (external IP address, external port, protocol).

In act E4, the NAT control management unit 54 sends an allocated NAT pinhole via a NAT control protocol message (e.g. PCP) to the NAT control management unit 34 of the CPE gateway 30.

The ALG management unit 32 performs ALG functionality on the packet payload wherever internal IP and internal port exists, e.g. the packet payload is translated from (internal IP and internal port) to (external IP and external port), and then sends, in act E6, on the communication link 43, the packet to the NAT management unit 52 of the NATCGN device 50.

In act E7, the NAT management unit 52 allows performing NAT on the packet which corresponds to one of the NAT mapping entry that was created by the NAT pinhole control message in act E3, and send it, in act E8, to the corresponding node 70.

The embodiment, illustrated by figure 2, also demonstrates an example of how a communication packet sent by the corresponding node 70 to the endpoint 10 traverses the NATCGN device 50. Such a packet may be, for example, a packet with 5-tuple IP header (corresponding node 70 IP address, corresponding node 70 port, external IP address, external port, TCP).

When a packet is received by the NAT management unit 52 of the NAT CGN device 50 for sending to an endpoint 10, the reservation management unit 53 checks, in act Eio, if the packet corresponds to one of the mapping entries previously NATed on the packet header by NATCGN device 50. If so, the NATCGN device 50 transmits, via the NAT management unit 52, in act Ell, the packet to the ALG management unit 32 of the CPE gateway 30, which then routes the packet to the corresponding endpoint 10.

In a second embodiment of the method according to the invention, described on figure 3, the NAT CGN device 50 performs NAT functionality both on the packet header and the payload, i.e. applies also ALG functionality.

5 In this embodiment, an endpoint 10 sends, in act Eo, a packet in order to initialize a communication with the corresponding node 70. The packet comprises here, in its payload, an internal IP address and an internal port to inform the corresponding node 70 to connect to the endpoint 10 on said internal IP address and an internal port. The packet comprises also an ID to identify the endpoint.

10 The packet is received by the CPE gateway 30 and the ALG management unit 32 analyzes, in act E1, whether the received packet needs applying ALG functionality. The received packet may need applying ALG, for example, if the IP header of the received packet comprises a 5-tuple (internal IP address, internal port, corresponding node 70 IP address, corresponding node port, protocol) and the payload of the
15 received packet comprises internal IP address and internal port.

When the ALG management unit 32 determines that the received packet needs applying ALG functionality, the reservation management unit 33 of the CPE gateway 30 sends, in act E2, via the NAT control management unit 34, a NAT control message, using e.g. PCP, on the communication link 45, to the NAT control management unit
20 54 of the NAT CGN device 50 for requesting an NAT pinhole.

The NAT control management unit 54 of the NAT CGN device 50 receives the NAT control message and the reservation management unit 53, in act E3', assigns, for the communication of the packet to the corresponding node 70 through the NAT CGN device 50, a pair of external IP address and external port, reserves this NAT pinhole
25 relating to endpoint ID and then add the allocated NAT pinhole to its bypass rules e.g. (endpoint ID, external IP, external port).

In act E4, the NAT control management unit 54 sends an allocated NAT pinhole via a NAT control protocol message (e.g. PCP) to the NAT control management unit 34 of the CPE gateway 30.

30 The reservation management unit 33 creates, in act E5', a NAT mapping according to the obtained NAT pinhole, e.g. (internal IP address, internal port) <-> (external IP address, external port, protocol).

The ALG management unit 32 of the CPE gateway 30 performs, in act E5", ALG and NAT functionalities on the packet wherever internal IP address and internal port exists, and then sends, in act E6, on the communication link 43, the packet to the
35 NAT management unit 52 of the NAT CGN device 50. For example, packet header may

be translated from (internal IP address, internal port, corresponding node 70 IP address, corresponding node 70 port, protocol) to (external IP address, external port, corresponding node 70 IP address, corresponding node 70 port, protocol) and packet payload translated from (internal IP address and internal port) to (external IP address and external port).

In act E7', the NAT management unit 52 allows the packet to bypass or go through the NAT CGN device 50 using the matching bypass rule, set up in act E3', and sends it, in act E8, to the corresponding node 70.

The embodiment, illustrated by figure 3, also demonstrates an example of how a communication packet sent by the corresponding node 70 to the endpoint 10 traverses the NAT CGN device 50. Such a packet may be, for example, a packet with 5-tuple IP header (corresponding node 70 IP address, corresponding node 70 port, external IP address, external port, TCP).

When a packet is received, in act E9, by the NAT management unit 52 of the NAT CGN device 50, for connecting to the endpoint 10, the reservation management unit 53 checks, in act E10', if a bypass rule has been previously set up (in act E3'). If so, the packet is transmitted, in act E11, by the NAT management unit 52, according to the endpoint 10 ID of the bypassing rule, to the ALG management unit 32 of the CPE gateway 30, which, perform, in act E11', ALG and NAT functionalities on the packet according to the NAT mapping entry created in act E5',

The packet is then transmitted, in act E12, to the corresponding endpoint 10, for example, by reaching the port which is identified by the internal IP address and internal port of the translated 5-tuple IP packet header.

The method according to the invention will now be described, still in reference to figure 3, in a Dual-Stack Lite telecommunication network wherein, in an embodiment, the endpoint 10 comprises a FTP client and the corresponding node 70 comprises a FTP server for communicating using the corresponding units and, in another embodiment, the endpoint 10 comprises a FTP server and the corresponding node 70 comprises a FTP client for communicating using the corresponding units.

In these exemplary embodiments, the CPE gateway 30 is a B4 element, embedding a FTP ALG functionality and a PCP client, and the NAT CGN device 50 is an AFTR 50 element embedding a PCP server. FTP active mode and passive mode are supported by this ALG functionality of the B4 element 30 in these embodiments. The ALG management unit 32 allows applying ALG functionality to FTP PORT command when the endpoint 10 runs a FTP client. The ALG management unit 32 allows

applying ALG functionality to PASV response when the endpoint 10 runs a FTP server.

In one embodiment, described in reference to figure 3, the endpoint 10 runs a FTP client and the corresponding node 70 runs a FTP server.

5 In active mode, the FTP client connects from a random unprivileged port ($N > 1023$) to the FTP server's command port, e.g. port 21. Then, the FTP client starts to listen on port $N+i$ and sends the FTP command PORT $N+i$ to the FTP server. The server will then connect back to the FTP client's specified data port from its local data port, which is e.g. port 20. Assuming an FTP client is listening on internal IP and internal port (e.g. PrilP: aaaa) and issue a FTP PORT command containing internal IP and internal port (PrilP, aaaa) in the payload of the packet to inform the FTP server to connect to (PrilP: aaaa), the process of how an FTP ALG functionality deployed on the B4 30 works with the AFTR 50 to make FTP data connection traverse AFTR 50 as described in reference to figure 3.

15 FTP ALG module on the B4 30 is monitoring, in act E1, the FTP traffic of packets, received in act E0. In other words, the B4 30 determines, in act E1, that a packet needs be applied ALG functionality.

Once the B4 30 has determined, in act E1, that a packet needs be applied ALG functionality, e.g. by finding a PORT command containing internal IP address and internal port, it goes to the next act. An example of packet that triggers ALG function may have an IP header with 5 tuple e.g. (PrilP, aaaa, SrvIP, 21, TCP), and a payload containing (PrilP, aaaa).

The B4 30 issues, in act E2, a PCP request to AFTR 40 requesting an NAT pinhole.

25 The AFTR 50 assigns, in act E3', a pair of external IP and external port, then reserve the NAT Pinhole relating to requested endpoint ID and add it to its bypass rules e.g. (Tunnel ID, ExtIP, bbbb).

The AFTR 50 returns, in act E4, to the B4 30, an allocated NAT pinhole via a PCP response.

30 The B4 30 creates, in act E5', a NAT mapping according to the obtained NAT Pinhole, e.g. (PrilP, aaaa) <-> (ExtIP, bbbb, TCP).

The B4 30 performs, in act E5'', FTP ALG and NAT on the packet (header and payload) wherever internal IP address and internal port exists,; e.g. packet header translated from (PrilP, aaaa, SrvIP, 21, TCP) to (ExtIP, bbbb, SrvIP, 21, TCP) and packet payload translated from (PrilP, aaaa) to (ExtIP, bbbb).

35 The B4 30 then sends out, in act E6, the packet to the AFTR 50.

The AFTR 50 bypasses, in act E7', the packets that match bypass rules e.g. (Tunnel ID, ExtIP, bbbb) created in act E3' and send it out, in act E8, to the FTP server of the corresponding node 70.

An incoming packet, e.g. a packet with 5-tuple IP header (SrvIP, 20, ExtIP, bbbb, TCP), sent by the FTP server of the corresponding node 70, may try to reach the endpoint's 10 FTP listening data port. When the packet is received, in act E9, by the AFTR 50 and if, in act E10', the packet corresponds to one of the AFTR 50 bypass rules, e.g. created in act E3', the packet bypass the AFTR 50, i.e. is transferred by the AFTR 50, in act E11, to the B4 30 according to tunnel ID of the bypassing rule e.g. (Tunnel ID, ExtIP, bbbb). ALG functionality is performed, in act E11', by B4 30 from (SrvIP, 20, ExtIP, bbbb, TCP) to (SrvIP, 20, PrilP, aaaa, TCP) according to the B4 30 mapping entry e.g. (PrilP, aaaa) <-> (ExtIP, bbbb, TCP) which was created in act E3'. Finally, the packet is sent by B4 30, in act E12, onto the listening port aaaa of the FTP server of the endpoint 10, which is identified by translated 5-tuple IP header e.g. 8 (SrvIP, 20, PrilP, aaaa, TCP).

In another embodiment, described still in reference to figure 3, the endpoint 10 runs a FTP server and the corresponding node 70 runs a FTP client.

In order to resolve the issue of a FTP server initiating a connection to a FTP client, a known method, called passive mode or PASV, is used. The FTP client notifies the FTP server it is in passive mode. In passive mode, the FTP client initiates both connections to the FTP server. However, when a FTP server is run by an endpoint behind an AFTR 50, ALG functionality is needed to translate the PASV response payload where containing internal IP address and port of the FTP server. Besides, to ensure FTP server command channel can be reached by the incoming connection from any clients, the port number 21 of the FTP server needs to be forwarded to the AFTR 50 by means of e.g. static reservation or PCP pinhole reservation. If an FTP server received a PASV command from a FTP client, it will listen on an unprivileged local ports e.g. cccc and response "227 Entering Passive Mode" containing private IP address and port e.g. (PrilP: cccc) in the payload to inform the FTP client to connect to (PrilP: cccc).

The FTP ALG functionality of the B4 30 monitors, in act E1, the FTP traffic packets received, in act E0, from the FTP server of the endpoint 10. In other words, the B4 30 determines, in act E1, that a packet needs be applied ALG functionality. Such a packet may have e.g. a IP header with 5 tuple e.g. (PrilP, cccc, ClilP, 21, TCP) and payload containing "227 Entering Passive Mode" (PrilP, , cccc).

Once the B4 30 has determined, in act E1, that a packet needs be applied ALG functionality, for example, when a PASV command response contains internal IP address and internal port, the B4 30 issues, in act E2, a PCP request to the AFTR 50 for requesting an NAT pinhole.

5 The AFTR 50 assigns, in act E3', a pair of external IP and external port and reserve this NAT Pinhole relating to requested Subscriber ID, and then add it to its bypass rules, e.g. (Tunnel ID, ExtIP, dddd).

The AFTR 50 returns, in act E4, to the B4 30, an allocated NAT pinhole via a PCP response.

10 The B4 30 creates, in act E5', a NAT mapping according to the obtained NAT Pinhole e.g. 4 (PrilP, cccc) <-> (ExtIP, dddd, TCP)

The B4 30 performs, in act E5", ALG and NAT functionalities, where internal IP and internal port exists, e.g. packet header translated from (PrilP, cccc, CHIP, 21, TCP) to (ExtIP, dddd, peer IP, CHIP, 21, TCP) and packet payload translated from (PrilP, cccc) to (ExtIP, dddd).

15 The B4 30 then sends out, in act E6, the packet to the AFTR 50.

The AFTR 50 bypasses, in act E7', the packets that match bypass rules e.g. (Tunnel ID, ExtIP, dddd) created in act E3' and send it out, in act E8, to the FTP client of the corresponding node 70.

20 An incoming packet, e.g. a packet with 5-tuple IP header (CHIP, 21, ExtIP, dddd, TCP), sent by the FTP client of the corresponding node 70, may try to reach the endpoint's 10 FTP server. When the packet is received, in act E9, by the AFTR 50 and if, in act E10', the packet corresponds to one of the AFTR 50 bypass rules, e.g. created in act E3', the packet bypass the AFTR 50, i.e. is transferred by the AFTR 50, in act E11, to the B4 30 according to tunnel ID of the bypassing rule e.g. (Tunnel ID, ExtIP, dddd). ALG functionality is performed, in act E11', by B4 30 from (CHIP, 21, ExtIP, dddd, TCP) to e.g. 8 (CHIP, 20, PrilP, cccc, TCP) according to the B4 30 mapping entry e.g. (PrilP, cccc) <-> (ExtIP, dddd, TCP) which was created in act E3'. Finally, the packet is sent by B4 30, in act E12, onto the listening port cccc of the FTP server of the endpoint 10, which is identified by translated 5-tuple IP header e.g. 8 (CHIP, 20, PrilP, cccc, TCP).

CLAIMS

1. A method of managing an Application Layer Gateway functionality in a telecommunication network comprising at least one endpoint (10), a Customer Premises Equipment gateway (30) and a Network Address Translation Carrier Grade Network device (50), said at least one endpoint (10) being configured for communicating packets with said Network Address Translation Carrier Grade Network device (50) through said Customer Premises Equipment gateway (30), the Network Address Translation Carrier Grade Network device (50) being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint (10), said method comprising, for the Customer Premises Equipment gateway (30), the act of performing an Application Layer Gateway functionality on a communicated packet.
2. A method according to claim 1, said method further comprising an act of managing an application control session of the communicated packet.
3. A method according to any of the preceding claims, said method further comprising an act of managing pinholes reservation.
4. A method according to any of the preceding claims, said method further comprising an act of managing Network Address Translation control.
5. A method according to claim 4, wherein the act of managing is performed using a Port Control Protocol.
6. A method according to any of the preceding claims, said method further comprising an act of performing a Network Address Translation functionality on the received packet and an act of routing said received packet to the corresponding endpoint (10).
7. A Customer Premises Equipment gateway for managing an Application Layer Gateway functionality in a telecommunication network comprising at least one endpoint (10), said Customer Premises Equipment gateway (30) and a Network Address Translation Carrier Grade Network device (50), said at least one endpoint (10) being configured for communicating packets with said Network Address Translation Carrier Grade Network device (50) through the Customer Premises

Equipment gateway (30), the Network Address Translation Carrier Grade Network device (50) being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint (10), said Customer Premises Equipment gateway (30) being configured for performing an Application Layer Gateway functionality on a communicated packet.

8. A Customer Premises Equipment gateway according to claim 7, said Customer Premises Equipment gateway (30) being further configured for managing application control sessions.

9. A Customer Premises Equipment gateway according to any of claims 7 and 8, said Customer Premises Equipment gateway (30) being further configured for managing pinholes reservation.

10. A Customer Premises Equipment gateway according to any of claims 7 to 9, said Customer Premises Equipment gateway (30) being further configured for managing Network Address Translation control.

11. A system for managing an Application Layer Gateway functionality comprising a telecommunication network comprising at least one endpoint (10), a Customer Premises Equipment gateway (30), according to any of claims 7 to 10, and a Network Address Translation Carrier Grade Network device (50), said at least one endpoint (10) being configured for communicating packets with said Network Address Translation Carrier Grade Network device (50) through said Customer Premises Equipment gateway (30), the Network Address Translation Carrier Grade Network device (50) being configured for performing a Network Address Translation functionality on a packet communicated with the at least one endpoint (10), the Customer Premises Equipment gateway (30) being configured for performing an Application Layer Gateway functionality on a communicated packet.

12. A readable computer program for managing an Application Layer Gateway functionality comprising instructions, which, when executed by a processor, perform the method according to any of claims 1 to 6.

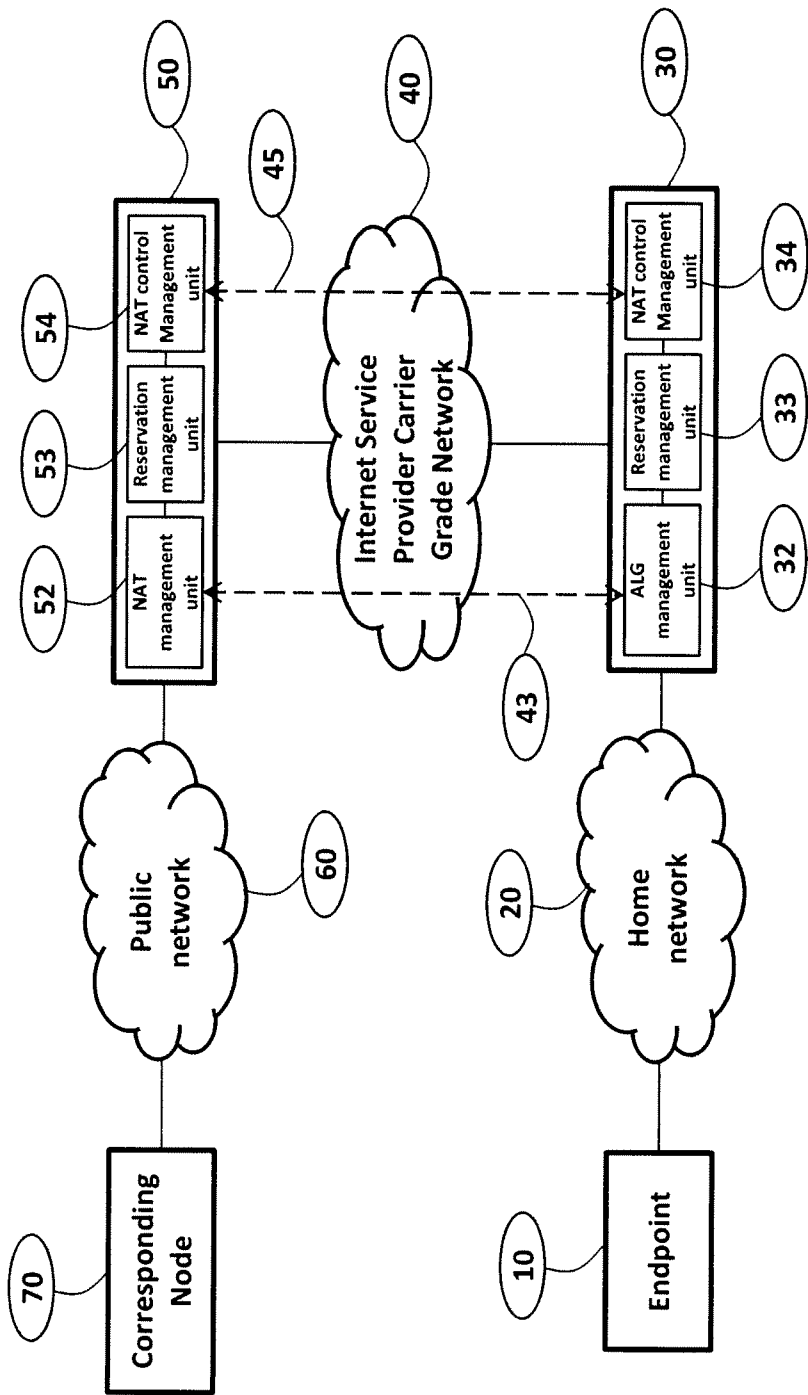


Figure 1

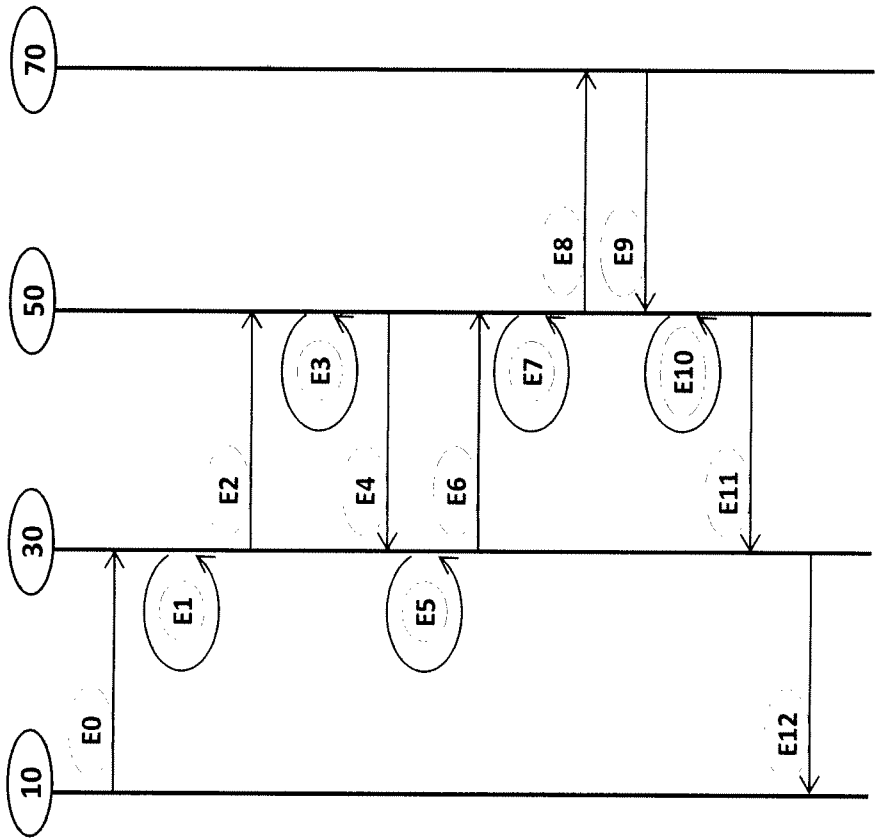


Figure 2

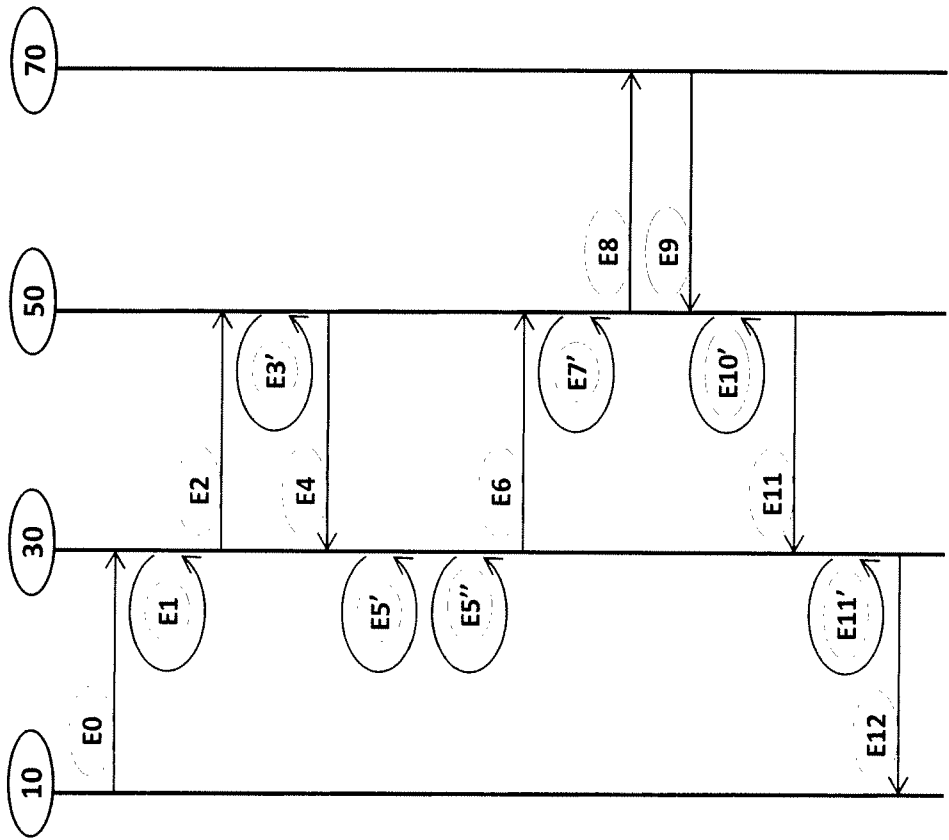


Figure 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/002922

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/12

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal , COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>DURAND JUNIPER NETWORKS R DROMS CISCO J WOODYATT APPLE Y LEE COMCAST A: "Dual -Stack Lite Broadband Deployments Following IPv4 Exhaustion; rfc6333 .txt" , DUAL-STACK LITE BROADBAND DEPLOYMENTS FOLLOWING IPV4 EXHAUSTION; RFC6333.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 8 August 2011 (2011-08-08) , pages 1-32 , XP015081258, [retrieved on 2011-08-08] sections 1, 4.2 , 8.3 , 8.5 ; figures 1-3</p> <p style="text-align: center;">----- -/--</p>	1-12



Further documents are listed in the continuation of Box C.



See patent family annex.

*** Special categories of cited documents :**

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

3 June 2013

Date of mailing of the international search report

07/06/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bbhmert, Jbrg

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/002922

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SRISURESH KUOKOA NETWORKS J KUTHAN FRAUNHOFER INSTITUTE FOKUS J ROSENBERG DYNAMICSOFT A MOLITOR ARAVOX TECHNOLOGIES A RAYHAN RYERS: "Mi ddl ebox communi cati on archi tecture and framework; rfc3303 .txt" , 20020801 , 1 August 2002 (2002-08-01) , XP015009080, ISSN: 0000-0003 secti ons 1, 2.1, 2.2, 2.6 to 2.8, 5.0 -----	1-12
A	SI P wg J ROSENBERG ET AL: "Getti ng SI P through Fi rewal l s and NATs; draft-rosenberg-si p-fi rewal ls-00. txt" , 20000222 , 22 February 2000 (2000-02-22) , XP015034699 , ISSN: 0000-0004 secti ons 2.2, 5, 5.1, 5.2 -----	1-12
A	J. William Atwood ET AL: "I Pv4/I Pv6 Transl ati on - Allowi ng I Pv4 hosts to communi cate wi th I Pv6 hosts wi thout modi fyi ng the software on the I Pv4 or I Pv6 hosts" , , 23 July 2003 (2003-07-23) , pages 1-12 , XP055020159 , Montreal , Quebec Retri eved from the Internet: URL: http://www. kernel .org/doc/ol s/2003/ol s 2003-pages-34-43 .pdf [retri eved on 2012-02-23] secti ons 2.2 and 2.3 -----	1-12
X, P	ZHOU HUAWEI TECHNOLOGIES T TSOU HUAWEI TECHNOLOGIES (USA) C: "Scenari os of I Pv4 sunsetti ng; draft-zhou-sunset4-scenari os-00. txt" , SCENARIOS OF I PV4 SUNSETTING; DRAFT-ZHOU-SUNSET4-SCENARIOS-00.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 9 July 2012 (2012-07-09) , pages 1-7 , XP015083979 , [retri eved on 2012-07-09] secti on 4.4 -----	1,6,7 , 11, 12