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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 November 2004 (18.11.2004)

PCT

(10) International Publication Number
WO 2004/100499 A1

(51) International Patent Classification[7]: H04L 29/12

(21) International Application Number:
PCT/IB2004/050578

(22) International Filing Date: 4 May 2004 (04.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101259.4 7 May 2003 (07.05.2003) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NIKOLOVA, Mariana, V.** [BG/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **SIMONS, David, P., L.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

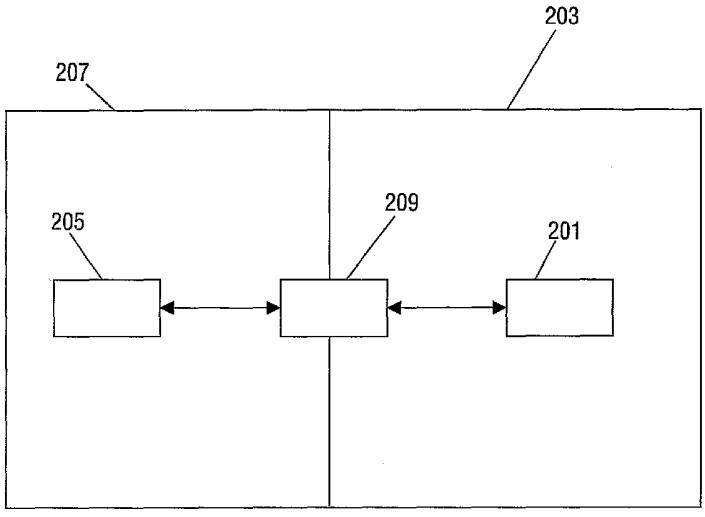
(74) Agent: **GROENENDAAL, Antonius, W., M.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

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

*[Continued on next page]*

(54) Title: A COMMUNICATION NETWORK, A NETWORK ELEMENT AND COMMUNICATION PROTOCOL AND METHOD OF ADDRESS AUTO-CONFIGURATION THEREFOR




(57) Abstract: The invention relates to a system for address auto-configuration for a first network element (201), being part of a first network (203) connected to a second network (207) through a gateway element (209). The first network element transmits an address inquiry message to a second network element (205) requesting an address of the gateway element (209). The second network element (205) in response transmits an address response message comprising a gateway address of the gateway element (209). Upon receiving the address response message, the first network element generates a first address in response to the gateway address. The gateway element (209) may specifically be an IPv4 home router for a private home network and the first network element (201) may be a combined IPv6/IPv4 network element. The first network element (201) may be provided with the public IPv4 address of the private home network from the second network element (205) thereby enabling it to generate an IPv6 address from the public IPv4 address.

WO 2004/100499 A1

**Declaration under Rule 4.17:**

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

**Published:**

— *with international search report*

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

# A communication network, a network element and communication protocol and method of address auto-configuration therefor

The invention relates to a communication network, a network element and communication protocol and method of address auto-configuration therefor and in particular to a system for address auto-configuration of an Internet Protocol address.

In recent years communication networks for data communication has become increasingly widespread. For example, there has been an immense growth in the use of the Internet, which is now used by a very large group of people. This has lead to an explosive growth in the number of terminals and network elements being interconnected, and this has exposed limitations in the fundamental standards used for the Internet.

Specifically, the data communication on the Internet is conventionally made in accordance with the Internet Protocol version 4 (IPv4) as standardized by the Internet Engineering Task Force (IETF). However, IPv4 uses a network node address that is limited to 32 bits. This significantly limits the number of available unique addresses, and it is expected that the number of required addresses quickly will exceed the number of possible IPv4 addresses.

The IETF has standardised the Internet Protocol version 6 (IPv6) in RFC (Request for Comments) 2460, Internet Protocol, Version 6 (IPv6) Specification, December 1998. IPv6 overcomes the address limitation by introducing 128 bit IPv6 addresses. This allows for a significantly increased number of available unique addresses, which is expected to be sufficient for a long time. IPv6 furthermore addresses a number of other limitations and shortcomings of IPv6 and for example includes functionality facilitating mobility and security.

However, although IPv6 solves some of the problems inherent to IPv4, it also introduces additional problems and technical challenges. Especially coexistence and interoperability of IPv4 and IPv6 devices is critical for the successful introduction of IPv6 into an existing IPv4 communication network such as the Internet.

One important aspect of interoperability and co-existence of IPv4 and IPv6 is the auto-configuration of IPv6 addresses. IETF has standardised two methods of configuring

the IPv6 address of a network device. One is known as the Stateless Address Auto-configuration and is standardised in RFC 2462, IPv6 Stateless Address Auto-configuration, December 1998. This approach requires no manual configuration of hosts, minimal (if any) configuration of routers, and no dedicated servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (e.g. MAC (Media Access Control) addresses) and information advertised by routers (e.g. a prefix).

The other address auto-configuration method is the IPv6 Stateful Address Auto-configuration that is described in RFC draft-ietf-dhc-dhcpv6-28.txt, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), October 2002. This approach requires the use of servers, e.g. DHCPv6 server, maintaining a database keeping track of which addresses have been assigned to which hosts. In this case, the hosts obtain interface addresses and/or configuration information and parameters from the server.

Private home IP networks, wherein a local network is connected to the Internet through a home router, have become increasingly popular in recent years. In these networks, private addresses, which are not known externally of the private home network, are used for addressing devices within the private home network. Typically, the home router has a single public IPv4 address for use in the public network as well as a private IPv4 address for use within the private home network.

Specifically, a private home network typically has a single subscription with an Internet Service Provider (ISP) that provides a single public IPv4 address (e.g. 130.145.174.7) to the home router, which is connected to the IPv4 Internet via a (broadband) modem. The home router can be either a software or hardware entity offering functionalities like routing, DHCP server, firewall, etc.

The private home network further has a number of private IPv4 addresses (e.g. 192.168.0.1, 192.168.0.2, etc., as defined in RFC 1918, Address Allocation for Private Internets, February 1996) assigned to the home devices by a DHCP server running on the home router. However, these addresses are private addresses and are not known externally to the private home network. Typically, the home router runs the NA(P)T (Network Address (Port) Translation) software as described in RFC 3022, Traditional IP Network Address Translator (Traditional NAT), January 2001, in order to map private into public IPv4 addresses and vice versa. Then, external devices can address a specific device in the private home network if a dedicated software runs on the home router. However, this is a complicated process based on software that is applications specific and requires specific set up in order to provide this functionality.

Private home IP networks, which are currently fully IPv4 based, should preferably be adapted to allow for introduction of IPv6 devices and for a transition to an IPv6 based private home network. Specifically, it would be advantageous if the IPv6 devices of a private home network can always auto-configure their global IPv6 address that may be used to address the IPv6 devices from the external network. However, each existing method for auto-configuration of network device is limited to a specific network topology or arrangement and is not generally applicable to all private home networks. Furthermore, some network topologies and configurations are not suitable for determining an address of device in a private home network in accordance with the known methods.

Hence, an improved system for address auto-configuration would be advantageous and in particular a system allowing for address auto-configuration in different network arrangements or configurations and/or where limited information is available would be advantageous.

Accordingly, the Invention preferably seeks to mitigate, alleviate or eliminate one or more of the above mentioned disadvantages singly or in any combination.

Specifically, the inventors have realised that address auto-configuration depends on the network arrangement or configuration. Specifically, the inventors have realised that address auto-configuration may preferably in some arrangements be based on a gateway address of a gateway element connecting two networks. The inventors have furthermore realised that in some network arrangements or configurations such information may not be available. Specifically, the inventors have realised that if a combined IPv4 and IPv6 network element is coupled to an IPv4-only gateway element (but not to other IPv6 network elements), an IPv6 address may preferably be generated by the public IPv4 address of the gateway element. However, the inventors have furthermore realised that the public IPv4 address is not available in the private home network.

According to a first aspect of the invention, there is provided a method of address auto-configuration for a first network element being part of a first network connected to a second network through a gateway element, the method comprising the steps of: sending an address inquiry message to a second network element requesting an address of the gateway element; receiving an address response message from the second network element comprising a gateway address of the gateway element; and generating a first address of the first network element in response to the gateway address.

Specifically, the first network may be a private network, the second network may be the Internet and/or the gateway element may be a home router. The network element may be a network node. The method allows for the first address to be generated based on the address of the gateway element even if this address is not directly available to the first network element. Hence, a simple and flexible method of address auto-configuration is provided which may be used in network configurations wherein information related to an address of the gateway element is not directly available.

According to a feature of the invention, the first address is in accordance with a different address protocol than the gateway address. Advantageously, the gateway address may be used to determine an address which is according to a different address protocol.

According to another feature of the invention, the first address is an IPv6 address and the gateway address is an IPv4 address.

Thus the invention allows for an IPv6 address to be generated from an IPv4 address of the gateway element and in particular may be generated from the public IPv4 address of a gateway element (e.g. a home router). The IPv6 address may be generated from the IPv4 address even if this is not directly available to the first network element. The term IPv6 address is intended to include addresses of subsequent versions of the Internet Protocol (e.g. an IPv6 address may be an address according to IP version 6 or later).

According to a feature of the invention, the gateway element is an IPv4 router and the first network element is a combined IPv4 and IPv6 network element. The first network element may be a dual stack device comprising both an IPv4 and IPv6 stack. The inventors have realised that in a network configuration wherein a combined IPv4 and IPv6 network element is coupled to an IPv4-only router, the public address of the IPv4-only router is not available to the combined IPv4 and IPv6 network element. Accordingly, the invention allows for auto-address configuration based on the IPv4 address of an IPv4 router even when that address is not directly available.

According to a feature of the invention, the first network element is a combined IPv4 and IPv6 router. Hence, the method provides an advantageous way for address auto-configuration for a combined IPv4 and IPv6 router.

According to another feature of the invention, the first network element is a combined IPv4 and IPv6 host. Hence, the method provides an advantageous way for address auto-configuration for a combined IPv4 and IPv6 host.

According to another feature of the invention, the step of generating the first address is substantially in accordance with the algorithm specified in RFC 3056, Connection

of IPv6 Domains via IPv4 Clouds, February 2001. Accordingly, the invention allows for the algorithm of IPv6 address auto-configuration specified in RFC 3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001 to be used even in network configurations wherein the public IPv4 address of the gateway element is not available.

According to another feature of the invention, the method further comprises the steps of: transmitting router solicitations in accordance with IPv6 standard RFC 2461; determining if a router advertisement in accordance with IPv6 standard RFC 2461 is received; and if a router advertisement is received, determining the first network address in accordance with IPv6 stateless address auto-configuration; and otherwise, determining if the first network element is connected to an IPv6 network node; and if so, determining the first network address in accordance with IPv6 stateful address auto-configuration; and otherwise, determining if the first network element is connected to an IPv4 network node; and if so, determining the first network address in accordance with a 6to4 address auto-configuration scheme as defined in RFC 3056; and otherwise, performing the steps of sending the address inquiry, receiving the address response message and generating the first address.

Accordingly, the address auto-configuration may determine the network topology, arrangement or configuration and configure the address using a suitable algorithm for the specific topology, arrangement or configuration. The method may provide a suitable algorithm for address auto-configuration in all possible network topologies, arrangements or configurations thus enabling a fully automatic address auto-configuration regardless of the network environment. Thus, fully automatic IPv6 address auto-configuration of IPv6 devices joining a home network may be provided thereby obviating the requirement for any manual intervention.

According to another feature of the invention, the second network element is part of the second network. Hence, the gateway may be retrieved from a network element external to the first network and address auto-configuration may thus be enabled even when the gateway address is not available in the first network.

According to another feature of the invention, the second network element is the gateway element. This provides for a simple method of address auto-configuration. The approach is particularly suited for implementations wherein the gateway element is a Universal Plug and Play (UPnP) gateway.

According to another feature of the invention, the second network is the Internet. Hence, the invention provides an advantageous method of address auto-configuration for devices of a home network connected to the Internet.

According to another feature of the invention, the second network element is associated with an Internet Service Provider (ISP). This provides for a suitable implementation wherein an ISP provides the gateway address.

According to another feature of the invention, the second network element is associated with a vendor portal associated with the first network element. This provides for a suitable implementation wherein a vendor may specifically guarantee the address auto-configuration functionality.

According to another feature of the invention, the second network element is associated with a third party host. This provides for a suitable implementation with high flexibility as any suitable third party host may be configured to provide the gateway address.

According to another feature of the invention, the step of generating the first address is further in response to identity information stored at the first network element. Specifically, the address may be generated in response to a public IPv4 address of the gateway element and a local built in identity code, such as a MAC (Media Access Control) address.

According to another feature of the invention, the gateway element has an associated second network address and an associated first network address, and the gateway address corresponds to the associated second network address. Specifically, the gateway element may have a public (e.g. IPv4) address known in the second network (e.g. the Internet) and a private (e.g. IPv4) address known in the first network (e.g. a home network).

According to a second aspect of the invention, there is provided a network element being part of a first network connected to a second network through a gateway element, the network element comprising: means for sending an address inquiry message to a second network element requesting an address of the gateway element; means for receiving an address response message from the second network element comprising a gateway address of the gateway element; and means for generating a first address of the first network element in response to the gateway address.

According to a third aspect of the invention, there is provided a communication network comprising at least one network element as described above.

According to a fourth aspect of the invention, there is provided a data communication protocol for network arrangement including a first network element being part of a first network connected to a second network through a gateway element, the data communication protocol comprising: an address inquiry message for sending from the first network element to a second network element requesting an address of the gateway element;

an address response message for receiving at the first network element from the second network element, the address response message comprising a data field for a gateway address of the gateway element; whereby a first address of the first network element may be generated in response to the gateway address.

These and other aspects, features and advantages of the invention will be apparent from and elucidated with reference to the embodiment(s) described hereinafter.

An embodiment of the invention will be described, by way of example only, with reference to the drawings, in which

FIG. 1 illustrates an example of a network configuration wherein a dual stack node is not coupled to an IPv6 router nor has IPv4 or IPv6 external connectivity;

FIG. 2 illustrates a communication network comprising a network element in accordance with an embodiment of the invention;

FIG. 3 illustrates the 6to4 address format: and

FIG. 4 illustrates a flowchart of a method of address auto-configuration in accordance with an embodiment of the invention.

The following description focuses on an embodiment of the invention applicable to a private home network coupled to the Internet. However, it will be appreciated that the invention is not limited to this application but may be applied to many other networks.

In the following description the following terminology has been applied for clarity and brevity:

A "node" denotes a device that implements either IPv4 or IPv6 or both in its network protocol stack.

A “router” denotes a node that forwards IP packets not explicitly addressed to itself.

A “gateway” denotes a node that includes additional functionality as compared with a router such as NA(P)T, DHCP server, etc.

A “host” denotes any node that is not a router or a gateway.

An “interface” denotes a node’s attachment to a link.

A “packet” denotes an IP header plus any payload.

The term "IPv4-only node" is used to refer to a host or a router that implements only IPv4 and does not understand IPv6.

The term "IPv6-only node" is used to refer to a host or a router that implements only IPv6 and does not understand IPv4.

The term "IPv6/IPv4 node" is used to refer to a host or a router that implements both IPv4 and IPv6.

The term "IPv4 node" is used to refers to a host or a router that implements IPv4. IPv6/IPv4 and IPv4-only nodes are both IPv4 nodes.

The term "IPv6 node" is used to refer to a host or a router that implements IPv6. IPv6/IPv4 and IPv6-only nodes are both IPv6 nodes.

The term "IPv4 packet" is used to refer to an IPv4 header plus payload.

The term "IPv6 packet" is used to refer to an IPv6 header plus payload.

An "IPv4 network" is used to refer to a network consisting exclusively of IPv4 nodes.

An "IPv6 network" is used to refer to a network consisting exclusively of IPv6 nodes.

An "IPv6/IPv4 network" is used to refer to a network consisting of both IPv4 and IPv6 nodes.

It is expected that Internet based networks will gradually migrate from IPv4 to IPv6 protocol based network elements. However, it is expected that due to the massive investment made in the existing IPv4 base, the convergence from IPv4 to IPv6 will probably take a decade or longer. Accordingly, the migration path from IPv4 to IPv6 will be long, implying that coexistence and interoperability will become very important for a long time. The latter is essential for gaining market acceptance and for protecting the huge investment made in the IPv4 infrastructure.

Presently, a home IP network is based only on IPv4. When introducing IPv6 devices to an IPv4 based home network several configurations may exist. Specifically, the following three different basic topologies may be identified with respect to introducing IPv6 devices to private home networks:

a. IPv6 devices may be introduced behind an IPv4-only home router.

b. IPv6 devices may be introduced behind an IPv6/IPv4 home router.

c. IPv6 devices may be introduced behind an IPv6-only home router.

The home router may thus be connected to the Internet using either the IPv4 protocol, or the IPv6 protocol, or both protocols.

If the home router is connected to the IPv4 Internet (also known as having IPv4 external connectivity), the home IP network has at least one valid, globally unique 32-bit IPv4 address. This address must be duly allocated to the home network by an address registry (e.g. via a DHCP server of an Internet Service Provider) and it must not be a private address. Hence, the home router is allocated a unique public 32-bit IPv4 address.

If the home router is connected to the IPv6 Internet (also known as having IPv6 external connectivity), the home IP network has at least one valid, globally unique IPv6 prefix (usually a 48-bit prefix). This prefix must be duly allocated to the home network by an address registry (e.g. via a DHCPv6 server of an Internet Service Provider).

If the home router is connected to the IPv6 and IPv4 Internet (also known as having IPv4 and IPv6 external connectivity), the home router has both a unique 32-bit IPv4 address and a globally unique (48-bit) IPv6 prefix.

As described in Section 5.5.1 of RFC 2462, when an IPv6 node joins a network it sends out Router Solicitations (RFC 2461, Neighbor discovery for IPv6, December 1998) in order to discover Router Advertisements. If the IPv6 node does receive a valid Router Advertisement (as defined in RFC 2461), this indicates that it is connected to a valid IPv6 router and it may therefore be configured as an IPv6 host. Further, the IPv6 router transmits information (such as the IPv6 prefixes) that allows the IPv6 host to perform IPv6 stateless address auto-configuration explained in RFC 2462. However, Router Advertisements may only be transmitted by IPv6 routers and not by IPv4 routers and accordingly this approach is only feasible if an IPv6 router already exists.

If the IPv6 node does not receive a valid Router Advertisement this indicates that the IPv6 node is not connected to an IPv6 router that can provide the required information for the stateless address auto-configuration. However, if the IPv6 node itself is connected to the IPv6 Internet (i.e. has IPv6 external connectivity) the IPv6 node may access a global DHCPv6 server whereby it may be assigned a unique IPv6 address. Thus, in this case the IPv6 node may perform an IPv6 address auto-configuration in accordance with the stateful address auto-configuration approach described in RFC draft-ietf-dhc-dhcpv6-28.txt, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), October 2002.

If the IPv6 node is not connected to an IPv6 router nor has external IPv6 connectivity, it cannot perform address auto-configuration in accordance with the stateful or the stateless address auto-configurations mentioned above. However, if the IPv6 node is a dual stack node, i.e. IPv6/IPv4, comprising both IPv6 and IPv4 stacks, its IPv6 address can be configure as explained below.

If the IPv6/IPv4 node has direct IPv4 external connectivity, i.e. it is itself a home router between the private home network and the IPv4 Internet, it may generate a special IPv6 address (called 6to4 address) from the unique IPv4 address it has been allocated.

As described in Section 2 of RFC 3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001, 6to4 addresses are applicable under the condition that a subscriber's home network has at least one valid, globally unique 32-bit IPv4 address. This address must be duly allocated to the home network by an address registry (possibly via an Internet Service Provider) and may not be a private address. The dual stack node having direct external IPv4 connectivity satisfies this condition and can therefore be configured according to the 6to4 scheme of RFC 3056.

However, in some network configurations, an IPv6/IPv4 host is located behind an IPv4-only router that provides only a private IPv4 address to the host. In this case, the IPv6/IPv4 host cannot configure its IPv6 address according to the 6to4 scheme. FIG. 1 illustrates an example of such network configuration wherein an IPv6/IPv4 node is not connected to an IPv6 router nor has direct IPv4 or IPv6 external connectivity.

FIG. 1 shows an example where a private home network is connected to the IPv4 Internet 103 through a gateway element in the form of an IPv4-only router 101. A private IPv4 network 105 is formed by the IPv4-only router 101 and a number of IPv4 devices 107. An IPv6/IPv4 network element 109 is connected to the IPv4-only router 101. The IPv6/IPv4 network node 109 functions as an IPv6 router 109 forming an IPv6 network 111 with a number of IPv6 hosts 113. In addition, another IPv6/IPv4 network node 115 is configured as an IPv6/IPv4 host and is connected to both the IPv4 network 105 and IPv6 network 111.

As can be seen from FIG. 1, the IPv6/IPv4 router 109 cannot auto-configure itself according to the stateless address auto-configuration as it is not connected to another IPv6 router. Nor can it perform the stateful address auto-configuration as it does not have external IPv6 connectivity. Furthermore, the IPv6/IPv4 router 109 has no knowledge of the public IPv4 address of the home network, it knows only private addresses and thus cannot perform address auto-configuration according to the 6to4 scheme.

Therefore, the IPv6 router 109 cannot perform address auto-configuration according to any of the prescribed address auto-configuration schemes. It should be noted that the same would apply to an IPv6/IPv4 host connected directly to the IPv4-only router 101. (In other words, if the example of FIG. 1 was modified by all IPv6/IPv4 hosts being

deleted and the IPv6/IPv4 router 109 being configured as an IPv6 host, the situation with respect to address auto-configuration would remain the same).

FIG. 2 illustrates a communication network comprising a network element in accordance with an embodiment of the invention. A first network element 201 belongs to a first network 203. Specifically, the first network 203 may be a private home network and the first network element 201 may be the IPv6/IPv4 router 109 of FIG.1. The first network is connected to a second network 207 comprising a second network element 205 through a gateway element 209. Specifically, the second network 207 may be the Internet 103 and the gateway element 209 may be the IPv4-only router 101 of FIG. 1.

In accordance with an embodiment of the invention, address auto-configuration may be performed by the first network element 201 in the following way. Initially, the first network element 201 may transmit an address inquiry message to the second network element 205. The address inquiry message requests information related to the address of the gateway element 209 in the second network 207. The second network element 205 is part of the second network 207 and therefore knows the address of the gateway element 209 in the second network. In contrast, the first network element 201 is only aware of the address of the gateway element 209 in the first network 203. In relation to the example of FIG. 1, the second network element 205 uses (and thus knows) the public unique IPv4 address of the gateway element 209 whereas the first network element 201 only knows the private IPv4 address.

In response to receiving the address inquiry message, the second network element 205 creates an address response message comprising the address of the gateway element 209 in the second network. This message is transmitted to the first network element 201.

The first network element 201 receives the address response message from the second network element 205 and generates a first address of the first network element 201 in response to the gateway address. In the specific example, the first network element 201 receives the public IPv4 address of the gateway element, and thus of the private home network, from the second network element 205. It may accordingly determine an IPv6 address in accordance with the 6to4 scheme for address auto-configuration.

Hence, in accordance with the embodiment, an address of the gateway element between two communication networks may be used to determine an address of a device of a network element of one of the networks even when this address is not directly available.

An embodiment of the invention specifically aimed at introducing IPv6 network elements in an IPv4 based private home network will be described in more detail. The embodiment will be described with specific reference to FIG. 1.

As mentioned previously, the IPv6 router 109 cannot directly follow the 6to4 procedure for IPv6 prefix allocation as described in RFC 3056. The reason is that it does not know the public IPv4 address of the home network, which the ISP has assigned to the IPv4-only router 101. The IPv6 router 109 has only knowledge of private addresses. However, the public IPv4 address of the IPv4-only router 101 is available to all communication parties located in the external network (the Internet 103) including the IPv4-only router 101.

In accordance with the embodiment, a new protocol is executed between the IPv6 router 109 and a party aware of the public IPv4 address of the private home network where the IPv6 router 109 is located.

In the embodiment, the IPv6 router 109 will get the public IPv4 address of its (home) network as a result of executing the new protocol with a second network having information of the public address of the home network. Once the IPv6 router 109 has received the public IPv4 address, it can construct itself the IPv6 prefix required by the 6to4 scheme. Further, it can construct its IPv6 global address based on the prefix plus the information that is locally available, such as the built in MAC address

In the following, a detailed example is described of how an IPv6/IPv4 device, such as the IPv6 router 109, may operate in accordance with the preferred embodiment of the invention.

In the example, it is assumed that a user has a single subscription with an ISP delivering a unique public IPv4 address, e.g. 130.145.174.7, to the user's IPv4-only router 101. When the IPv6/IPv4 device (e.g. the IPv6 router 109) boots on the home network it preferably performs the following steps:

The IPv6/IPv4 device receives an IPv4 private address, for example 192.168.0.4. This is obtained in a stateful manner e.g. via the DHCP server running on the IPv4-only router 101.

Using the IPv4 private address 192.168.0.4 and the NA(P)T functionality of the IPv4-only router 101, the IPv6/IPv4 Internet device contacts a second network element which is located in the Internet 103. The new address inquiry and response protocol is executed. As a result the IPv6/IPv4 device receives information of the public IPv4 address of the home network, i.e. 130.145.174.7.

Having the public IPv4 address of the home network, the IPv6/IPv4 device constructs the IPv6 prefix and its global IPv6 address according to the 6to4 scheme defined in RFC 3056. The 6to4 address format is illustrated in FIG. 3. The low-order 80-bits contain information locally available to an IPv6 node, such as a SLA ID (Site Level Aggregation Identifier) and an Interface ID. The latter is usually the same as the MAC address of the IPv6 node which is built in during manufacture. The high-order 48-bits are known as a 6to4 prefix. The IANA (Internet Assigned Numbers Authority) has permanently assigned one 13-bit TLA (Top Level Aggregation) identifier under the FP 001 (Format Prefix) to the 6to4 scheme. Its numeric value is 0x0002, i.e., it is 2002::/16 when expressed as an IPv6 address prefix. The 32-bit NLA (Next Level Aggregation) identifier is reserved for colon-hexadecimal representation of the globally unique public IPv4 address of the subscriber's network. The 6to4 prefix, which corresponds to the public IPv4 address 130.145.174.7, is 2002:8291:ae07::/48.

The IPv6/IPv4 device advertises its IPv6 global address to an IPv6-enabled DNS server in accordance with RFC 1886, DNS Extensions to support IP version 6, December 1995, by securely sending a dynamic DNS update messages in accordance with RFC 3007, Secure Domain Name System (DNS) Dynamic Update, November 2000. The IPv6 address is globally unique, therefore the IPv6/IPv4 Internet device can be uniquely and individually addressed using the IPv6 address.

Having configured both an IPv4 and an IPv6 address, the IPv6/IPv4 device can automatically adapt to the version of the Internet Protocol (either IPv4 or IPv6) used by the corresponding communication peer. Accordingly the IPv6/IPv4 Internet device is fully adaptive to the network configuration. In particular, when a Content Provider wants to deliver a particular service to the IPv6/IPv4 device, it will send a DNS request to a DNS server to find the IPv6 address of that particular device. After receiving it, all traffic directed to the IPv6/IPv4 device will be tunnelled over the IPv4 Internet infrastructure and the IPv6 packages can be encapsulated into IPv4 packages as is known to the person skilled in the art.

When a user buys a second IPv6 device, the first IPv6/IPv4 device will become an IPv6/IPv4 router, and more specifically a 6to4 router. It will advertise the 6to4 prefix on the local link. This may happen transparently to the user since the router capabilities are automatically integrated into the IPv6/IPv4 device. Therefore, the second and following IPv6 devices may be configured as IPv6 hosts following the IPv6 stateless address auto-configuration introduced in RFC 2462.

If there is a second IPv6/IPv4 device in the home network and the first IPv6/IPv4 device functioning as a router becomes unavailable (e.g. due to failure), the second IPv6/IPv4 device can take over the routing functionality. Thus, reliability and down time can be improved.

In different embodiments, different functional modules or network devices may be used as the second network element.

In the preferred embodiment, the second network element is part of the second network. For example, it may be an Internet service or Internet node or network device.

Specifically, the second network element may be the gateway element itself. For example, the IPv4-only router 101 of FIG. 1 may itself provide the public IPv4 address to the IPv6 router 109. Specifically, if the IPv4-only router 101 is a UPnP Gateway, this will facilitate the implementation.

However, many of the IPv4 home routers that are currently deployed are not UPnP compliant yet. Therefore, in some embodiments, vendors may provide a service for IPv6 address auto-configuration of their IPv6/IPv4 devices. Thus the second network element may be a vendor portal associated with the first network element. For example, the manufacturer of the IPv6/IPv4 devices may provide a portal supporting the new protocol and may provide functionality for delivering the public IPv4 address in accordance with this protocol. In this case, the implementation of the protocol may be vendor specific.

Alternatively or additionally, the implementation of the new protocol may be standardized allowing for e.g. an ISP or a 3rd party to provide the functionality of the second network element. In this case, all IPv6/IPv4 devices, independently of their vendors, may carry out the standardized protocol either with the ISP that holds the subscription of the private home network or with a 3rd party that is aware of the protocol

The new address inquiry and response protocol may run on top of the TCP/IP (IPv4) protocol, and specifically the HTTP protocol may be used. An HTTP client may run on the IPv6/IPv4 Internet device while an HTTP server may be incorporated in the second network element. The HTTP client can make a specific HTTP GET request to get a Perl script from the HTTP server. The script may use the environment variable $ENV{REMOTE_ADDR} provided by the HTTP server to determine the public IPv4 address of the network where the remote HTTP client is located, i.e. the IPv6/IPv4 Internet device. The HTTP server returns this public IPv4 address (in plain text) as response to the GET request of the HTTP client.

In another embodiment where e.g. an existing 3rd party HTTP server, such as http://showmyip.com, is used, the IPv4 address is embedded in a HTML file rather than as a plain text. This may require some additional parsing by the client device.

Preferably, the first network element operates a full address auto-configuration algorithm wherein the topology, configuration or arrangement of the network is determined and the appropriate address auto-configuration method is used.

FIG. 4 illustrates a flowchart of a method of address auto-configuration in accordance with an embodiment of the invention.

In step 401, the first network element transmits router solicitations in accordance with IPv6 standard RFC 2461. Thus, upon boot, an IPv6 device first sends out Router Solicitations as described in RFC 2461 in order to discover Router Advertisements.

In step 403 it is determined if a router advertisement in accordance with IPv6 standard RFC 2461 is received.

If so, the first network element is connecetd to an IPv6 router and the method proceeds in step 405 by determining the first network address in accordance with IPv6 stateless address auto-configuration as defined in RFC 2462.

Otherwise, the method proceeds in step 407 by determining if the first network element is connected directly to the IPv6 Internet network node. Thus, it is determined if the first network element has external IPv6 connectivity.

If so, the method proceeds in step 409 where the first network address is determined in accordance with IPv6 stateful address auto-configuration as described in DHCPv6.

Otherwise, the method proceeds in step 411 wherein it is determined if the first network element is connected directly to an IPv4 network node. Thus it is determined if the first network element has external IPv4 connectivity.

If so, the first network element has information of the public IPv4 address and thus the method proceeds in step 413 where the first network address is determined in accordance with the 6to4 scheme described in RFC 3056.

Otherwise, the first network element does not have the information related to the public IPv4 address. Accordingly, it proceeds in step 415 to send an address inquiry message to a second network element requesting an address of the gateway element and subsequently to receive an address response message from the second network element comprising a gateway address of the gateway element. The gateway address is specifically the public IPv4 address of the private home network, and the first network element 201

proceeds to determine the first network address in accordance with the 6to4 scheme described in RFC 3056 using the received gateway address.

Thus, a completely automated process for address auto-configuration which automatically adapts to the network configuration is provided in accordance with this embodiment. The algorithm proposed is fully autonomous and an IPv6 node executing the algorithm will, provided that it has either IPv4 or IPv6 connectivity or both, end up with a configured IPv6 interface independently of the topology in which the IPv6 node is situated.

The invention can be implemented in any suitable form including hardware, software, firmware or any combination of these. However, preferably, the invention is at least partially implemented as computer software running on one or more data processors and/or digital signal processors. The elements and components of an embodiment of the invention may be physically, functionally and logically implemented in any suitable way. Indeed the functionality may be implemented in a single unit, in a plurality of units or as part of other functional units. As such, the invention may be implemented in a single unit or may be physically and functionally distributed between different units and processors.

Although the present invention has been described in connection with the preferred embodiment, it is not intended to be limited to the specific form set forth herein. Rather, the scope of the present invention is limited only by the accompanying claims. In the claims, the term comprising does not exclude the presence of other elements or steps. Furthermore, although individually listed, a plurality of means, elements or method steps may be implemented by e.g. a single unit or processor. Additionally, although individual features may be included in different claims, these may possibly be advantageously combined, and the inclusion in different claims does not imply that a combination of features is no feasible and/or advantageous. In addition, singular references do not exclude a plurality. Thus, references to "a", "an", "first", "second" etc do not preclude a plurality.

CLAIMS:

1. A method of address auto-configuration for a first network element (201) being part of a first network (203) connected to a second network (207) through a gateway element (209), the method comprising the steps of:

sending an address inquiry message to a second network element (205) requesting an address of the gateway element (209);

receiving an address response message from the second network element (205) comprising a gateway address of the gateway element (209); and generating a first address of the first network element (201) in response to the gateway address.

2. A method as claimed in claim 1 wherein the first address is in accordance with a different address protocol than the gateway address.

3. A method as claimed in claim 2 wherein the first address is an Internet Protocol version 6 (IPv6) address and the gateway address is an Internet Protocol version 4 (IPv4) address.

4. A method as claimed in claim 3 wherein the gateway element (209) is an IPv4 router and the first network element (201) is a combined IPv4 and IPv6 network element.

5. A method as claimed in claim 4 wherein the first network element (201) is a combined IPv4 and IPv6 router.

6 A method as claimed in claim 4 wherein the first network element (201) is a combined IPv4 and IPv6 host.

7. A method as claimed in claim 4 wherein the step of generating the first address is substantially in accordance with the algorithm specified in RFC (Request for Comments) 3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001.

8. A method as claimed in claim 4 wherein the method further comprises the steps of:

transmitting router solicitations in accordance with RFC 2461;

determining if a router advertisement in accordance with RFC 2461 is received; and

if a router advertisement is received, determining the first network address in accordance with IPv6 stateless address auto-configuration; and

otherwise, determining if the first network element (201) is connected to an IPv6 network node; and

if so, determining the first network address in accordance with IPv6 stateful address auto-configuration; and

otherwise, determining if the first network element (201) is connected to an IPv4 network node; and

if so, determining the first network address in accordance with a 6to4 address auto-configuration scheme as defined in RFC 3056; and

otherwise, performing the steps of sending the address inquiry, receiving the address response message and generating the first address.

9. A method as claimed in claim 1 wherein the second network element (205) is part of the second network (207).

10. A method as claimed in claim 1 wherein the second network element (205) is the gateway element (209).

11. A method as claimed in claim 1 wherein the second network (207) is the Internet.

12. A method as claimed in claim 11 wherein the second network element (205) is associated with an Internet Service Provider (ISP).

13. A method as claimed in claim 11 wherein the second network element (205) is associated with a vendor portal associated with the first network element (201).

14. A method as claimed in claim 11 wherein the second network element (205) is associated with a third party host.

15. A method as claimed in claim 1 wherein the step of generating the first address is further in response to identity information stored at the first network element (201).

16. A method as claimed in claim 1 wherein the gateway element (209) has an associated second network address and an associated first network address, and wherein the gateway address corresponds to the associated second network address.

17. A method as claimed in claim 15 wherein the first network address is not available to the first network element (201).

18. A computer program enabling the carrying out of a method according to claim 1.

19. A record carrier comprising a computer program as claimed in claim 18.

20. A network element (201) being part of a first network (203) connected to a second network (207) through a gateway element (209), the network element (201) comprising:

means for sending an address inquiry message to a second network element (205) requesting an address of the gateway element (209);

means for receiving an address response message from the second network element (205) comprising a gateway address of the gateway element (209); and

means for generating a first address of the network element (201) in response to the gateway address.

21. A communication network comprising at least one network element in accordance with claim 20.

22. A data communication protocol for network arrangement including a first network element (201) being part of a first network (203) connected to a second network (207) through a gateway element (209), the data communication protocol comprising:

an address inquiry message for sending from the first network element (201) to a second network element (205) requesting an address of the gateway element (209);

an address response message for receiving at the first network element (201) from the second network element (205), the address response message comprising a data field for a gateway address of the gateway element (209);

whereby a first address of the first network element (201) may be generated in response to the gateway address.

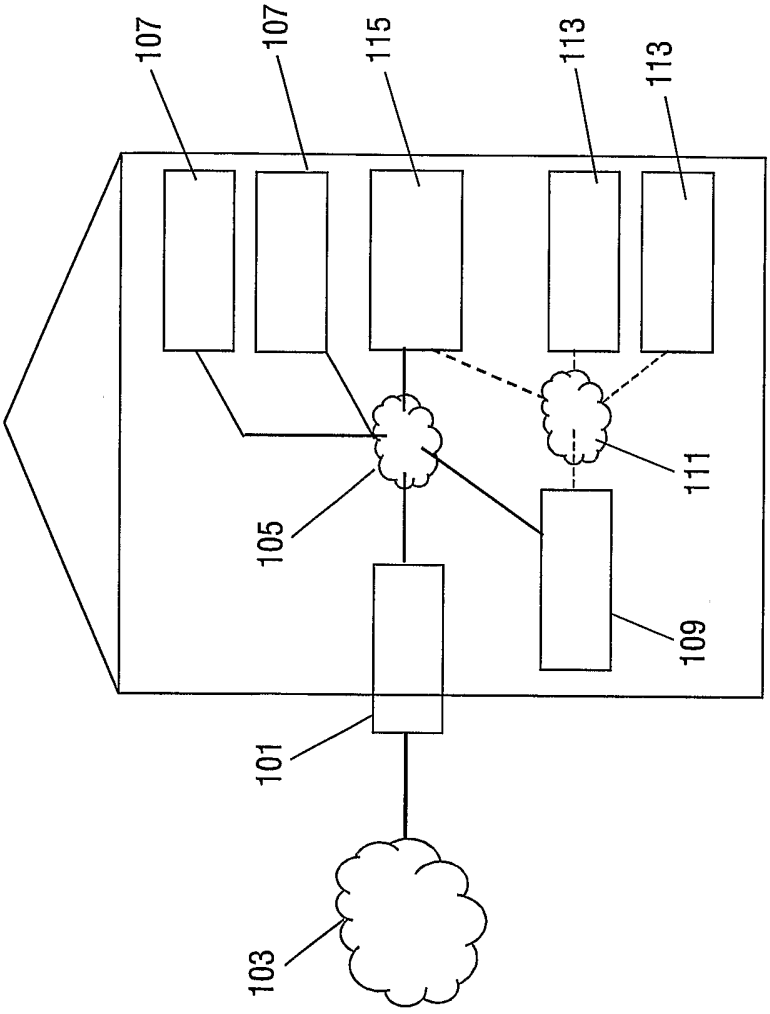



FIG.1

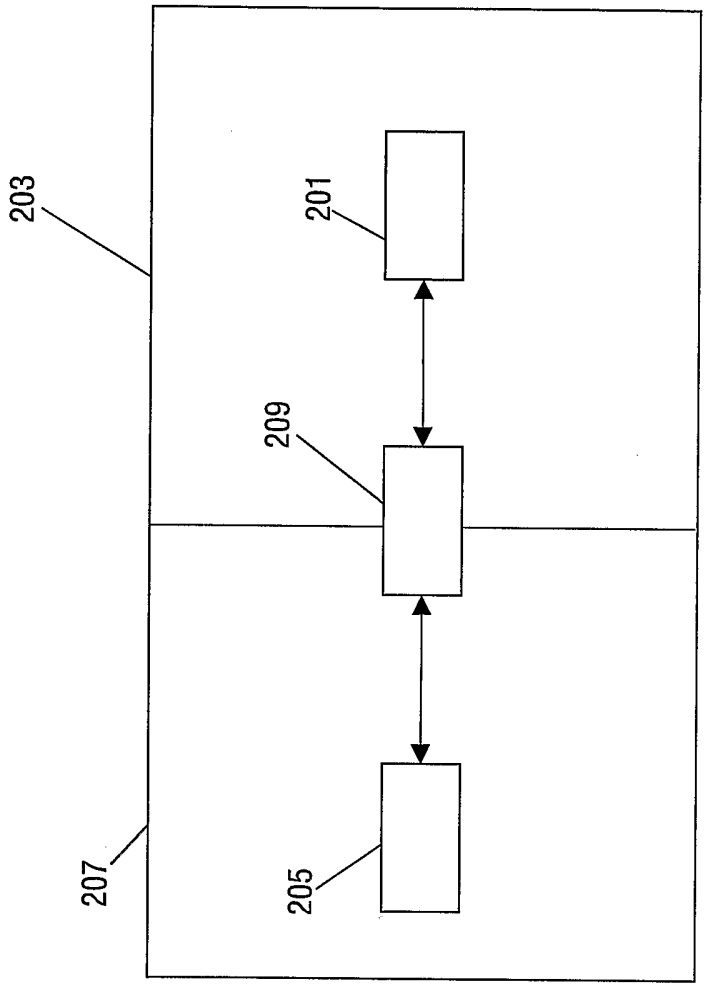
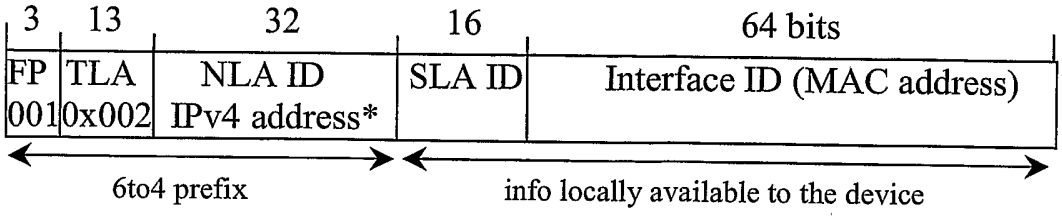



FIG.2




*- in a colon-hexadecimal representation

FIG.3

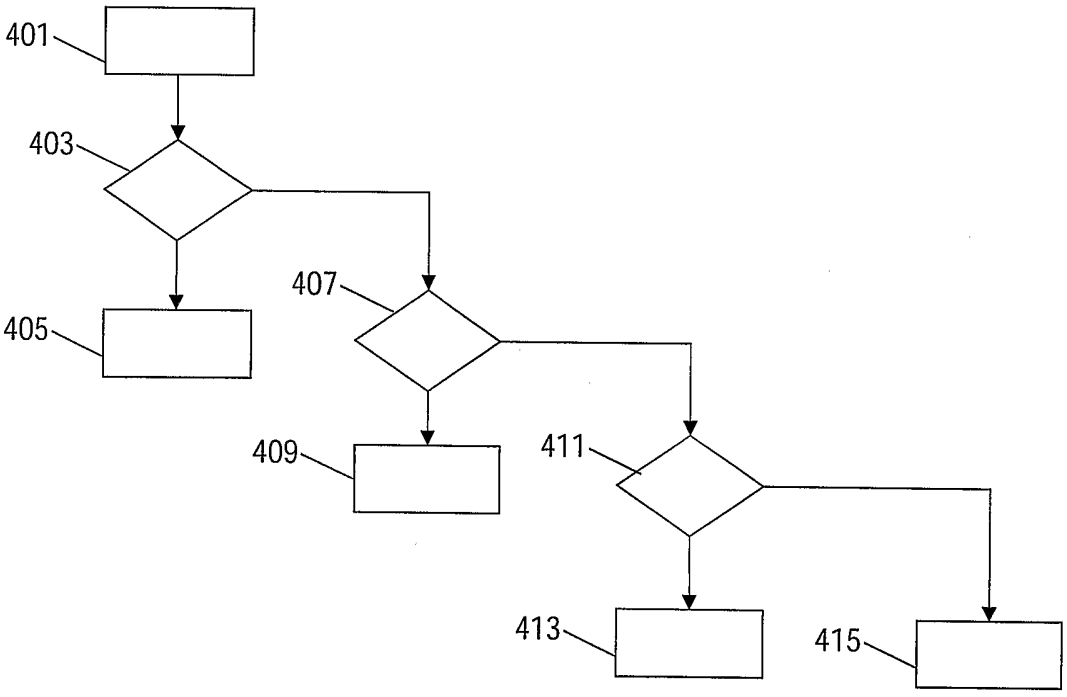



FIG.4

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050578

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12

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)
IPC 7 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 practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | C. HUITEMA: "Teredo: Tunneling IPv6 over UDP through NATs" DRAFT-HUITEMA-V6OPS-TEREDO-00.TXT, 17 September 2002 (2002-09-17), pages 1-54, XP015002876 | 1-9, 11-22 |
| Y | page 1, paragraph 1<br>page 9, paragraph 4.1.1<br>page 10, paragraph 4.1.2<br>page 21, paragraph 5.1 | 10 |
| Y | M. BORELLA, J. LO, D. GRABELSKY, G. MONTENEGRO: "Realm Specific IP: Framework" IETF RFC 3102, October 2001 (2001-10), XP015008883 GENEVA, SWITZERLAND<br>page 2, paragraph 1 -page 3<br>page 6, paragraph 2 -page 7 | 10 |

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in 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 document 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 | Date of mailing of the international search report |
|---|---|
| 11 August 2004 | 30/08/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Peeters, D |

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050578

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JORDI PALET ET AL: "IPv6 Tunnels through Routers with NAT" EUROGIX CONSORTIUM, 'Online! 10 April 2003 (2003-04-10), pages 1-8, XP002291967 Retrieved from the Internet: <URL:http://www.euro6ix.org/documentation/euro6ix_co_upm-consulintel_wp4_ipv6_tunnels_nat_v1_6.pdf> 'retrieved on 2004-08-10! page 3, paragraph 1 ----- | 1-22 |