Communication device having VPN accommodation function

Kommunikationsgerät mit VPN-Ermöglichungsfunktion

Dispositif de communication comprenant une fonction d’amenagement VPN

Designated Contracting States:
DE FR GB

Date of publication and mention of the grant of the patent:
18.02.2015 Bulletin 2015/08

Application number: 10185985.8

Date of filing: 16.06.2000

References cited:

• TSIRTSIS BT P SRISURESH CAMPIO
COMMUNICATIONS G: "Network Address Translation - Protocol Translation (NAT-PT);
rfc2766.txt", IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, 1
February 2000 (2000-02-01), XP015008549, ISSN: 0000-0003

• HINDEN R M: "IP NEXT GENERATION
OVERVIEW", COMMUNICATIONS OF THE
ASSOCIATION FOR COMPUTING MACHINERY,
ASSOCIATION FOR COMPUTING MACHINERY.
NEW YORK, US, vol. 39, no. 6, 1 June 1996
(1996-06-01), pages 61-71, XP000641615, ISSN:
0001-0782

• LEE D C ET AL: "THE NEXT GENERATION OF
THE INTERNET: ASPECTS OF THE INTERNET
PROTOCOL VERSION 6", IEEE NETWORK, IEEE
28-33, XP000739805, ISSN: 0890-8044

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).
Description

FIELD OF THE INVENTION

[0001] The present invention relates to a communication device having a VPN (virtual private network) accommodation function for use in the Internet.

BACKGROUND OF THE INVENTION

[0002] The Internet is a network enabling worldwide interconnection among users, the number of which is proliferating. In recent years, a variety of techniques have been developed actively to implement a VPN using the Internet.

[0003] The VPN, or virtual private network, is a service connecting throughout the Internet. An example of a network configuration providing VPN is shown in FIG. 1. In this FIG. 1, a variety of network organizations including A - C are connected through routers 20 - 25 to a network 1 which is managed by a service provider. These routers are referred to as VPN edge routers.

[0004] Network 1 provided by the service provider generally interconnects with other networks provided by other service providers. As a VPN, a network for an organization A, as an example, is exclusively interconnected within this organization A only, separated from organizations B and C, through network 1 by the service provider. In other words, only each network inside organization A, B or C is logically interconnected.

[0005] Here, either a global address or a private address is used in an intranet whereas a global address is normally used in the Internet. The private address is an address to be applied in a network which is closed in the scope of an organization, and therefore an identical address may possibly be used in different organizations.

[0006] Accordingly, in a device accommodating VPN, it becomes necessary to provide the packet routing function for both Internet and intranet. Normally, in the direction from intranet to Internet, any packet for communication in an intranet is converted to a packet which can be processed in the Internet. In the direction from Internet to intranet, the packet format is converted in an opposite way to the above.

[0007] In the prior arts for performing such processing, as a first art, there is a method of either combining an IPv4 (Internet Protocol, version 4) header, the format of which includes a source address 26 and a destination address 27 shown in FIG. 2, with another IPv4 header, or combining with an IPv6 (Internet Protocol, version 6) header, the format of which includes a source address 28 and a destination address 29 shown in FIG. 3. Thus the headers are encapsulated as shown in FIGS. 4A and 4B, respectively (corresponding to the Internet standard recommendation document, RFC 1853). Further, as a second prior art, there is a method of employing an MPLS (MultiProtocol Label Switching) shim header shown in FIG. 5 to encapsulate both an IPv4 header and a shim header, as shown in FIG. 4C.

[0008] Both of the aforementioned prior arts employ a method of establishing a packet path on the boundary between the Internet and the intranet (which is referred to as tunnel).

[0009] More specifically, the encapsulation technique shown in FIG. 4C using an MPLS header shown in FIG. 5, the tunneling between both sides of the boundary is enabled by setting a unique value in a label field (Label) of the shim header on a link-by-link basis, and setting a virtual path by converting this value included in the label field in the device connecting the links.

[0010] Meanwhile, according to the encapsulation method by a shim header shown in FIG. 4C using a MPLS header shown in FIG. 5, the tunneling between both sides of the boundary is enabled by setting a unique value in a label field (Label) of the shim header on a link-by-link basis, and setting a virtual path by converting this value included in the label field in the device connecting the links.

[0011] However, according to the aforementioned prior arts, the number of settings in the device incorporating VPN becomes the number of tunnels x 2 (i.e., both end points of the tunnels). Therefore, there is a problem that a substantially large number of settings become necessary as the number of sites increases.

[0012] The number of the tunnels among N sites is (N - 1) x 2 in the case of a star connection network in which the number of tunnels is minimized. The number becomes N x (N - 1) in case of a full mesh connection. If one site is added, it is necessary to add two (2) settings in the case of star connection, or N settings in case of the full mesh connection.

[0013] In case of the star connection, the performance of a root node may cause a bottleneck. In addition, because a communication between nodes other than root has to be transmitted through the root, an identical packet has to be transmitted twice in the Internet. This raises a problem of additional bandwidth consumption, so use of full mesh connection is desirable.

[0014] EP 0 840 482 A1 discloses that in an apparatus, there is provided an IP transmitting and receiving unit for transmitting and receiving an IPv4 packet and an IPv6 packet; an IP header converting unit for performing a mutual conversion of the IPv4 packet and the IPv6 packet by an IP header conversion; a DNS substituting unit for receiving a domain information capturing request sent from an IPv4 terminal or an IPv6 terminal and substituting its process; an IPv4 address capturing unit for capturing an IPv4 address from a DHCP server; and an IP address conversion information holding unit for holding an IPv6 address of the IPv6 terminal and the IPv4 address captured by the IPv4 address capturing unit in correspondence to each other. Thus, a communication with the IPv4 terminal can be executed without preliminary fixedly allocating the IPv4 address to the IPv6 terminal.

[0015] US, 6,038,233 A discloses a translator for coupling a first network such as an internet protocol version 4 (IPv4) and a second network such as an internet protocol version 6 (IPv6) having different addressing architectures for IP addresses due to a difference in version...
or the like so as not to exhaust the IP addresses of one of the two networks, a network system using the translator, and a network coupling method therefore are provided. When a packet is transferred from the IPv6 network to the IPv4 network, the translator assigns any of a plurality of previously prepared IPv4 addresses to an IPv6 address stored in a source storing field of the IPv6 packet. The assigned address is stored in a source storing field of an IPv4 packet. A packet translation unit is provided for assigning the foregoing IPv6 address to an IPv4 address stored in a destination storing field of the IPv4 packet, when a packet is transferred from the IPv4 network to the IPv6 network, and for storing this address in a destination storing field of the IPv6 packet.

SUMMARY OF THE INVENTION

According to a first aspect of the invention there is provided a method as set out in Claim 1.

According to a second aspect of the invention there is provided an apparatus as set out in Claim 2.

Further scopes and features of the present invention will become more apparent by the following description of the embodiments with the accompanied drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows an example of network configuration diagram constituting a virtual private network (VPN).

FIG. 2 shows an explanation drawing of an IPv4 header.

FIG. 3 shows an explanation drawing of an IPv6 header.

FIG. 4 shows a drawing illustrating header encapsulation.

FIG. 5 shows a diagram illustrating an MPLS shim header.

FIG. 6 shows a drawing illustrating the configuration concept of the present invention.

FIG. 7 shows a diagram illustrating the definition of VPN address.

FIG. 8 shows a typical embodiment of the present invention.

FIG. 9 shows an example of configuration of a VPN accommodation function portion shown in FIG. 8, illustrating an example of converting an IPv4 header into an IPv6 header.

FIG. 10 shows another exemplary configuration of the VPN accommodation function portion shown in FIG. 8 in the example of converting an IPv4 header into an IPv6 header.

FIG. 11 shows a diagram illustrating an IPv6 address generated in the exemplary configurations shown in FIGS. 8, 9.

FIG. 12 shows an example of configuration of the VPN accommodation function portion shown in FIG. 8, illustrating an example of encapsulating an IPv4 packet with an IPv6 header.

FIG. 13 shows another example of configuration of the VPN accommodation function portion shown in FIG. 8 in an example of encapsulating an IPv4 packet with an IPv6 header.

FIG. 14 shows an example or configuration of a VPN accommodation function portion shown in FIG. 8, illustrating an example of employing IPv6 in the intranet.

FIG. 15 shows another example of configuration of the VPN accommodation function portion shown in FIG. 8 in an example of employing IPv6 in the intranet.

FIG. 16 shows a diagram illustrating a VPN address corresponding to the configurations shown in FIGS. 14, 15.

FIG. 17 shows a diagram illustrating an address used in a site-local address format.

FIG. 18 shows an example of an aggregatable global address.

FIG. 19 shows a diagram illustrating an example of a VAN address having a scope as an application example of the present invention.

FIG. 20 shows a diagram illustrating an example of a VPN address employing an IPv4 global address, as an application example of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiment of the present invention is described hereinafter referring to the charts and drawings, wherein like numerals or symbols refer to like parts. It is to be noted that these charts and drawings illustrating the embodiments are attached for explaining the present invention.

The scope of the protection in the present invention is not to be limited to these illustrations.

FIG. 6 is a drawing illustrating the configuration concept of the present invention. In FIG. 6, a VPN accommodation function portion 32 is provided between an internee router function portion 30 and a VPN router function portion 31.

This VPN accommodation function portion 32 has a function of either converting a header of a packet for transmission into a header having a VPN address format, or encapsulating by including a header of the VPN address format. VPN accommodation function portion 32 also has a function of converting a packet to an identical format of an original packet or deleting a header having the VPN address format on receiving a packet having the VPN address format.

A VPN address format shown in FIG. 7 is defined. A header conforming to the address format is generated by adding an ID for identifying a VPN, i.e. a VPN number 34 to an IP address 33 for use in an intranet.
VPN number 34 is a number uniquely assigned in a certain region. This region may be the whole region of the Internet or a region of an Internet service provider (ISP). The address in the structure described herein is distinguished from an address of other type by an FP (Format prefix) 35.

According to the scheme described herein, when compared to the case of a full mesh network producing better efficiency, the number of settings required for performing VPN can be reduced to N in contrast to N x (N - 1) in the prior art. For the reference, the number required for a star connection in the prior art is (N - 1) x 2. Namely, a full mesh network can be obtained with the number of settings smaller than in the case of star connection in the prior art.

Also, in the case of adding a site in a full mesh network, only one setting is needed in the embodiment, in contrast to N settings required in the prior art.

In regard to processing for performing normal routing in the Internet, path establishment on a link-by-link basis is necessary in the method employing MPLS shim header. In contrast, in an embodiment of the present invention, it is only necessary for route switching to use an existing protocol like RIP (Routing Information Protocol) widely in use having abundant operational results, as well as OSPF (Open Shortest Path First), IS-IS (Intermediate System - Intermediate System) or BGP (Border gateway Protocol), which are modified so as to conform to the Internet protocol IPv6.

Therefore, such a protocol as employed in MPLS which requires to set label value is not needed. Here, by combining the technique of encapsulating an IPv6 packet with an IPv4 header, it becomes not necessary that all network device of service provider conform to IPv6.

Now, a typical embodiment of the present invention is described hereafter referring to the example shown in FIG. 8, in which an IPv4 address (either global address or private address) is used in the intranet, and an IPv6 address is used in the Internet.

In the example shown in this FIG. 8, a router function portion (on Internet side) 30, a router function portion (on VPN side) 31 and a VPN accommodation function portion 32 are provided as a VPN edge router 20. A router 300 is a router function portion for connecting between VPN edge routers 20.

VPN router function portion 31 has a routing table 501, while router function portion 30 and router 300 have routing cables 502 and 503, respectively. A destination address and a source address are described in an IPv4 packet header referring to these routing tables.

When packet communication is carried out from one site in a VPN to another site in the VPN, an IPv4 packet for use in the originating site is transmitted to VPN accommodation function portion 32 in VPN edge router 20.

In VPN accommodation function portion 32, IP addresses (both source address and destination address) included in the IPv4 packet are extracted in an IPv4 address extraction portion 320.

Using a VPN-ID (number) being set in a VPN-ID retention portion 321 in advance for identifying the VPN of interest, a VPN address in the form of IPv6 for the Internet is generated by combining a VPN-ID 40 with an IPv4 address 41 in a VPN address generation portion 322, as shown in FIG. 11.

The IPv6 VPN address thus generated is used for an IPv6 header address to be added in an IPv6 header addition portion 324 after an IPv4 header is deleted in an IPv4 header deletion portion 323, as shown in FIG. 9. Thus the IPv4 header is converted into an IPv6 header.

The IPv6 packet thus converted is transferred to VPN accommodation function portion 32 in VPN edge router 20 to which the destination site is connected through the Internet 1. This VPN accommodation function portion 32 is explained also referring to FIG. 9. In FIG. 9, an IPv6 packet is input to an IPv6 packet address extraction portion 325.

The IPv6 address extracted in IPv4 address extraction portion 325 is input to VPN-ID/IPv4 address separation portion 326 to separate the IPv4 address. The separated IPv4 address is then used as an address in the IPv4 header to be added in IPv4 header addition portion 328 to a packet of which IPv6 header is deleted in an IPv6 header deletion portion 327. Thus the packet concerned is returned to an IPv4 packet.

FIG. 6B shows an aspect of header conversion between intranet and the Internet corresponding to the aforementioned description referring to FIG. 9.

In the above description, it may also be possible to check whether the VPN-ID of the packet input to VPN accommodation function portion 32 coincides with a predetermined VPN-ID. In such a case, VPN accommodation function portion 32 is configured as shown in FIG. 10. Namely, a comparison circuit 329 is additionally provided compared to the configuration shown in FIG. 9.

Using this comparison circuit 329, a predetermined VPN number corresponding to the VPN of interest retained in VPN-ID retention portion 321 is compared to the VPN-ID separated in VPN-ID/IPv4 address separation portion 326.

As the result of this comparison, if the VPN numbers are different, the packet is discarded in an IPv4 header addition portion because the packet has no relation with the VPN of interest. This enables to prevent any packet from flowing in or flowing out from/to a different VPN, thus enabling to improve security.

Further, as a result of VPN accommodation function portion 32 outputting a route including up to an IPv4 prefix shown in FIG. 11, routing by IPv6 is carried out according to routing table 502 shown in FIG. 8.

In the above description, a case of converting an IPv4 header into an IPv6 header is shown. However,
In such a case, the configurations of VPN accommodation function portion 32 shown in FIGS. 9, 10 are replaced by the configurations shown in FIGS. 12, 13, respectively. In the configurations shown in FIGS. 12, 13, IPv4 header deletion portion 323 and IPv4 header addition portion 328 become unnecessary.

Namely, an IPv6 VPN address generated in VPN address generation portion 322 is added to an IPv44 packet in IPv46 header addition portion 324 to encapsulate. Therefore, IPv4 header deletion portion 323 is not required in FIGS. 12, 13.

Also, in FIGS. 12, 13, the IPv6 address included in a signal input from the Internet is extracted in IPv6 address extraction portion 325, while the IPv4 address remains unchanged. Therefore, IPv4 address addition portion 328 is not required also.

This situation is shown in FIG. 6C, taking the header conversion shown in FIG. 4A as an example.

The foregoing description is based on the intranet employing IPv4. When IPv6 is employed in the intranet, a similar operation can be achieved by handling an IPv4 address a subnet ID, or a data under a site prefix, included in a site-local address (i.e. a local address not connected to the Internet).

FIGS. 14, 15 show examples of configuration block diagram of VPN accommodation function portion 32 when IPv6 is used in the intranet, which respectively correspond to FIGS. 9, 10. As shown in FIGS. 14, 15, IPv6 address extraction portions 330, 332 and address substitution portions 331, 333 are provided for handling IPv6 addresses.

FIG. 16 shows an explanation drawing of a VPN address corresponding to the configurations shown in FIGS. 14, 15. In these FIGS. 14, 15, a VPN address is generated by the address conversion using a VPN-ID 40 shown in this FIG. 16, a subnet ID/SLA 42 in the site-local address format or the aggregatable global address format and an Interface ID field 43 in an IP header address used in an organization or among organizations.

This address conversion is performed in address substitution portion 331 shown in FIGS. 14, 15.

Here, an exemplary address in the site-local address format is shown in FIG. 17. In this FIG. 17, field I denotes a global address, and field II denotes an address in an organization having a subnet ID and an interface ID.

FIG. 18 shows an example of an aggregatable global address, in which field I includes global address, and field II includes Site-Level Aggregation ID and Interface ID.

Further, as an application of the present invention, it is possible to use VPN address shown in FIG. 19. Here, FIG. 19A shows a case of employing IPv4 in the intranet, while FIG. 19B shows a case of employing IPv6 in the intranet.

In FIG. 19, there is provided a scope field 44 which stores a flag indicating whether or not VPN-ID 45 is a VPN closed in a service provider. In the case of closed VPN in the service provider, it becomes possible for the service provider to assign VPN-ID 45.

As another application of the present invention, a VPN address shown in FIG. 20 may be used. FIG. 20A shows the case of IPv4 employed in the intranet, while FIG. 20B shows the case of IPv6 employed in the intranet.

FIG. 20 shows an example that using an IPv4 global address as a VPN-ID inevitably results in obtaining a unique VPN-ID 45. For example, using an IPv4 global address assigned to an organization produces a unique address. At the same time, this makes it unnecessary to manage for maintaining VPN-ID 45 uniquely.

The foregoing description of the embodiments is not intended to limit the invention to the particular details of the examples illustrated. Any suitable modification and equivalents may be resorted to the scope of the invention. All features and advantages of the invention which fall within the scope of the invention are covered by the appended claims.

INDUSTRIAL APPLICABILITY

The techniques described herein allow a VPN service to be achieved with a remarkably reduced number of settings compared to other methods. This brings about less possibility of setting errors or operational mistake and therefore an operator may provide the service safely.

Because of the reduced number of settings against end user demands, the service may be provided in a short preparation period. In addition, a simple functional addition in an edge router is only required. For routers on users’ side and routers not located on user boundary, routers for general use may be used without need of modification, thus facilitating installation.

Further, when considering multi-vender connection using routers of multi-vender products, the method requires only a unicast routing protocol of general use having sufficient actual operation results, such as RIP, OSPF, IS-IS or BGP. Any peculiar protocol such as MPLS label distribution protocol is not necessary. Therefore, multi-vender connection may be achieved easily.

Moreover, the service may be introduced even when addresses assigned in an organization is overlapped.

To conclude, the present invention brings about a large effect, greatly contributing for the expansion of VPN services on the Internet.

The foregoing description of the embodiments is not intended to limit the invention to the particular details of the examples illustrated. Any suitable modification and equivalents may be resorted to the scope of the invention. All features and advantages of the invention which fall within the scope of the invention are covered by the appended claims.

Claims

1. A method of communication, comprising the steps of:

   receiving a first IP packet including a first source IP address and a first destination IP address from a network which is in compliance with IP
version 4;
converting the first source IP address and the first destination IP address of the first IP packet under IP version 4 into a second source IP address and a second destination IP address of a second IP packet under IP version 6 by combining an identifier identifying the network which is in compliance with IP version 4 with the first source IP address and with the first destination IP address; and
transmitting the second IP packet to the Internet in compliance with IP version 6, wherein the second source IP address under IP version 6 includes the first source IP address under IP version 4, and the second destination IP address under IP version 6 includes the first destination IP address under IP version 4.

2. An apparatus, comprising:

means (31) for receiving a first IP packet including a first source IP address and a first destination IP address from a network which is in compliance with IP version 4;
means (32) for converting the first source IP address and the first destination IP address of the first IP packet under IP version 4 into a second source IP address and a second destination IP address of a second IP packet under IP version 6 by combining an identifier identifying the network which is in compliance with IP version 4 with the first source IP address and with the first destination IP address; and
means (30) for transmitting the second IP packet to the Internet in compliance with IP version 6, wherein the second source IP address under IP version 6 includes the first source IP address under IP version 4 and the second destination IP address under IP version 6 includes the first destination IP address under IP version 4.

Patentansprüche

1. Verfahren zur Kommunikation, aufweisend die folgenden Schritte:
Empfangen eines ersten IP-Pakets, aufweisend eine erste Quellen-IP-Adresse und eine erste Ziel-IP-Adresse von einem Netzwerk, das in Übereinstimmung mit IP-Version 4 ist;

2. Gerät, aufweisend;
Mittel (31) zum Empfangen eines ersten IP-Pakets, das eine erste Quellen-IP-Adresse und eine erste Ziel-IP-Adresse von einem Netzwerk, das in Übereinstimmung mit IP-Version 4 ist, enthält;

Revendications

1. Procédé de communication, comportant les étapes consistant à :
recevoir un premier paquet IP comprenant une première adresse IP de source et une première adresse IP de destination provenant d’un réseau qui est conforme à la version IP 4 ;
convertir la première adresse IP de source et la première adresse IP de destination du premier paquet IP sous la version IP 4 en une seconde adresse IP de source et une seconde adresse IP de destination d’un second paquet IP sous la version IP 6 en combinant un identifiant identifiant le réseau qui est conforme à la version IP 4 avec la première adresse IP de source et avec la première adresse IP de destination ; et
transmettre le second paquet IP à Internet conformément à la version IP 6, dans lequel la seconde adresse IP de source sous la version IP 6 comprend la première adresse IP de source sous la version IP 4, et la seconde adresse IP de destination sous la version IP 6 comprend la première adresse IP de destination sous la version IP 4.
2. Appareil, comportant :

un moyen (31) pour recevoir un premier paquet IP comprenant une première adresse IP de source et une première adresse IP de destination provenant d’un réseau qui est conforme à la version IP 4 ;

un moyen (32) pour convertir la première adresse IP de source et la première adresse IP de destination du premier paquet IP sous la version IP 4 en une seconde adresse IP de source et une seconde adresse IP de destination d’un second paquet IP sous la version IP 6 en combinant un identifiant identifiant le réseau qui est conforme à la version IP 4 avec la première adresse IP de source et avec la première adresse IP de destination ; et

un moyen (30) pour transmettre le second paquet IP à Internet conformément à la version IP 6, dans lequel la seconde adresse IP de source sous la version IP 6 comprend la première adresse IP de source sous la version IP 4 et la seconde adresse IP de destination sous la version IP 6 comprend la première adresse IP de destination sous la version IP 4.
FIG. 2

```
+---+---+---+---+---+---+---+
|   |   |   |   |   |   |   |
+---+---+---+---+---+---+---+
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------------------------------------------+
| Version | IHL | Type of Service | Total Length |
+-----------------------------------------------+
| Identification | Flags | Fragment Offset |
+-----------------------------------------------+
| Time to Live | Protocol | Header Checksum |
+-----------------------------------------------+
| Source Address |
+-----------------------------------------------+
| Destination Address |
+-----------------------------------------------+
| Options | Padding |
+-----------------------------------------------+
```

FIG. 3

```
+---+---+---+---+---+---+---+
|   |   |   |   |   |   |   |
+---+---+---+---+---+---+---+
|   |   |   |   |   |   |   |
+---+---+---+---+---+---+---+
+-----------------------------------------------+
| Version | Traffic Class | Flow Label |
+-----------------------------------------------+
| Payload Length | Next Header | Hop Limit |
+-----------------------------------------------+
| Source Address |
+-----------------------------------------------+
| Destination Address |
+-----------------------------------------------+
```
FIG. 4

DATA IPv4 HEADER

FIG. 4A

DATA IPv4 HEADER IPv6 HEADER

FIG. 4B

DATA IPv4 HEADER IPv4 HEADER

FIG. 4C

DATA IPv4 HEADER Shim HEADER

FIG. 5

0 1 2 3

0123456789012345678901

+----------------------------------------+
<table>
<thead>
<tr>
<th>Label Exp</th>
<th>S</th>
<th>TTL</th>
</tr>
</thead>
</table>

Label: Label Value, 20 bits
Exp: Experimental Use, 3 bits
S: Bottom of Stack, 1 bit
TTL: Time to Live, 8 bits
FIG. 17

<table>
<thead>
<tr>
<th>10 bits</th>
<th>38 bits</th>
<th>16 bits</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>111111011</td>
<td>0</td>
<td>subnet ID</td>
<td>interface ID</td>
</tr>
</tbody>
</table>

I  II

FIG. 18

<table>
<thead>
<tr>
<th>3</th>
<th>13</th>
<th>8</th>
<th>24</th>
<th>16</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP</td>
<td>TLA</td>
<td>RES</td>
<td>NLA</td>
<td>SLA</td>
<td>Interface ID</td>
</tr>
<tr>
<td>ID</td>
<td>ID</td>
<td>ID</td>
<td>ID</td>
<td>ID</td>
<td></td>
</tr>
</tbody>
</table>

<---Public Topology----> Site
<-------->
Topology
<--------Interface Identifier-------->

Where

FP Format Prefix (001)
TLA ID Top-Level Aggregation Identifier
RES Reserved for future use
NLA ID Next-Level Aggregation Identifier
SLA ID Site-Level Aggregation Identifier
INTERFACE ID Interface Identifier
REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6038233 A [0015]